Tech

JO AL™

APAC
ISSUE 3

All-In: FACING DOWN CYBERCRIME

♠♥ With a Fold-Proof Strategy ♣♦

PAGE 4

Insight®

Table of Contents

Editorial

Editor-in-chief

Athena Thompson & Amy Protexter

Production managers

Megan Hayes, Maria Mahanes, Kayeene Asistio, Sil Suelto

Senior editor

Isabel Ticlo

Editors

Kellie Herson, Heather Horn, Claudia Hrynyshyn, Lauren Kawalec, Krista Leland, Jesse Millard, Rachel Tucker, Jillian Viner, Scott Walters, Athena Thompson, Matt Garrod, Paul Cina

Featured contributors

Jason Rader, Mike Morgan, Jonathan Parnell, Lloyd Tanaka, Amol Ajgaonkar, Carmen Taglienti, Roland Leggat, Rob Elliot, Chris Kapusta, Bob Bogle

Design

Art director

Chris Reddoch

Art production managers

Charles Cruz, Rovi Sia, Nicola Stamm

Creative designers

Chancel Gonzales, Mervin Lorenzo, Katherine Magpantay, Angelie Perez, Reyman Santos, Anthony Urbano

Letter From the Editor

Are You All-In?

To be honest, I'm not much of a gambler. It's not that I'm entirely risk averse, it's just that I recognise the difference between a risk and a gamble. With proper insight, support and planning, a calculated risk can really pay off. But a gamble — that's purely a game of chance, and it's hard to feel lucky when you know the odds are never in your favour.

That's how it is right now with cybersecurity. Security leaders are doing the best they can to play their cards right, but it's a raw deal when everyone else at the table isn't playing by the rules. So how do you win at something when you're playing with cheaters, scammers and hackers?

You outsmart them.

In this issue of the Tech Journal, we're going all-in on cybersecurity. We invite you to take a seat while our cybersecurity experts divulge how a programmatic and strategic approach can strengthen your odds at gaining — and keeping — the upper hand. You'll learn how advanced tools are helping to detect the "tells" of cyberthreats (All-In: Facing Down Cybercrime With a Fold-Proof Strategy), how to play your ace against ransomware (Mounting a Ransomware Defense for the Big Picture), and how to play a winning hand by adopting passwordless authentication (How to Navigate the Journey to Passwordless Authentication).

Also in this issue, we're sharpening your automation strategy (Slowing Down to Speed Up: How to Build a Winning Automation Strategy), we're keeping a close eye on hot computer vision trends (6 Computer Vision Trends Transforming the Business Landscape), and we're sharing some great client stories to help you plan your next move across your technology journey. This edition we share how Hauora Tairāwhiti, a district-health service in New Zealand, embarked on their Cloud journey and adopted modern secure ways of working, as well as how L'Oréal Travel Retail APAC, based in Hong Kong, has been navigating COVID with uninterrupted productivity and security protocols.

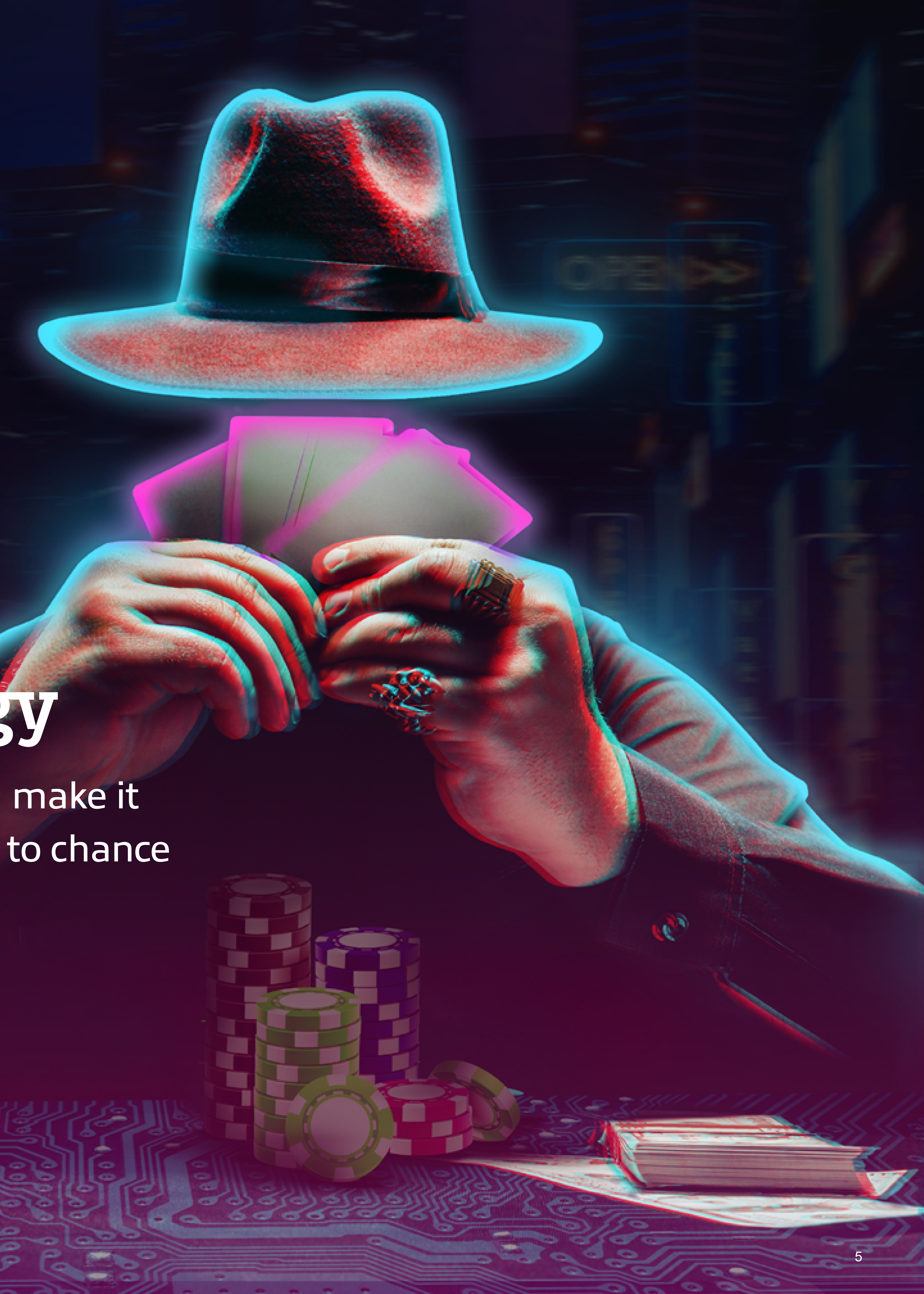
We hope you enjoy this issue and walk away with greater confidence that, even when the stakes are high, there's a path – and a trusted partner – to ensure you're holding all the aces.

Athena

Athena Thompson
Director Marketing and Strategic Partnerships ,
Insight APAC

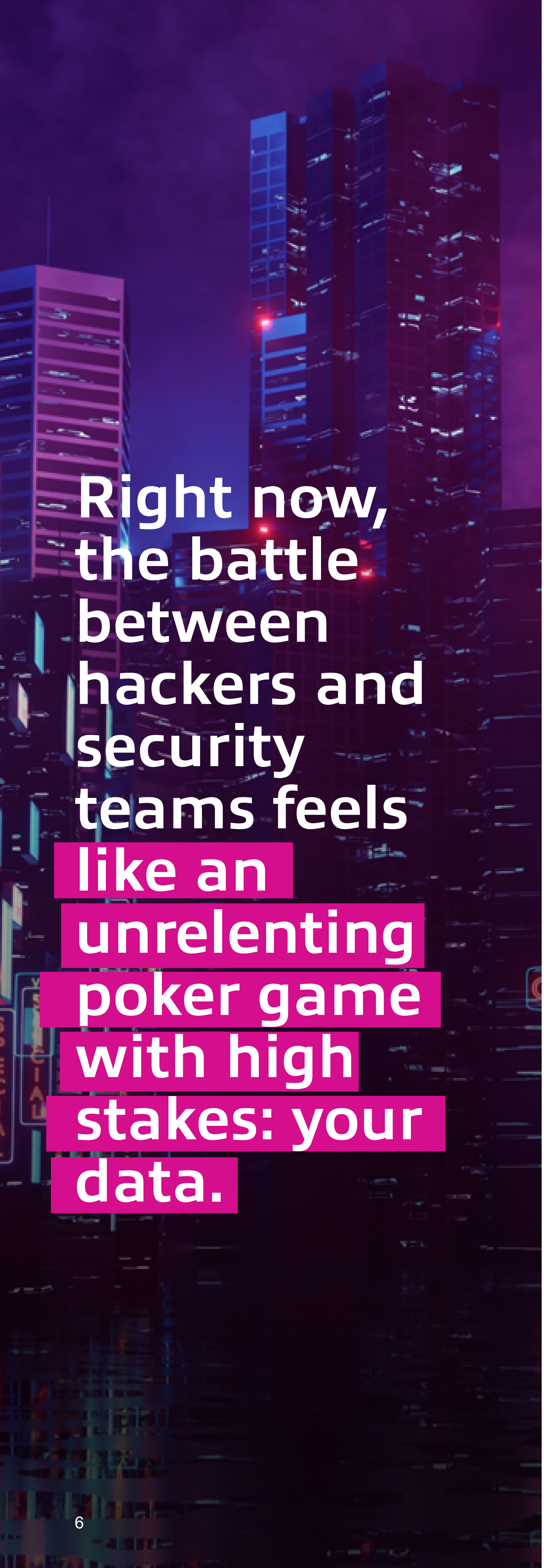
All-In: Facing Down Cybercrime With a Fold-Proof Strateg

How do you take a high-stakes game of chance and work to your advantage? You perfect what isn’t left — and start playing a better version of the game.



gy

make it
to chance



Right now, the battle between hackers and security teams feels like an unrelenting poker game with high stakes: your data.

You don't know what tool sets cybercriminals have — or what hand they're playing — and they don't know what you have, either (unless you've got a clear tell). Your data is powering the pot, and it's growing relentlessly whether you like it or not.

After working in the cybersecurity space for 25 years, I think there will always be some elements of murkiness or chance when it comes to cybersecurity. But I also see an opportunity to lean into what you can control, learn to play the hand you have now and graduate to a more measured game.

As the national director of network and cloud security for Cloud + Data Centre Transformation at Insight, here's how I help organisations do it.

It all starts with the north star of cybersecurity maturity: The National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The framework offers best-practices guidance across five areas: Identify, Protect, Detect, Respond and Recover. It was created precisely because too many organisations were betting most of their resources in one area and getting compromised in others.

Here's my take on the NIST Cybersecurity Framework — along with some poker mantras that will put you on a path to mastering it.

1. Identify

Know thy hand, know thyself.

Let's say you're brand new to the game of poker. You have no concept of hand rankings. If you're playing a three of a kind, how would you know that it's better than a pair? If you have a strong hand, such as a flush, how would you know that a full house can beat it? Getting good at anything — a sport, an art or cybersecurity — requires arming yourself with foundational knowledge around what you have and how it works.

Admittedly, it concerns me when security teams say, "I don't know what I don't know." When it comes to cybersecurity, you can't protect what you don't know exists. It's why assessments are wildly important to Insight's approach. It's also why governance falls under this bucket, which means defining what your objectives are, the overall risk associated with those objectives, and the assets or endpoints you're trying to secure.

> When it comes to cybersecurity, **you can't protect what you don't know exists.**

$8.64M

The United States has the world's highest average data breach cost, according to IBM.

The good news is that this mantra spans across the entire NIST Cybersecurity Framework. There are assessments built to improve your awareness in every one of the five areas across a variety of use cases, so it's always possible to know what you're bringing to the table.

But even once you have that foundational knowledge, you should always be evolving your cybersecurity program — the way the best poker players continue studying the game and learning new strategies. Remember: The game of poker is ongoing. You're regularly getting dealt new hands (new technologies, tool sets and methodologies). So are cybercriminals. Because of that, you always need to know what you're working with, because *it will change*.

2. Protect

Ace your poker face.

In the NIST Cybersecurity Framework, the Protect category is all about prevention — making sure you aren't letting your guard down or exposing a weak spot that can be exploited.

I find that organisations' security controls are largely protective and include:

- Identity and access
- Perimeter controls
- Data encryption
- Regular backups and updates
- End-user training

But even with the wealth of protective solutions available, many security teams remain unsure. According to Cybersecurity Insiders' 2020 State of Enterprise Security Posture Report, 64% of organisations said they lack confidence in their security posture.

Perfecting your cybersecurity poker face isn't so much about concealing a good or bad hand. Rather, it's about doing what needs to be done to keep people from even thinking about taking advantage of your team. Someone with a great poker face sends the same message that good protective controls do: I'm a fortress, and I can't be rattled.

Phishing emails: Top subject lines helping hackers cash in

According to Q4 2020 analysis from KnowBe4

- Password Check Required Immediately
- Touch Base on Meeting Next Week
- Vacation Policy Update
- COVID-19 Remote Work Policy Update
- Important: Dress Code Changes

3. Detect

Watch the table. Play your opponent.

I'm a big fan of the poker scene in the 2006 James Bond film, "Casino Royale." In the scene, Bond spends the first few rounds keenly observing his main opponent, Le Chiffre, to find out what his tell is. Bond even mucks his cards on purpose early on, eventually learning Le Chiffre's tell: placing a single finger on the left temple. This know-your-enemy strategy pays off for our hero to the tune of $115 million in winnings.

In many ways, it was a masterful display of tuning in to the table (the way great security teams invest in thoughtful detection processes). In the NIST Cybersecurity Framework, the detect layer is about scanning for anomalies and events, and continuously monitoring your software, hardware and network. It's also worth noting that detection is largely procedural. It's critical to have a clearly defined process in order to detect, as well as know what to *do* once something *is* detected.

With the variety of tool sets hackers use to exploit your environment, threat intelligence can play a huge part in shifting your cybersecurity strategy. Take advantage of the array of premium and free threat intelligence feeds to validate the traffic you see on your network.

Operationalising this technology — and making it your security team's modus operandi — is very much worth the effort when playing the long game of cybersecurity.

Remember: If you don't have the best hand during the game, it's possible to tip the scales in your favour simply by paying attention.

Security analytics is evolving.

Artificial Intelligence (AI) and Machine Learning (ML) aggregate user and entity behaviours, combining with threat intelligence to give you the best odds at winning at detection and shutting down formidable opponents.

World's fastest hacker?

Kevin Mitnick made the FBI's Most Wanted list by hacking into 40 major corporations. After serving time, Mitnick now uses his skills for good — offering highly sought after security consulting and awareness training.

4. Respond

Don’t let setbacks throw your game off.

Tilt is a fascinating phenomenon in poker. It hits when a player is mentally unnerved by a bump in the road, whether it’s a string of bad hands or a trash-talking opponent. Tilt causes players to play emotionally, make bad calls or even lose entire games. Even though it’s widely dreaded, many players don’t have a thoughtful plan to deal with tilt. They’d much rather work on other aspects of their game.

It’s common for organisations to silo a lot of money, time and resources into one cybersecurity category, leaving response for last. If and when a breach occurs, this proves to be a flawed approach. Mitigate the chances of getting caught off guard by building a response playbook guided by questions like:

- How will we notify users of incidents and whose data may be at risk?
- How will we investigate and contain the breach?
- How will we report the incident to law enforcement and other authorities?
- How will we document lessons learned and update our methods as needed?

Every minute you put into planning your response is going to save you days, hours and dollars on the backend.

The **worst** time to figure out what to do — is when it’s critical that **you do it now**.

Types of poker tilt

Loose tilt: This is the most common type of tilt caused by frustration, too much confidence, impatience or a longing to make up for losses.

Passive tilt: Difficult to detect, this tilt leads to unassertive, weak playing. It’s frequently caused by a loss of confidence or fear of taking risks.

Stereotypical tilt: This means playing by the book in a fixed pattern without adapting to the game at hand, causing slipups.

Fancy play syndrome: This occurs when a player overthinks and uses an over-the-top strategy to dupe an opponent.

5. Recover

Live to play another day.

Cybersecurity response is planning what you'll do in the heat of a setback to prevent a downward spiral — and avoid tilt. Recovery is your process for picking yourself back up and playing on.

Classic security has long been about putting up walls, keeping the bad guys out or locking down your protective controls. There's a wealth of options for protection. But how many options are there for recovery-corrective-based controls? Not a lot. Because of this, it's critical to take the corrective options that do exist, such as restoring from backup or malware deletion, and get very clear about the how these types of tools integrate with your environment. Beyond that, it's all about rebuilding and getting back to business with as little disruption or further damage as possible.

This can be done through:

- Having a detailed cyber incident recovery strategy and plan
- Training all parties on that strategy
- Testing the strategy in a variety of ways (tabletop, simulation, etc.)
- Updating that plan when changes occur or whenever necessary

When it comes to cybercrime, it's no longer if, but when. The goal shouldn't be to never have a security event. It's that when an incident occurs, it doesn't decimate your business.

Are you going to take some hits in poker? Yes. But you can employ strategies that could help you win your money back — or even the whole game in the end.

Five data breach downswings in 2021

As reported by Identity Force

1. **Guess**: A ransomware attack on the retail fashion giant resulted in a data breach compromising sensitive customer information. The breach exposed Social Security numbers, passport numbers and financial account numbers.

2. **Volkswagen & Audi**: A third-party marketing services supplier disclosed the personal information of 3.3 million customers, including names, addresses and phone numbers.

3. **Facebook**: The personal data of 533 million Facebook users from 106 countries was leaked and released to a low-level hacking forum.

4. **Hobby Lobby**: A cloud-bucket misconfiguration led to a database leak of 300,000 customer records, including names, the last four digits of payment cards and the Hobby Lobby app source code.

5. **California DMV**: Personal information from the last 20 months of California vehicle registration records were stolen, including names, addresses and license plate numbers.

Transcending chance

There's hot debate whether poker is mostly skill or chance. I think it's both.

A single hand of poker is an irrefutable instance of chance. Playing a full game, or a tournament, is a different story. That's when you can use the controllable aspects of the game to your advantage: your understanding of the deck, the players and the rules; the risk you have related to what you've got; how much you're betting and how much is at stake.

Organisations already have people, processes and technologies in place. That's why poker is a good analogy for the current state of most organisations. Maybe you already have a king and an ace. Maybe your protective controls are over a 10. Maybe you have all hearts, or products, that integrate well together. But remember that in poker, you don't just play one hand, and you certainly don't bet it all on the first hand. That's the iterative process of security — it's many hands.

With a programmatic approach, I believe that organisations can transcend the chance aspect of poker and even graduate to a new, more measured game.

And on we'll play.

Strengthen your hand.

See how Insight is helping organisations reduce risk, maintain compliance and make confident technology decisions.

About the author

Jason Rader

National Director of Network and Cloud Security for Cloud + Data Centre Transformation, Insight

Microsoft Sentinel Foundations

Gain control and visibility of your entire IT security environment

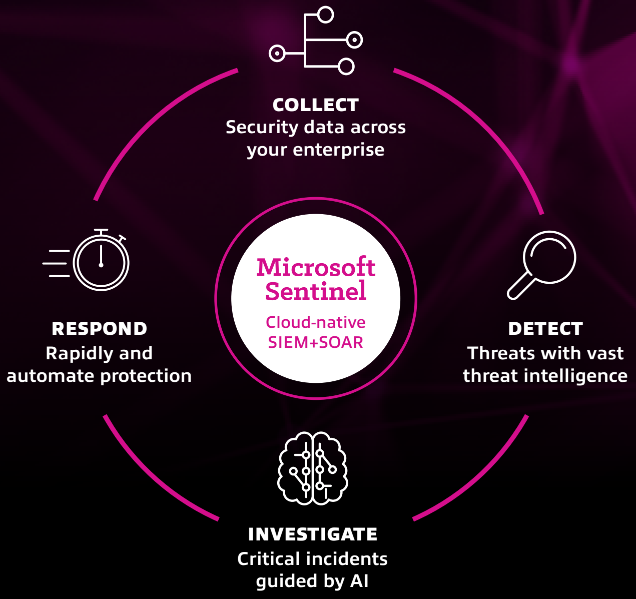
The proliferation of platforms, data, users and mobility is creating new challenges for security teams. Visibility and manageability are hard to attain, let alone staying on top of endless alerts and tool updates.

Microsoft Sentinel lets you combine and analyse security data from all your users, endpoints and infrastructure to make threat protection smarter and faster.

HOW WE HELP

Insight's Microsoft Sentinel Foundations offers expert-led workshops that combine training and assessment of your security envrionment.

Centred around best practices for cloud and security, this engagement familiarise your team with new technology and provide you with a working environment you can begin using right away.


COLLECT
Security data across your enterprise

DETECT
Threats with vast threat intelligence

INVESTIGATE
Critical incidents guided by AI

RESPOND
Rapidly and automate protection

Microsoft Sentinel
Cloud-native SIEM+SOAR

BENEFITS

- Collect security data across your enterprise
- Detect threat with vast threat intelligence
- Respond rapidly and automate protection

Learn more about Insight's Microsoft Sentinel Foundations

Insight.

Tech from the Heart

Diversity and Inclusion

Brings True Change, Impact and Business Results

> **At Insight, we believe that the more diverse our teammates' skill sets, perspectives, and backgrounds, the more innovative we can be when uniting on our common goal of building meaningful connections to help businesses run smarter.**

Here at Insight, diversity and inclusion isn't simply a box to be ticked. It brings major benefits for our teammates, our growth-mindset culture - and to our business results.

I'm passionate about diversity and inclusion because I think it is a pragmatically better outcome for everybody. We can be a faster-growing, more innovative, more rewarding and better business through diversity, inclusion and belonging.

Our true competitive advantage lies in our people, bringing their whole selves to work, coupled with their empowerment to challenge the status quo, and each other, respectfully, and bring new ideas and perspectives into the mix. As Katherine Clayton, Insight ANZ People & Culture Lead says: "Diversity brings new ways of thinking, new innovation, and enables us to push the boundaries of performance; and when we are successful, when we're adding value and performing to our potential, we're also more likely to enjoy our work."

But diversity is just one part of the solution. While I am passionate about getting more women in the room, I'm equally passionate about ensuring that once women are in the room, their voices are clearly heard, and their leadership and impact is championed across the organisation. Of course, gender is only one aspect of diversity, and at Insight we're focused on embracing and celebrating all facets of individual difference that contribute to the identity of our teammates.

Getting the balance of people in business right is only half the story. If you don't pursue strategies to make sure that everyone in that now diverse pool of talent is able to show up, bring their authentic selves to work and all of their diverse experiences to the table, then you are really not getting the benefits you were seeking in the first place.

With that in mind, Insight Asia Pacific has a Diversity and Inclusion Council looking at diversity with three specific impact areas in mind: Women in Technology; Reconciliation and representation of Aboriginal and Torres Strait Islander Peoples; and People with Disabilities. With a focus on the Women in Tech lens for this article, I'd like to share a few impactful initiatives we're focused on right now: including the Champions of Change, a Microsoft-sponsored

Women in TECH with Insight

Partner Community syndicate, the Women Rising Leadership program and our Women In Technology spotlight.

Champions of Change acknowledges that women are significantly under-represented at Board and senior-executive level and aims to create change by engaging male leaders who currently occupy those positions to drive change from the top. I participate in the Microsoft Partners Chapter to learn, collaborate and contribute to practical positive change. This forum is driving for me personally, and the momentum within our organisation and industry is tremendous.

Women Rising is also a Microsoft sponsored program and it's having a significant impact on our business. Designed by women, for women, it provides the tools and techniques to help women "rise through the ranks", while Women in Technology works to build the pipeline of women interested in starting or transitioning into technology from any industry or background. We recently had two alumni of the Women Rising program talk with our APAC Executive Leadership team, which has 45% women ratio, and the ideas and appetite to drive new initiatives was palpable.

Across these three programs, it's a balance of reflecting on the fact that the technology industry is still largely run by men who need to consciously create more space for more women to be heard, to thrive and to lead, and at the same time, we need to provide the resources to allow women to become a bigger voice. It's a top down, bottom-up approach which we believe can make structural shifts in the industry.

Here at Insight, and with a global perspective, I'm particularly excited about the recent announcement on October 19, 2021, that our new Chief Executive Officer, as of January 2022 upon the retirement of our current CEO Ken Lamneck, will be Joyce Mullen, our current President of Insight North America. This is terrific for our company, and for the industry; it's terrific and the right next step and the right next global leader for Insight.

When you're prepared to challenge the status quo, you open a portfolio of opportunities for you personally, for your team, and for your business. While I'm proud of how far Insight has come, I'm conscious of how far we still must go. Likewise, while we're all accustomed to the rapid change of continuously emerging new technology, change on deeper issues doesn't happen overnight. By working together, we can make a lasting impact for good.

About the author

Mike Morgan
Senior Vice President & Managing Director,
Insight APAC

Slowing Down to Speed Up:

How to Build a Winning Automation Strategy

IT automation is about going faster — building out a good automation strategy is about something else entirely.

Have you ever been riding a bike when suddenly, you get speed wobbles? You feel like you're going at warp speed. The bike seems to take on a life of its own. You can't pedal any faster to get back on track.

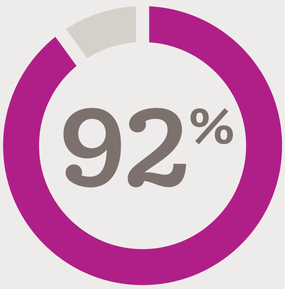
On the surface, IT automation and cycling have nothing to do with each other. But automation without a thoughtful strategy is a lot like riding a bike with speed wobbles: In the race to go faster with automation, you have to slow down to regain control.

So, how do you automate with purpose? Here's an approach for creating a thoughtful automation strategy for a more enjoyable ride.

Define why you're making the trek.

Start by asking a few questions: "What does automation mean to our organisation? Why do we want to automate? What business outcomes are we hoping to achieve? Is our desire to automate making up for a step we're skipping in business decisions?"

The process of asking and answering questions like these uncovers intent. It unearths valuable information that will help you set realistic and measurable goals. During automation projects, it's common to not consider the implications for the entire ecosystem — and often, there isn't enough discussion about how to turn the ideas you have into reality. Those early discussions matter. They force you to take a bird's eye view before zooming in on the details.



92% of business leaders agree:

Automation is key to succeeding in a post-COVID-19 world.

Once you've figured out your organisational goals, it's imperative to understand what your organisation's policy and guidelines are for automated releases. Without understanding these aspects of your environment, automation can cause problems like backpedaling, failed adoption and more inefficiencies.

After you've determined your purpose for automation and figured out where you can get the greatest gains, assess your cultural readiness. For many organisations, this is often the biggest roadblock.

What makes IT automation worth the journey?

Enhanced agility and scalability for the workforce

Greater focus on customer experience

Improved end-to-end process flow

Increased efficiency through process standardisation

Commit to a mindset shift.

Automating with purpose requires addressing silos that happen all too frequently within an organisation.

As a senior consultant for Cloud + Data Centre Transformation at Insight, when I talk to clients, I often find that they want to implement an overarching governance policy — and yet, there are too many silos preventing effective coordination. In order to implement automation that makes sense across teams, you must work on deconstructing siloes, as well as shifting a change-resistant culture.

Only

1 in 5

organisations are embracing process automation in its most advanced forms — and nearly

1 in 10

have only taken the initial steps toward automation.

In my experience, changing culture always starts with relationships. It requires talking to different people within the organisation and building trust through cross-team visibility. Although it’s tempting to only operate within the clearly defined boundaries of your own role, once you determine what you need from other people in the organisation — and what they need from you in return — you can begin figuring out what types of automation initiatives can realistically be embraced across teams.

Generating buy-in for automation doesn't happen organically and requires the weight of leadership behind it. So, finding a high-level champion who will use their influence to help change the culture is also critical.

4 main test validations for easy coasting

Unit testing
Vetting individual components of a system and fixing bugs as needed

Integration testing
Ensuring various interfaces function together well

System testing
Testing your programming framework against predefined needs

User acceptance testing
Using the product through the eyes of the end user

For instance, your organisation may have a centre of excellence with staff working on plenty of exciting automation projects. But if there's a certain culture within the company sending the message that these projects aren't necessary, then it's doomed to fail. Alternatively, if you have a high-level person championing the technicians working on these projects, the projects are much more likely to succeed in the long term.

Now, map your route.

Once you've slowed down, asked thoughtful questions and ensured cultural buy-in, the nuts and bolts can take centre stage via a process map and Value Stream Mapping. This involves:

- Test validations (unit, system, integration and user acceptance)
- Service-Level Agreements (SLAs)
- Service-Level Objectives (SLOs)
- Service-Level Indicators (SLIs), which can be defined once SLAs and SLOs are intact

- Objective and Key Results (OKRs)
- Key-Performance Indicators (KPIs), which can be defined once OKRs are intact; will be how you measure the speed which results from your automation

> ”Observability should always come before a release — never after.”

The process of Value Stream Mapping can be intensive. But for every client I’ve worked with, it’s a worthy endeavor and a key piece to successful automation adoption. There’s nothing worse than getting something out to market, then finding out something else broke along the chain because testing protocols weren’t defined or acted upon beforehand. Observability should always come before a release — never after.

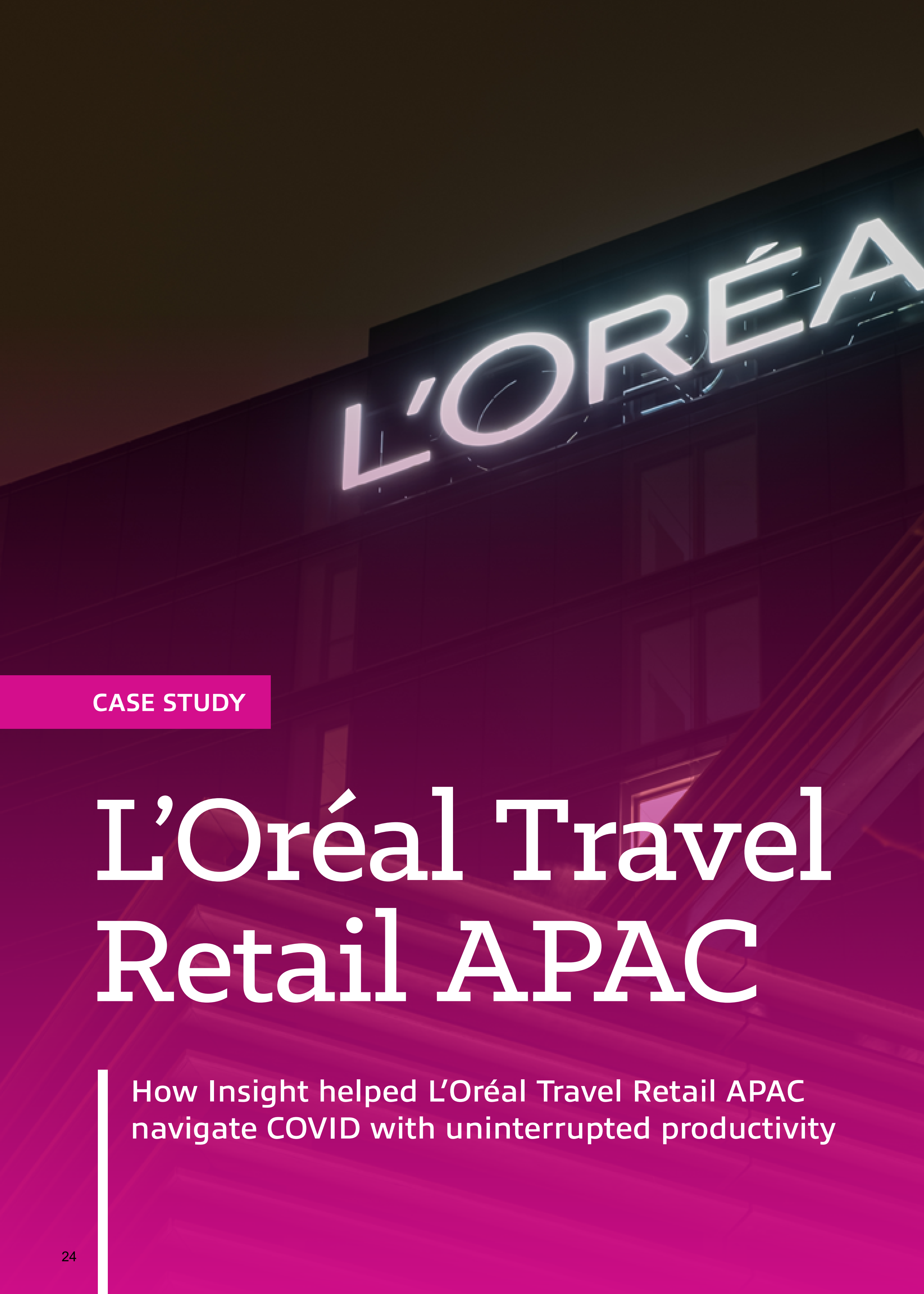
Ride on.

It can be easy to confuse automation with orchestration. Automation is about a set of repetitive tasks, while orchestration is about a lot of tasks working together for an outcome. But orchestration doesn’t happen hastily. It’s deliberate. It’s intentional. It forces you to take a step back, the way speed wobbles force you to slow down. If we can start thinking about automation as a strategic journey with purpose, we’ll be far more likely to hit our strides and thrive.

Automate with purpose. Building out a multilayered strategy can seem daunting. Enrolling guidance at every phase can help ensure long-term success.

About the author

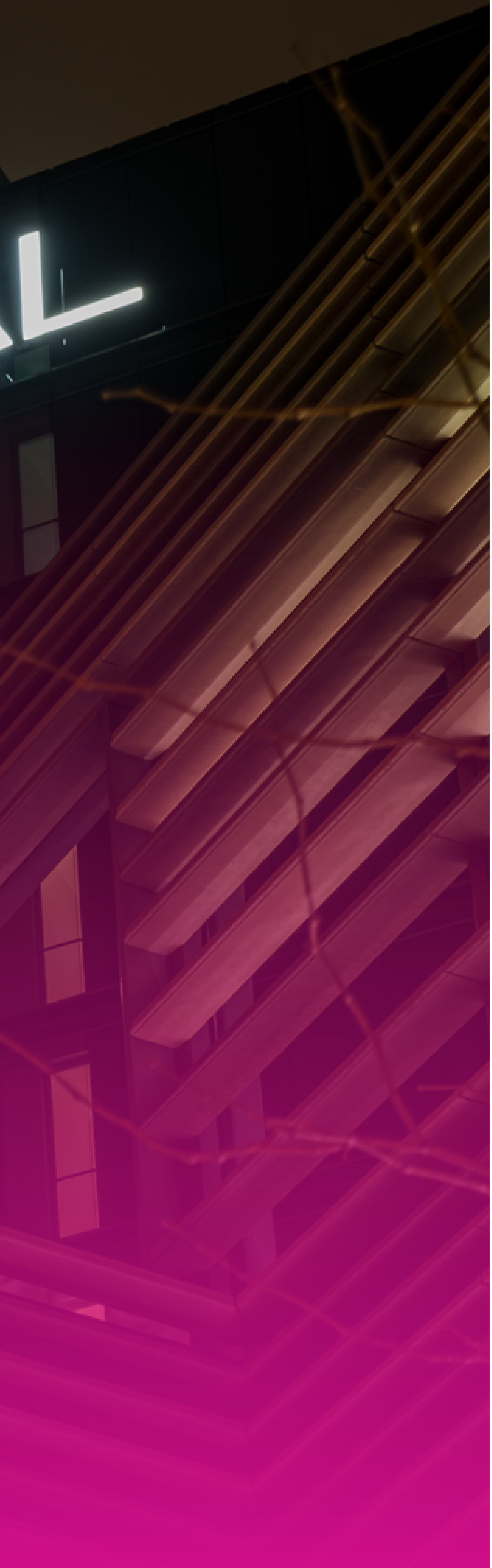
Jonathan Parnell
Senior Consultant for Cloud + Data Centre Transformation, Insight



CASE STUDY

L’Oréal Travel Retail APAC

How Insight helped L’Oréal Travel Retail APAC navigate COVID with uninterrupted productivity



As COVID restrictions hit Hong Kong, cosmetics company L'Oréal Travel Retail APAC realised the necessity for rapid change to the way in which its people access and use technology resources and receive support for their devices. It also recognised an immediate requirement to equip employees with everything they require to work successfully from home, all of which had to happen in a vanishingly small space of time and within the restrictions imposed as the local government sought to stamp out the spread of the disease. Through an engagement with Insight, the company has benefited from a professional advisor delivering quality remote support, along with new solutions that addressed short term requirements while positioning L'Oréal Travel Retail APAC to continue powering productivity into the future even when faced with unusual times.

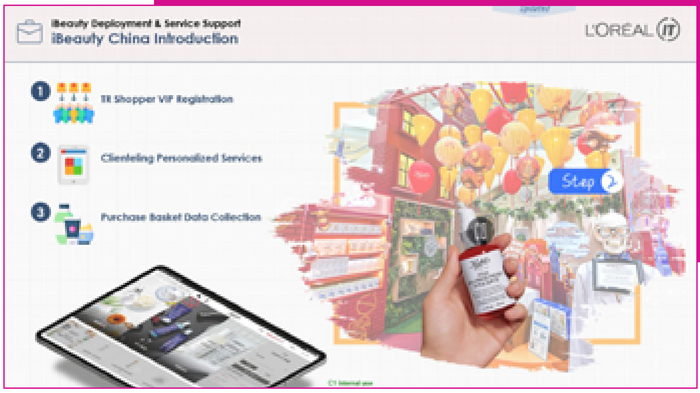
L'Oréal Hong Kong was established in 1983 as a subsidiary of the L'Oréal Group and comprises three divisions, L'Oréal APAC, L'Oréal Travel Retail APAC, and L'Oréal Hong Kong. The company offers more than 20 world-famous brands of high-quality products within four divisions, namely L'Oréal LUXE, Consumer Products, Professional Products, and Active Cosmetics. Recognised as a 'Caring Company' by the Hong Kong Council of Social Services since 2003, L'Oréal is a community-minded organisation and has offices in the Sun Hung Kai Centre.

Situation

Prior to the pandemic, L'Oréal Travel Retail APAC had five helpdesk engineers supporting a staff complement numbering more than 1,400 individuals. When the government mandated citizens to work from home to slow the spread of the coronavirus, the cosmetics company needed an improved technology support regime along with the rapid rollout of devices and software which would equip all employees to work from home.

CIO Specky Wong explains that while most staff occasionally worked from home ahead of the pandemic, not all are appropriately equipped with the devices, connectivity or even workspaces to do so. "Internally we had changed most of our systems already to online platforms which allow ‘work from anywhere’, with many staff using those platforms while in the office. The problem was, with the government recommending working from home and other social distancing initiatives, we suddenly had a lot more staff at home. Those staff want to work as much as the company needs their contribution.”

A further complication was presented by newly hired senior employees arriving in the city. Required to quarantine, these individuals needed access to devices and provisioning into the L’Oréal Travel Retail APAC business systems with which they would work. “Our internal IT department just wasn’t equipped to keep things moving in this dramatically different business environment,” Wong points out.



iBeauty Deployment & Service Support

iBeauty China Introduction

L’ORÉAL IT

1 TR Shopper VIP Registration

2 Clienteling Personalized Services

3 Purchase Basket Data Collection

Solution

With Insight already a trusted partner for other aspects of its technology sourcing requirements, L’Oréal Travel Retail APAC turned to the solutions provider for additional support. Understanding the pressing need for a comprehensive response, Insight responded with the rapid establishment of an improved support team, while also immediately sourcing a range of approved devices from which L’Oréal Travel Retail APAC’s staff members could choose. These include devices from vendors such as Apple, HP and others.

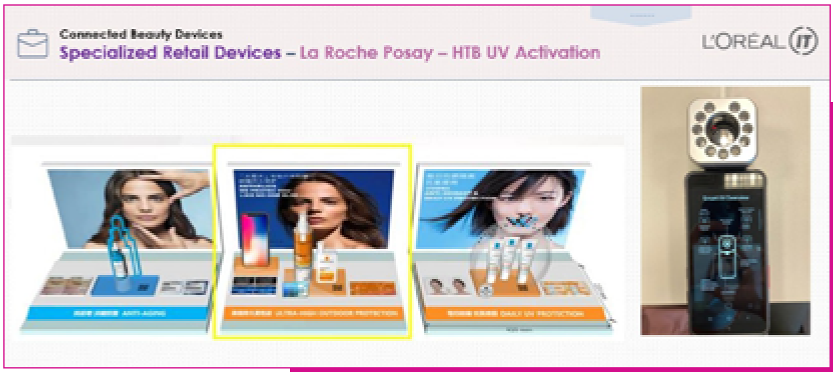
Wong stresses that for the cosmetics company, quality and performance is expected across the board. “We were looking for a VIP service as all our users, and especially executives, expect a very high standard from the IT department. With COVID affecting business as usual, Insight has accurately and rapidly equipped the whole workforce with everything needed to work from home; in some cases, that meant issuing a new laptop or a new phone, or deploying WiFi equipment, and all the services needed to get the job done.”

A further dimension was added as L’Oréal Travel Retail APAC was compelled to adjust the way in which its retail outlets operate. Social distancing measures meant staff members could no longer directly interact with customers, so the company embarked on a process of implementing Apple iPads and Microsoft HoloLens devices in-store, with interactive displays where shoppers can experience products, suggestions, and ideas. These devices, too, were rapidly sourced and delivered – along with connectivity solutions where necessary – to L’Oréal Travel Retail APAC stores around the city.

Devices, of course, are only part of the solution, as they must be appropriately configured and supported so working people can perform their duties without interruption. Wong says Insight has successfully worked with the global L’Oréal team to image devices to the company’s standards, delivering devices compatible with its environment from day 1.

Additional services packaged into the services delivery by Insight include mobile device management for the Device as a Service solution which covers orders, deployment, configuration setup, backed by workflow in support of standard operating procedures. This includes iOS deployment for iPhones, iPads and MacBooks, as well as Windows based devices. A further key component of Insight’s work addressed video conferencing setup with Microsoft Teams consulting, fully connecting L’Oréal’s Hong Kong and Shanghai offices; where necessary, Insight has equipped L’Oréal Travel Retail APAC staff members with headsets and mobile monitors, allowing every individual to benefit from a satisfying video conferencing experience.

An initial three months of help desk support has included the establishment of an employee hotline, giving the company's people the full assurance of service should they require it, from the comfort and safety of their homes, while relieving an overwhelmed internal helpdesk.



Connected Beauty Devices

Specialized Retail Devices – La Roche Posay – HTB UV Activation

L'ORÉAL IT

Results

Wong credits the rapid and comprehensive response from Insight with supporting L'Oréal Travel Retail APAC's productivity in highly unusual circumstances. "They sourced the equipment we needed from multiple vendors, meeting the business need and timelines which meant there wasn't any need to postpone business projects," he confirms.

The adoption of video conferencing within the organisation has progressed smoothly, with Insight reaching out to individuals, providing advice and consulting to help optimise equipment and build knowledge. "They have also proposed a range of options with the devices, along with pros and cons. The business team appreciates that."

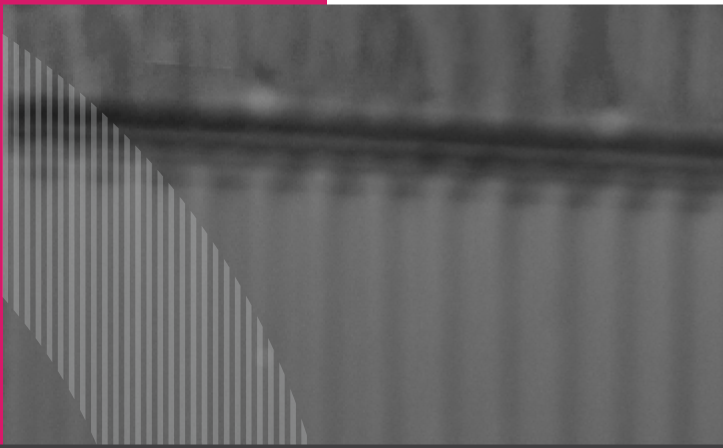
A larger support team has proven invaluable for the company's now-distributed workforce, and Wong notes that when any L'Oréal Travel Retail APAC employee requires IT support, it is immediately available by remote link through Insight – including, even, direct delivery of new equipment to homes.

Feedback from management and the business in general, says Wong, is that Insight consistently meets its Service Level Agreements. "That's much appreciated. We've seen that Insight doesn't mind working overtime, and with our 7 teams in locations all over the world with odd time zones, this willingness to go above and beyond has proven invaluable."

He further credits Insight with flexibility and ingenuity, attributes which have helped negotiate the unpredictable landscape of COVID restrictions. "For example, we've needed to get devices to people in hotels. It's never an issue for Insight."

Finally, Wong says the value of a true partnership has become clear in extenuating circumstances. "When we needed help, Insight stepped up. We've been able to work properly, meet project timeframes and organisational goals even without people in the office. They have provided us with choice and convenience – and with the pandemic rolling on, the investment we've made into equipping our people for flexible work is paying ongoing dividends."

> *"When we needed help, Insight stepped up. We've been able to work properly, meet project timeframes and organisational goals even without people in the office. They have provided us with choice and convenience – and with the pandemic rolling on, the investment we've made into equipping our people for flexible work is paying ongoing dividends."*
>
> **Specky Wong**
> CIO, L'Oreal Retail Travel



HOW SECURE IS YOUR SUPPLY CHAIN?

As the world strives to rein in COVID-19, many organisations are being challenged by a second universal threat — the cyber pandemic. Both are taking a heavy toll on people, organisations and communities.

In the last year, over 4.3 million lives have been lost in 220 countries and territories due to COVID-19 — and ramped up cybercrime totaled nearly $1 trillion. Both viral and cyber crises have surged with variants, deflating efforts to prevent further destruction.

These pandemics are intertwined.

Opportunistic cybercriminals have used COVID-19 disruption to strike consumers and businesses. The global shift to lockdowns and hybrid working fueled increases in cyberattacks, sparing no industry, including front-line organisations fighting outbreaks. Threat intelligence research estimates that organisations globally have experienced a 29% increase in cyberattacks.

The real breakout cybersecurity story in 2021, however, is the rise of retooled ransomware attacks, increasing 93% in the first six months of 2021. This new version of ransomware can identify and exploit vulnerabilities within interconnected supply chains. Technology providers, second- and third-level partners, and the users themselves are all susceptible to a “triple extortion” ransomware technique. This means that in addition to stealing sensitive data, criminals are threatening to release the data unless payment(s) are made.

Ransomware is not new, but the rules have changed.

CEO and Founder of Check Point Software, Gil Shwed, stated, “Countries and businesses are all realising the changing shape of life. In the past, there were clear rules about retaliation and why should someone attack someone else. Now, all the rules are being redefined and it’s much harder to attribute who’s behind a cyberattack than a physical or kinetic attack on a country or business.”

Long before the viral outbreak, Shwed warned of increasingly more potent, illusive and disruptive Gen V or fifth generation cyberattacks. This is no more fitting than with 2021’s high-profile ransomware cyberattacks that have included:

- **Colonial Pipeline:** A single compromised password found on the dark web was used for the hack.
- **JBS:** REvil, the prolific cybercriminal organisation responsible for this attack and Kaseya, went offline.

> **Ransomware** is an ever-evolving form of malware designed to encrypt files on a device, rendering the files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom isn’t paid.

These are the well-publicised attacks, but threat researchers say 15 new REvil attacks have occurred each week in the last several months with the U.S., Germany, Brazil and India as the top targets. On average, criminals behind ransomware attacks hit a new organisation every 10 seconds.

Mitigating risk with supply chain partners

One of the most complete analysis of supply chain attacks to date is in a recent European Union Agency for Cybersecurity (ENISA) publication. The following are recommendations for customers and suppliers to mitigate the risks with supply chain cyberattacks.

Suppliers should adhere with commonly accepted security practices:

- Ensure the infrastructure used to design, develop, manufacture and deliver products, components and services follows cybersecurity practices.
- Implement a product development, maintenance and support process consistent with commonly accepted product development processes.
- Implement a secure engineering process consistent with commonly accepted security practices.
- Consider the applicability of technical requirements based on product category and risks offering Conformance Statements to customers for known standards i.e., ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (or specific ones such as the CSA Cloud Controls Matrix (CCM) for cloud services), and ensuring and attesting to, to the extent

possible, the integrity and origin of open-source software used within any portion of a product.

- Define quality objectives such as the number of defects or externally identified vulnerabilities.
- Report security issues and use them as an instrument to improve overall quality.
- Maintain accurate and up-to-date data on the origin of software code or components, and on controls applied to internal and third-party software components, tools and services present in software development processes.
- Perform regular audits to ensure that the above measures are met.

To manage the relationship to suppliers, customers should:

- Manage suppliers over the whole lifecycle of a product or service, including procedures to handle end-of-life products or components.
- Classify assets and information that are shared with or accessible to suppliers, and define relevant procedures for their access and handling.
- Define obligations of suppliers for the protection of the organisation’s assets, for the sharing of information, for audit rights, for business continuity, for personnel screening, and for the handling of incidents in terms of responsibilities, notification obligations and procedures.
- Define security requirements for the products and services acquired.

- Include all these obligations and requirements in contracts; agree on rules for sub-contracting and potential cascading requirements.
- Monitor service performance and perform routine security audits to verify adherence to cybersecurity requirements in agreements; this includes the handling of incidents, vulnerabilities, patches, security requirements, etc.
- Receive the assurance of suppliers and service providers that no hidden features or backdoors are knowingly included.
- Ensure regulatory and legal requirements are considered.
- Define processes to manage changes in supplier agreements e.g., changes in tools, technologies, etc.

Conclusion

As long as viral and cyber pandemics continue to morph and evade eradication, they'll continue to take their toll on the global community. It's important to realise that as you invest further in cybersecurity prevention and deploy more advanced tools, the decades of cyberthreat activity show well-funded threat actors will also evolve. Ransom, phishing and other malware techniques will continue to advance, necessitating frequent assessments of your cybersecurity strategies and practices.

About the author

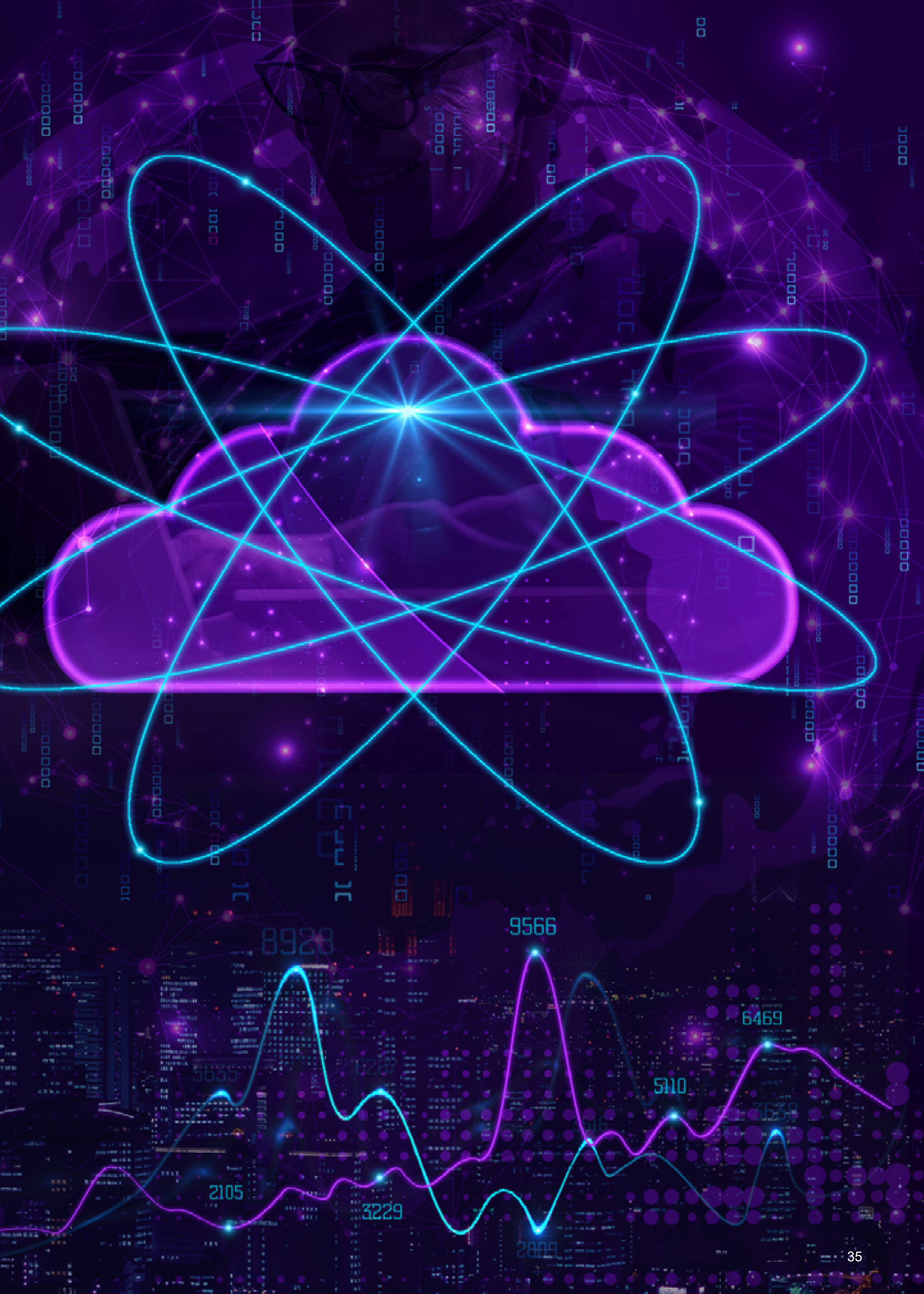
Lloyd Tanaka
Content Manager, Check Point Software

Cloud + Edge: The Innovation Equation

Maximise the value of your data by making the most of your infrastructure.

By now, most organisations are leveraging the cloud in some way, and usage is only increasing. Gartner forecasts worldwide public cloud spending will grow by 23% in 2021 as organisations face ongoing pressure to support complex workloads and the demands of hybrid work.

While some continue to focus on core business functions such as IT cost optimisation, risk reduction and the digitisation of processes, the majority of organisations are now looking further ahead — seeking opportunities to leverage their infrastructure to drive growth, accelerate product development and scale innovation.

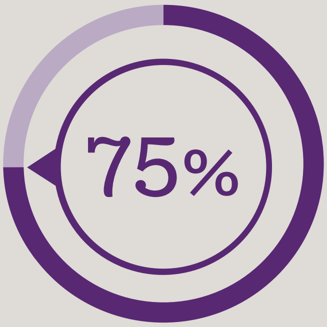

8928
9566
6469
5110
2105
3229
2809

Cloud foundations

The reason many organisations fail to transform — and therefore survive long term — comes down to a lack of skills needed to rapidly adopt new technologies. By providing access to democratised services and capabilities, the public cloud brings solutions such as Artificial Intelligence (AI) or the Internet of Things (IoT) within reach, without requiring deep, in-house expertise. This enables businesses to do more with less, faster.

No matter the intended outcome, the effectiveness of these solutions begins with the availability and accessibility of good, clean, unbiased data. Today's cloud providers make it easy to ingest, store, query and visualise massive amounts of data in support of a wide range of use cases. Backed by security, resiliency and geoproximity capabilities, the cloud enables users to access the tools and information they need to make better business decisions from anywhere in the world — without the need to connect to an on-premises data centre.

Ultimately, accelerated innovation in the cloud supports accelerated innovation across your company. Having the tools to execute on individual projects more effectively empowers your organisation to ideate and transform faster, driving disruption and competitive advantage. This is why, according to McKinsey, 75% of the cloud's predicted value comes from its ability to enable innovation.



75% of the cloud's predicted value comes from its ability to enable innovation.

But while public cloud has been established as foundational to enterprise innovation, focus is increasingly shifting to the edge. IDC reports companies worldwide are on pace to spend $240.6 billion on edge computing through 2024, investing in hardware, software and services at a compound annual growth rate of more than 15%.

So, what value does edge computing add to the innovation equation?

The edge advantage

Put simply, edge computing is an extension of your organisation's distributed or hybrid architecture which allows data to be processed closer to its source. As a result, one of the primary benefits of the edge is low latency.

Sending data back to a centralised public cloud for analysis causes lag, which may render the information unusable or, more importantly, result in missed opportunities to provide services within the critical user experience window. This is a key consideration for many AI- or IoT-based solutions, including predictive maintenance, defect detection, security and surveillance, and more. On a product assembly or food processing line, for example, data often has an extremely limited lifespan. Anomaly response must occur immediately to prevent low-quality products from reaching distribution. Other solutions such as Augmented Reality (AR) or Virtual Reality (VR) also depend on low latency to deliver real-time experiences.

The edge also supports innovation initiatives on the whole by reducing the technical, financial and security burdens associated with storing massive amounts of data in the cloud. Running workloads at the edge enables organisations to build solutions that leverage short-term or single-use data that can be discarded to reserve storage space or protect Personally Identifiable Information (PII). Sending only the inferences or insights derived from this data to the cloud informs broader decision-making while reducing risk, preserving privacy and improving overall bandwidth.

By 2025, Gartner predicts 75% of enterprise-generated data will be created and processed at the edge.

Cloud + edge benefits

While both cloud and edge solutions offer distinct benefits, when it comes to driving innovation, the most effective strategies capitalise on the complementary features of both approaches.

The cloud provides:

- The tools and managed services to easily develop applications, IoT and AI solutions
- The scale to manage the data needed to develop and refine solutions, as well as to gather insights from these solutions over time
- The ability to manage edge devices from both an Operational Technology (OT) and Information Technology (IT) perspective
- The flexibility to swap out edge workloads quickly as new use cases arise
- Automated and remote management capabilities — rather than relying on manual, on-prem processes to achieve these goals

The edge:

- Demystifies the implementation of solutions from AI to IoT
- Enables rapid deployment, testing and modification of these solutions
- Reduces latency and improves the value of real-time data
- Increases flexibility, allowing workloads to be shifted quickly with minimal disruption
- Provides a more effective way to process massive amounts of data, enabling key insights to be sent to the cloud

Together, cloud + edge establishes a robust framework for rapidly developing, delivering, managing and modifying your approach to innovation. Rather than requiring a full week to build an on-prem solution, cloud services may be used to prototype a concept overnight. It can then be deployed to the edge for rapid testing, modification and proof of value. The faster your organisation can test and learn, the faster you can transform over time.

But in order to effectively leverage your architecture from core to edge, there are a few things to consider.

1 Tools and services

When designing an architectural strategy that supports innovation, public cloud managed services are key. While the specific offerings will vary by cloud provider, they typically support security and compliance, monitoring and management, solution design, modernisation and more. By offloading the technical burdens associated with managing cloud and edge environments, these services accelerate time to value while lowering your overall cost profile.

There are also many solution-specific cloud platforms which

can be leveraged by internal teams to build and deploy custom AI (Azure AI, Google Cloud AI, Amazon SageMaker, IBM Watson), IoT solutions (Azure IoT Central, Google Cloud IoT, AWS IoT Core, IBM Watson IoT) as well as chatbots, computer vision models and more. These tools provide the foundations to make complex solutions more approachable without the need for custom code.

Cloud providers are also increasingly expanding their offerings to simplify the process of operationalising data at the edge. Frameworks such as Google Anthos, Azure Arc, AWS Outposts and others can be used to manage clusters and the workloads deployed on them.

New tools and services are released regularly, so as part of your architectural strategy, it's important to reevaluate which solutions may be best suited to your environment. Relying on a static approach will result in missed opportunities to reduce operating costs and improve efficiency or scale.

2 Data alignment

Intel's The Edge Outlook report shows that while most businesses understand the edge is integral to unlocking future innovations — 76% say identifying "the ideal" location for data is a challenge.

There's no one right way to determine where data should be managed and stored; the decision ultimately comes down to where a particular workload will be most useful, practical or desirable. But in general, applications or workloads

that benefit from being processed at the edge are those that require low latency, high bandwidth, strict data privacy and/or a short data lifespan. Edge applications also tend to be more "lightweight" and specialised, while solutions that are more broadly focused and more compute intensive tend to be better suited to the cloud.

Industry- or company-specific privacy policies, such as HIPAA or GDPR, will also play a role in determining where your data will live.

3 Managing complexity

As your cloud + edge architecture becomes increasingly distributed, challenges of scale and complexity are bound to arise, particularly if edge deployments are treated as point solutions rather than integrated aspects of your network. To enable operational efficiency, organisations must manage edge and core cloud workloads in a secure, maintainable and scalable way. This requires a consistent operational approach to automate processing and execution as data is sent from the edge to the cloud and back again.

Leveraging a microservice or container-based approach can simplify the process of extending cloud-native services and applications to the edge. A container-based application is scalable and can run in the cloud or on the edge, making it easier to manage. This reduces the cost of managing different frameworks and deployment strategies.

4 Security factors

As with any technology implementation, security must be considered when implementing solutions at the edge. This is a broad topic with many facets to evaluate, but in general you'll want to prioritise:

- The physical security of each edge device
- The framework used for onboarding these devices
- The security of your data pipeline and configuration
- Imaging and securing at the OS level, as well as the solution level
- Out-of-band management and patch management
- Securing data at rest

The good news is that some of these requirements can be managed by your cloud provider. The rest should be kept top of mind as your team moves applications and workloads from proof of concept to production at the edge.

A calculated approach

The ability to "fall quickly" — not *fail* quickly but *fall* quickly — then get up and move on to the next solution is a cornerstone of innovation. A robust cloud + edge strategy enables this approach by circumventing many of the lengthy, manual processes associated with a traditional on-prem or core cloud architecture.

By building on the benefits of each aspect of your infrastructure, your business will ultimately be able to develop a robust approach to data-driven innovation that's greater than the sum of its parts.

Take a deeper dive into innovation at the edge with expert panels, breakouts and a keynote from Forrester Research. Insight *Accelerate* is now on demand.

About the authors

Amol Ajgaonkar
CTO of Intelligent Edge,
Insight

Carmen Taglienti
Principal Cloud & AI Architect,
Insight

The Evolution of Cybersecurit and the Role of the CI

Q&A With Arun DeSouza, CISO and CPO, Nexteer Automotive

The large-scale migration to remote work redefined the threatscape for cybersecurity leaders everywhere. Now, more than a year later, many are still trying to identify and close potential security gaps, while staying one step ahead of cybercriminals. We wanted to know, what role does the Chief Information Security Officer (CISO) play in this constantly evolving, cat-and-mouse game of threat detection and prevention? We sat down with Arun DeSouza, CISO and CPO for Nexteer Automotive, to find out.

y SO

Arun DeSouza,
CISO and CPO,
Nexteer Automotive

What’s your role today? How has it evolved and where do you see it going?

I’m the Chief Information Security and Privacy Officer (CISO & CPO). I pioneered an integrated global InfoSec and Privacy program, developed a long-range strategic roadmap linked to business objectives and built a strong team from the ground up. I’m responsible for the delivery of multiple services, including but not limited to:

- Strategic planning
- Identity and access management
- Incident management
- Privacy management
- Risk management
- Governance and standards
- Security operations
- Training and awareness

The CISO role has evolved significantly in this decade. Depending on the risk appetite and scale of digital transformation in organisations, the CISO role now spans across some or all of the following personas:

Technical ◆

Business aligned ◆

Risk focused ◆

Transformational ◆

When I started my career as a CISO in 2003, I was spending most of my time in persona one. Currently, my role spans personas two through four. The convergence of security, privacy and enterprise risk also offers potential for CISOs to become Chief Risk Officers (CROs) of organisations going forward.

Cybersecurity is top of mind for IT and security professionals today. Why is cybersecurity so challenging right now?

The winds of change are blowing through today’s workplaces. Macro trends such as Industry 4.0 and distributed work require companies to enact and accelerate digital transformation powered by the cloud. Technologies such as Artificial Intelligence (AI), blockchain, edge computing, the Internet of Things (IoT), autonomous vehicles, robotic process automation, etc., are helping to foster innovation and competitive advantage.

The security and privacy risk nexus of the IoT brings a unique set of challenges. Nation-state hacking and supply chain threats are also major factors in the evolution of cyber risk.

Cybersecurity Ventures projected there would be 3.5 million open positions by the end of 2021. Thus, companies are not able to staff up appropriately with the highly skilled resources needed to protect the enterprise. Ultimately, the exponential rise in security threats and the acute shortage of InfoSec resources makes these very challenging times in cybersecurity.

Some IT leaders have argued that IT spending is being wasted on cybersecurity that supports remote work. Yet, the workforce is demanding "anywhere work" flexibility. What are your thoughts on this?

Remote or distributed work is here to stay. There's a paradigm shift underway due to:

- **Flexibility and work-life balance:** Many employees enjoy this feature, especially if their daily commute is significant.
- **Talent acquisition:** Companies can leverage distributed talent and hire the best people. In many instances, this allows both parties to make a win-win arrangement.
- **Executive buy-in:** Companies like Twitter have embraced this trend and are enabling their employees to work remotely indefinitely.

As a CISO, I believe I should help enable the business. Given the above trends, it's now par for the course. Further, the trifecta of identity, Zero Trust and software-defined perimeter power seamless access to "anytime, anywhere, authorised" access to digital applications and services.

Advice for your journey

When we asked DeSouza what he'd recommend for IT professionals who want to progress in their careers, he shared this advice:

- Join industry groups and build your network.
- Leverage social media like LinkedIn.
- Gain a mentor(s) who can advise you.
- Take on tough challenges — don't fear failure.
- Be authentic — find a role that complements your values and personality.
- Commit to lifelong learning (reading, conferences, seminars, etc.).

How do you think security will evolve in response to trends such as anywhere operations and edge computing?

I believe that adoption of Zero Trust will accelerate. Dynamic threat protection will be further propagated by security providers banding together in alliances and tightly integrating their platforms to strengthen Zero Trust. One such example is the Spectra alliance between Okta, Proofpoint, Crowdstrike and Netskope. Another example is the Zero Trust alliance between ZScaler, Cloudflare and SentinelOne. This trend benefits enterprises and providers. I expect that this trend will grow. InfoSec professionals will also band together to share best practices via organisations like the Cloud Security Alliance.

Nexteer Automotive received the 2021 CSO50 Award from IDG. The award recognises security initiatives that demonstrate "outstanding business value and thought leadership." Your project was NEXTINTRUST. Can you tell us about it?

This is the second CSO50 award for Nexteer during my tenure — our first was for identity lifecycle management. Our 2020 award was for the thought leadership and deployment of an IoT security platform in our manufacturing plants. This platform enables:

- Device visibility
- Policy definition
- Behaviour and risk analysis
- Enforcement of policies and standards

As Nexteer embraces digital manufacturing to increase efficiency and optimise operating costs, there's been an explosion of IoT devices on the plant floor. Further, more and more of our home devices are becoming internet connected. The exponential proliferation of IoT devices and immature security practices make them targets for attack.

Key CISO guiding principles for Nexteer's IoT security deployment are as follows:

1. **Characterise** – Identify and classify assets and stratify them by business value and risk.
2. **Demarcate** – Implement network zones with a clear demarcation between IT and OT networks.
3. **Understand** – Visualise and identify threats and vulnerabilities across networks inclusive of devices, traffic, etc.
4. **Unify** – Control access by users and devices across both secure wireless and wired access.
5. **Adapt** – Leverage Zero Trust to enact adaptive control schemes in real time.
6. **Converge** – Develop explicit, third-party access and risk management protocols, including Privileged Remote Access. These are particularly relevant to OT networks to strengthen the security architecture.
7. **Beware** – The following root causes have led to IoT device security issues in the past:
   - Static credentials embedded in the device
   - Lack of encryption
   - No software updates
   - API security gaps

The IoT security platform enables visibility to all devices on the manufacturing network. It allows us to identify device posture in real time, detect embedded threats and drive proactive control strategies. This enables enterprise risk management and strengthens cybersecurity.

IT talent, particularly for cybersecurity, is in high demand and short supply. How is your team designed for success?

My first step was to build a detailed services and competency framework with the skills needed for each role as well as a strategic hiring plan. We periodically review and update this framework. It can also be used for career pathing and succession planning.

Further, I employ the following steps and strategies to manage and develop talent:

- Define an appropriate mix of in-house and outsourced services.
- Conduct cross training across service tiers.

- Utilise managed services.
- Leverage training and development and succession plans.
- Negotiate cost savings to "self-fund" key roles.
- Develop a "grassroots" talent pipeline (students and co-ops).
- Identify talent early and strengthen the pipeline.
- Build affiliations with industry groups and universities to identify interested talent.

I'm also pleased to say that my team is diverse, with 50% men and 50% women. This has also helped drive synergies and creativity.

What's been the most profound executive decision you've made as a CISO?

Early in my CISO career, I was on the cusp of enacting a global network and security transformation. I worked hard to build a strong business case and payback to illustrate the value. However, times were tough, so my budget was reduced, and I was still asked to lead and complete the transformation.

I embraced what I now call "the power of federation." I reached out to all the key partners for help and found win-win strategies. I obtained significant discounts for professional services. For software, I consolidated contracts in the U.S., since our budget was euro-based, allowing us to benefit from the exchange rate. Ultimately, we finished the project under budget.

We saved significantly on operating costs, strengthened enterprise security, enhanced network quality of service and consolidated servers. The project inspired multiple case studies and resulted in a Network World All Star award.

Essentially, the most profound executive decision I made was to ask for help and not quit. I learned early on that building strategic, trusted partnerships and strong business relationships can be a great asset to all parties.

Key takeaways

Follow these guiding principles:

- Embrace change fearlessly.
- Build and maintain trusted partnerships.
- Manage priorities effectively.
- Foster a culture of respect and trust.
- Leverage communication and relationship management.
- Differentiate requirements from "desirements" in projects.
- Manage stakeholder expectations.

These ingredients are key to success:

- Collaboration and communication
- Envisioning and storytelling
- Program management
- Negotiation and vendor management
- Strategic cost optimisation

Microsoft Partner

2021 Partner of the Year Winner
Migration to Azure Award
Solution Assessment Award

Azure Advanced Specialisation Spotlight

As the 2021 Microsoft Worldwide Partner of the Year for Azure Migration and Solution Assessments, Insight is the leader in helping clients achieve a cohesive, single source of truth for data.

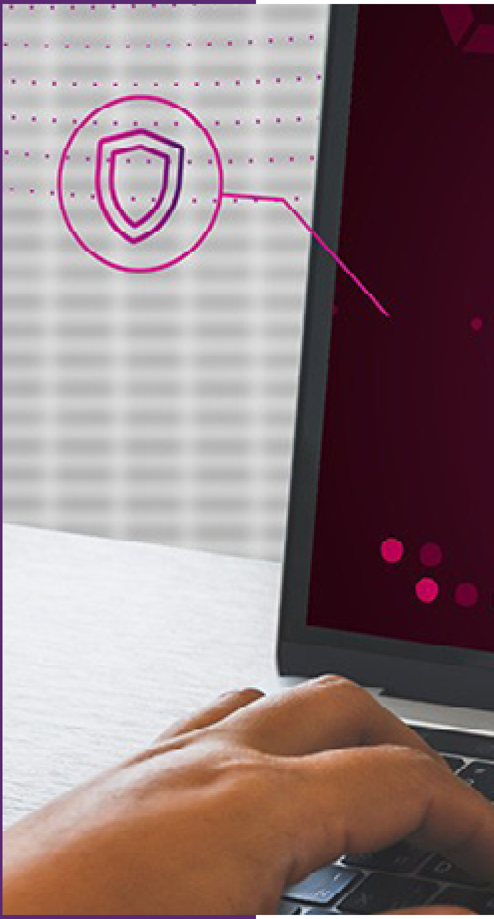
We have the expertise to help clients discover, assess, modernise, support, and optimise their data estates, and drive operational efficiencies and deliver profitability back to the business.

Advanced Specialisations = Expert Partnership

Insight's capabilities are demonstrated by our certification in 10 Advanced Specialisations across Microsoft Azure, Modern Work and Security.

TAFE NSW recently leveraged Insight's Solution Assessments' capabilities to respond to evolving industry needs, government regulations and the need to prepare business for the future.

Navigate the Journey to Passwordless Authentication



> Complexity is the arch enemy of security but creating modern authentication needn't be a headache.

Bill Gates famously predicted the death of the password back in 2004 saying **traditional password-based security** couldn't meet the challenge of keeping critical information secure.

Seventeen years down the track and in the midst of a pandemic which has seen both remote work and cyberattacks explode, many are still on that journey.

The way we authenticate is outdated and vulnerable and there are plenty of reasons why we need to move to more modern authentication methodology:

Hackers love passwords and passwords are under attack. Research from Verizon shows 81% of security breaches are down to weak or default passwords.

Users hate passwords. Alpha numeric passwords are hard to remember, and we've got too many of them. There's no surprise passwords are frequently reused. Microsoft says up to **73% of passwords** are duplicates and a Google study found 13% of people reuse the same password across all accounts.

IT also hates passwords because of the big administrative overhead. Gartner says between 20% to 50% of all help desk calls are for password resets.

Secure, yet functional

I have a catch cry: Complexity is the arch enemy of security. As security professionals we have to balance security

and functionality. We can make systems extremely secure, but make them too complex and users will find a way to circumvent them.

A boardroom with a 16-digit pin and fingerprint scanner on the door is very secure, but it's not very functional and someone is going to just take a chair and jam that door open.

Microsoft is on a mission to get everyone to **move passwordless** to address the issue of secure, yet functional, authentication, and that mission continues with Windows 11.

They've received some criticism about the seemingly high hardware requirements, however, when viewed in the context of a passwordless future, those requirements make sense. It's all to do with the Trusted Platform Module (TPM) chip – essentially a mini safe on your computer where all your biometric information can be safely stored.

The TPM chip locks the data away. Then when a user logs on it authenticates them using the scanned data on the TPM chip and sends a private key to the cloud, which holds the corresponding public key. It's not sending your biometrics to the cloud. It's not sending a password to the cloud. It's simply sending a certificate that says you are who you say you are.

Next comes multi factor authentication (MFA). Now when you log into the cloud you get a message on your phone authenticating that it really is you logging into the cloud. According to Microsoft, implementing MFA mitigates 99% of common password attacks.

But your password *is* still shared and a shared secret is never good. An SMS to the phone is also not that secure, as it is delivered in clear text and leaves you vulnerable to interception.

If we want to go to a high-security environment, there are three key options that provide choice with standards-based passwordless authentication:

Windows Hello, introduced in 2016 this enables you to sign in securely by showing your face or pressing your finger.

The Microsoft Authenticator app is a step up from a text message and relies on your phone authenticating you. It requires that you register in Microsoft's cloud which gives us MFA push notifications.

Then there's FIDO, a standards-based passwordless authentication which comes in the form of a USB key, toggle or token of some kind.

About the author

Roland Leggat
Modern Workplace Specialist,
Insight APAC

5 steps to make your cloud secure

1 Enable Azure AD

2 Allow MFA and self-service password reset

3 Identify and update applications to allow Azure AD authentication. This enables passwordless authentication for an unlimited number of apps through native functionality in Windows Hello, the phone-as-a-token capabilities of Microsoft Authenticator or FIDO keys, so users won't have to enter multiple passwords.

4 Plan for hardware and devices. Devices will need a TPM chip if you want to use facial recognition. If you don't have them already, are you going to buy new hardware? Little things like this are going to be technology blockers on your journey to passwordless success, so prepare in advance for them

5 Start with a pilot of Windows Hello, Microsoft Authenticator or Fido, assess and plan from there.

Complexity is the arch enemy of security

Yet **78% of organisations use more than 50 cybersecurity products** to protect their environment[1]

4 ways Microsoft 365 E5 protects users, data, apps, and devices

1 Advanced threat protection

Think of threat protection as the security around the front door of your organisation, like CCTV. For the proactive prevention of breaches, Microsoft 365 E5 monitors identities, endpoints, user data and documents, cloud apps and infrastructure.

3 Information protection

Locate and classify information anywhere it lives or travels, with information protection taking place at the file level.

2 Identity and access management (IAM)

With person-based security incidents increasing in frequency and severity,[2] IAM is the cornerstone of any security platform.

4 Security management

Microsoft 365 E5 integrates your productivity and security tools for simpler management.

[1] CIO, 2020, *Cybersecurity threats are exploding exponentially; how IAM can assist*; [2] KPMG, 2021, *The Changing Shape of Ransomware*

Secure your business today

To find out more or get started with Microsoft 365 E5, get in touch with an Insight security specialist on 1800 671 118.

Insight

6 Computer Vision Trends Transforming the Business Landscape

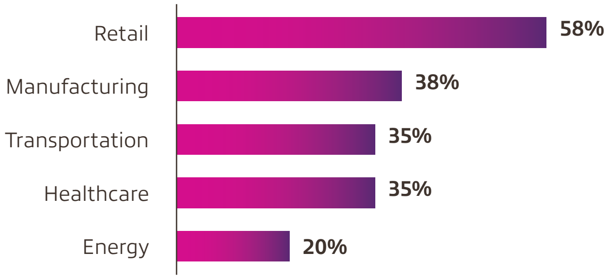
New data from Insight and IDG reveals how the success of early adopters is driving new perspectives, investments and applications of computer vision across industries.

1 Adoption is accelerating.

86% of businesses expect investments in AI to increase over the next 12 months.

While just **10%** of organisations are using computer vision today, **81%** report they're currently **investigating or actively implementing the technology**.

Plans to implement computer vision by industry:



2 The value of visibility is clear.

96% of respondents agree computer vision can help their organisation **grow revenue**.

97% agree computer vision can help their organisation **save time and money**.

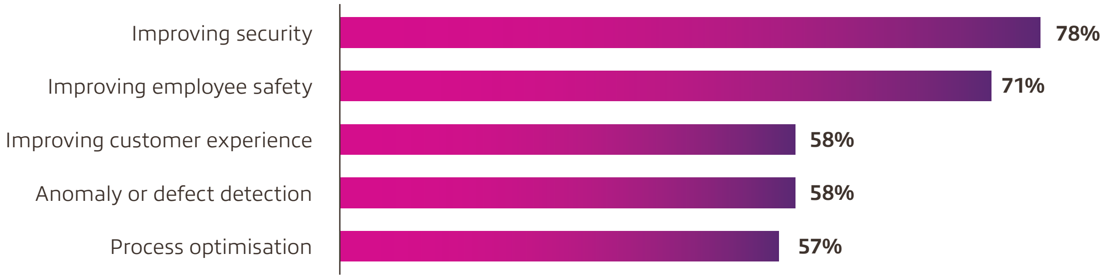
Among those investigating, planning to implement or actively using computer vision:

45% see opportunities for **cost cutting** and **efficiency gains**.

45% cite the technology as a **driver for innovation**.

3 Common drivers include safety and security.

Specific applications for computer vision vary by industry, but across the board, **the most common use cases include**:



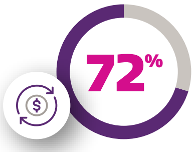
Computer vision:
The use of machine learning to recognise and respond to input from cameras or video

This emerging technology ranks among the fastest growing applications of Artificial Intelligence (AI) today — and early adopters already report significant benefits.

To help businesses navigate this rapidly evolving landscape, Insight commissioned a MarketPulse Research survey from IDG, uncovering key computer vision trends across energy, manufacturing, transportation, retail and healthcare industries.

4 Seeing is believing.

As organisations investigate the value and feasibility of implementing computer vision, time-to-ROI is a key consideration.

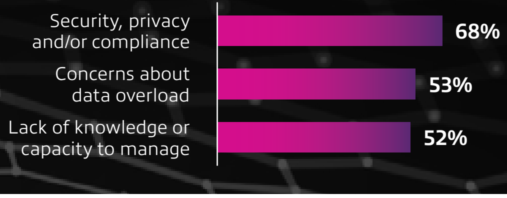


of businesses expect to see a Return on Investment (ROI) within two to three years. But those that have put computer vision into production are more likely to expect **ROI within just one year.**

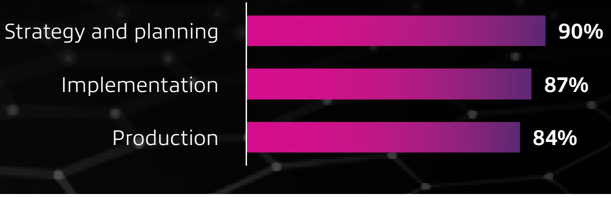
Early adopters are also the most likely to strongly agree that computer vision has the potential to grow revenue.

5 Expertise is essential.

As with any new technology, there are bound to be challenges or concerns inhibiting early investment. Across industries, **organisations reported common obstacles**:



To overcome these challenges, the majority of organisations report a high likelihood to **seek support from external consultants** or system integrators.



6 Early adopters gain an early advantage.

While just 10% of organisations have positioned themselves at the forefront of this trend, there's ample opportunity for other early adopters to capitalise on the benefits of computer vision.

As more organisations shift from investigating to investing in this technology, those that get ahead of the curve and put the technology into motion will capture ROI and gain a competitive edge.

For deeper industry analysis and a breakdown of the survey results, access the full report: **Early Adopters See Value in Computer Vision.**

IDG

SPONSORED BY: Adobe

How Digital Docum

Processes & E-sign

Are Driving Business Resilience in a Time of Econo

In the spring of 2020, when COVID-19 transformed the global business landscape virtually overnight, companies in every industry had to pivot to adapt and survive. Many transitioned their employees to remote work, and then had to quickly establish new ways of getting things done. Sales of collaboration and productivity technologies like digital document and e-signature software rose as companies made every effort to keep business moving forward.

At Adobe, we wanted to understand exactly how companies were using these solutions to manage day-to-day processes, connect employees across distances, continue providing exceptional customer and employee experiences, and ultimately facilitate business recovery in a challenging economic climate. We commissioned Forrester Consulting to dig into the details, find answers and discover insights.

ent

atures

mic Upheaval

Digital document processes — a shift from best practice to business necessity

Between May and June of 2020, Forrester surveyed senior IT and business decision-makers in North America, Western Europe and Asia Pacific. Survey responses showed that, as remote work grew, it became even more important that employees and customers were able to securely share, review, sign and store digital documents — without the need for hard copies.

Survey participants reported that their organisations were relying on digital document processes to help them serve their customers, reduce business risk and more. Here are just a few of the findings:

72% of respondents agreed that digital document processes support business continuity amidst unforeseen circumstances.

47% said their digital document solutions were enabling them to pursue opportunities and gain new customers during the economic crisis.

54% predicted that the benefits of increased employee collaboration will last beyond the pandemic, and 47% said the same about increased customer satisfaction.

Driving efficiencies with e-signature solutions

The Forrester study also revealed that e-signatures are becoming essential to business evolution. This seems to be because, as in-person interactions decline, both customers and employees expect to be able to sign documents digitally.

In the study, 58% of respondents said the pandemic had caused their organisation to accelerate the adoption of e-signature capabilities. In addition:

60% of companies reported that e-signatures support business resilience.

72% of respondents said they consider e-signatures critical to business continuity.

66% of customers said they request digital solutions like e-signatures.

Saving time & money by integrating e-signatures into business workflows

Even before the pandemic, businesses were realising productivity gains and cost savings by integrating e-signatures into their everyday digital document workflows. Take the case of Adobe Sign.

Microsoft's preferred e-signature solution, Adobe Sign is deeply integrated across so businesses around the world can create documents, send them for signature and manage workflows right from apps like Word, Outlook, PowerPoint, Teams, SharePoint, Dynamics365 and Power Automate.

In an Adobe-commissioned study conducted in 2019, Forrester interviewed customers who use both Microsoft 365 and Adobe Document Cloud. The study showed that using Microsoft 365 with Adobe Sign and Acrobat DC has the potential combined benefits of $9.1 million over three years. Findings included the following:

- **28x faster cycle times:** For documents requiring signatures, using Adobe Sign from within the Microsoft applications employees use every day replaces inefficient, error-prone manual document signing processes.
- **65 hours saved:** Employees saved 65 hours per year using Acrobat DC with Microsoft 365 apps by digitising paper-based tasks, reducing rework through converting and editing PDFs, and leveraging mobile capabilities to continue workstreams outside the office.
- **1.5 hours saved:** Sales reps saved time with each transaction using Adobe Sign from within Microsoft Dynamics, leading to faster sales cycles.
- **$6 saved on average:** Companies saved money per document transaction with Adobe Sign.

Ensuring security and compliance

While time and cost savings are critical, digital document and e-signature solutions also need to be secure and compliant, and they should easily scale as businesses grow. That's why, for 25+ years, Adobe has been the trusted leader in digital documents.

Adobe Document Cloud is a complete solution that helps companies transform paper-based workflows into digital experiences, removing friction from business processes. And it includes Adobe Sign, which supports the strictest e-signature regulations while complying with legal, industry and regulatory requirements around the world.

Looking beyond the current moment to long-term benefits

As the pandemic has shown how critical it is for companies to be able to conduct business remotely, digital document and e-signature solutions are proving to be sound investments that address both immediate and long-term needs. They drive resilience during difficult times and help businesses establish new ways of working that can boost productivity — giving employees more time to focus on the innovations that will ensure future success.

About the author

Rob Elliot
Adobe Business Manager, Insight

Discover how to keep business moving with e-Signature workflows.

Mounting a Ransomwar Defense for the Big Picture

When it comes to ransomware defense, protective controls have always been critical — but more security pros are saying goodbye to a siloed approach.

e

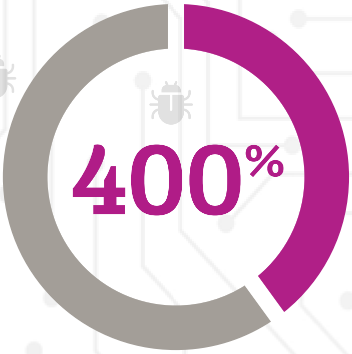
As we've stressed in this Fall issue of the Tech Journal, a siloed approach to defending your business from cybercrime just won't cut it anymore. A ransomware use case is no exception. These days, organisations need a more robust approach to mounting a defense against the incredibly real — and costly — threat of ransomware.

In August of 2020, just five months after the onset of COVID-19, hackers were waging

4,000

successful ransomware attacks per day on unsuspecting business.

It was a 400% increase from pre-COVID-19 numbers, according to the FBI.



Today, the attacks persist and tend to surge even more around the holidays.

In fact, CBS News reported that up to 1,500 businesses in the U.S. and other parts of the world were impacted by a ransomware attack over the 2021 Fourth of July weekend.

The lure of ransomware

Why has ransomware become such a mainstay for hackers? Why have organised crime rings and even nation states joined with bad actors, magnifying the threat — and reach — of these types of attacks? It's because the financial payoff for ransomware in particular has become significant, so more hackers are investing in those tactics. Anytime the juice is worth the squeeze, you're going to have more people doing it.

Extortion-style attacks, where data wasn't encrypted but the victim was still held to ransom, have more than doubled since 2020.

The 4 basic ransomware types:

1. **Application-level lockers** prevent users from accessing applications or operating systems until a ransom has been paid.
2. **System-level lockers** overwrite a system's Master Boot Record (MBR) with its own microkernel, preventing any type of use until a ransom has been paid.
3. **File encryptors** encrypt user files and data, demanding a ransom for the release of the decryption key.
4. **Fake ransomware** is malware that claims to have encrypted a user's data but actually hasn't; ransomware language is used to collect a panic-induced payment from the victim.

So how is your organisation supposed to mount any kind of effective defense against these types of attacks? As with any cybersecurity use case, creating a multilayered defense will best protect your environment and assets from ransomware.

A multilayered defense includes:

- Prevention of malware
- Detection of bad actors
- Recovery and continuity

It's time to go beyond protective controls.

A layered approach to preventing ransomware is not all that different than the approach that we take with malware. Yes, it means keeping the bad guys out by deploying effective endpoint security and teaching users not to click on malicious links or unknown documents. It also means improving threat intelligence, particularly around command and control. The protective, or preventive, side of ransomware defense is straight forward — limiting the vectors that the ransomware actor has to inject into an environment.

But when it comes to ransomware, it's not enough to just keep bad actors out. We must also focus on the recovery and continuity aspects of security. To do this, organisations need to ask themselves key questions like:

What is my storage environment doing to help me recover?

How can my data protection help me recover?

How quickly can I restore entire environments in the event of an attack?

How do I effectively secure these environments?

How do we get back up and running in a way that avoids putting our last resort data back into a compromised environment?

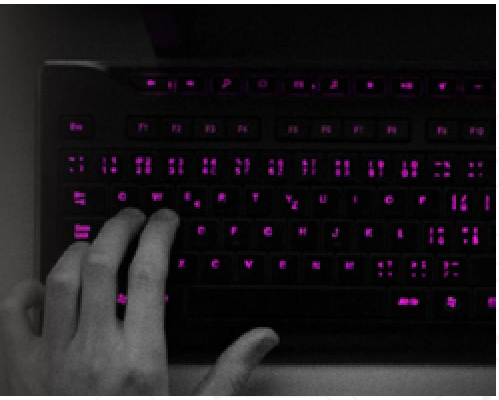
According to Sophos' State of Ransomware 2021 survey, the number of organisations that paid a ransom increased from 26% in 2020 to 32% in 2021 — but fewer than one in 10 (8%) managed to get back all of their data. As lose-lose situations like these become more commonplace, having the nuclear option has become increasingly helpful to security teams.

Options like immutable storage and backup are becoming popular, despite them being last-resort solutions.

As we move from the traditional data centre model to centres of data and see more edge computing involving artificial intelligence. These areas, along with remote workstations, need to be protected with the same type of multilayered approach.

> In the 90s, when there was a security issue, the IT pro might have said ‘Let me buy this tool to fix it.’ But that’s not the case anymore.

Three mantras to live by



As you pursue excellence across your ransomware defense strategy, remember:

1. **There’s no silver bullet.** We all wish it were true, but there’s no one holy grail product that will stop ransomware in its tracks. A tool may be a very important piece of a strategy and response plan, but there’s no point solution that covers it all.

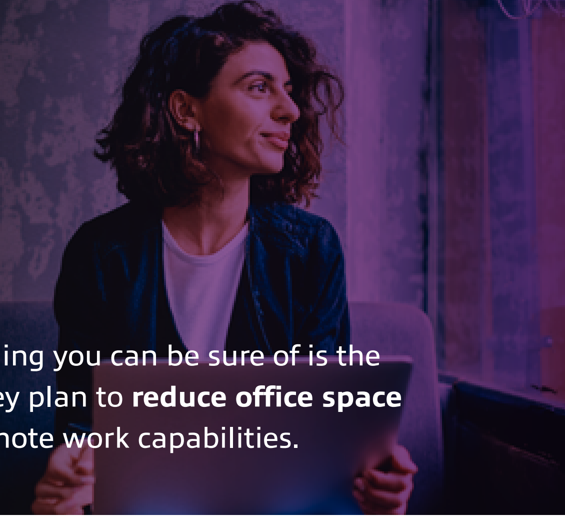
2. **End-user training will always be vital.** You can have all the sophisticated tools in the world, but the end user will always be the weakest link. Make training a priority. Make it fun. Do whatever you need to do to keep end users invested in your security policies.

3. **There’s no start and stop.** The most successful teams look at ransomware defense through a business continuity lens. Test your methodology, and test it often — whether it’s annually, bi-annually or however often your business deems it appropriate. Every 10–11 seconds, an organisation will fall victim to a ransomware attack according to research compiled by PurpleSec. That’s simply too often for a “set it and forget it” strategy.

Always be evolving. Explore more ways to ensure a strong defense — from assessing readiness to strategising across key focus areas.

About the author

Chris Kapusta
Senior Manager for
Cloud + Data Centre
Transformation, Insight



Enable Anywhere Work with VMware

While the world moves into a post-pandemic era, one thing you can be sure of is the persistence of remote work. Surveyed Executives say they plan to **reduce office space by 30%**. IT Leaders around the globe are prioritising remote work capabilities.

Modern Solutions for Traditional Challenges of Anywhere Work

Legacy systems

On-premise systems often lack visibility to remote endpoints.

95% of security breaches originate with endpoints

Modern endpoint management – Provides line-of-sight into all your endpoints, whether they're on-premises or off

Too many vendors

47% of enterprises manage more than 10 vendor relationships.

17% say it's easy to manage their multi-vendor relationships

Carbon Black Delivers all the security tools you need through a single solution, providing full visibility across your infrastructure. Carbon Black will keep you covered with features such as: next-gen antivirus, Endpoint Detection and Response (EDR), Managed detection, Auditing and Remediation.

Frustrating end-user experience

It's hard to adequately support and enable remote workers.

76% of employees complain of lacking access to essential apps

Device provisioning allows for faster deployment, less downtime and simpler device management

What's the VMware advantage?

A harmonious IT environment that enables and secures all users, endpoints and networks – anywhere your users want to work.

- Broader security coverage
- Reduce operational overhead
- Improve resiliency & flexibility
- Create seamless remote experience
- Streamline tools and processes

Your building blocks to a modern workplace:

Horizon Unified desktop and application delivery

Workspace Unified Endpoint Management (UEM)

Carbon Black Intrinsic security

Sources

AV Comparatives. Business Security Test 2020 (March — June).
Forrester Consulting. (May 2020).
Tension Between IT and Security Professionals Reinforcing Silos and Security Strain.
Gralla, P. (May 2021). Office 365: A Guide to the Updates. ComputerWorld.
Insight. (Summer 2020). IT Vendor Consolidation: An Essential Initiative for Today's Businesses. Tech Journal.
Momentum Cyber. Cybersecurity Almanac 2021.
VMware. VMware's Move to a Digital Workspace.
VMware internal research.

Visit au.insight.com or contact your Insight Account Manager for more information.

Insight vmware®

3 Key Challenges Facing Business Optimisation

And How a Technology Partner Can Help

Leveraging trending technology can optimise your business costs and operations — but how do you navigate the constant evolution? With the right tools and technology partner, you'll help your business reach its full potential.

The impact of COVID-19 across industries has driven business optimisation at an unprecedented pace. Virtually overnight, companies were forced to design and execute highly complex projects, including remote work, infrastructure adaptations, digital modernisation and additional security layers to support rapid change. To ensure resilience, organisations have been tasked with overcoming these challenges and more, all while growing and supporting the company.

As pandemic restrictions change, many businesses are permanently transitioning to a hybrid workforce environment: a mix of on-site and remote employees, modern digital experiences, and on-demand access to software and solutions. With this shift, optimisation across the new IT landscape becomes incredibly important. IT departments worked tirelessly to implement urgent transformations in 2020; we'll need to reexamine where those systems stand today, as well as areas for enhancement.

Navigating a post-pandemic world will come with its share of additional challenges, and strategic optimisation can reframe the future of business.

There's a new ask of IT:

Be the innovators. Technology teams are expected to function as a profit centre, rather than a cost centre. So, how do you optimise costs and increase output? It's all about the right technology.

But let's take a step back: What exactly is business optimisation, and how does it apply to you? At Insight, we look at optimisation as the process of improving the efficiency, productivity and performance of an organisation. This can apply both to internal operations and external products.

Big data and connective technology can be used to influence new approaches that drive business optimisation — allowing organisations to achieve more.

Optimising your business may look like:

- Reducing costs with improved productivity
- Enhancing cybersecurity with modern tools
- Utilising advanced software to streamline operations
- Applying new onboarding systems for hybrid workers

At the heart of each optimisation lies one crucial benefit: speed. By improving the pace at which you accomplish goals, you'll save valuable time — and the old saying holds true: Time is money.

At Insight, we offer testing, assessment and auditing services for your current cybersecurity.

Whether you're looking to satisfy compliance requirements or need a long-term remediation roadmap, we can help. Our technicians leverage more than a decade of experience and two dozen testing tools to pinpoint vulnerabilities and security weaknesses.

By leveraging trending technology, you'll optimise costs, achieve your goals and thrive in an evolving digital world.

Let's explore three key challenges in today's technology that are apt for optimisation.

1. Heightened cybersecurity

When it comes to key risks facing businesses today, it's impossible to overemphasise the importance of security. The rapid transition to remote and hybrid work brought about an urgent need for heightened cyber defense. In today's world, becoming a victim of a cyberattack is a matter of when, not if.

A cyberattack can bring down your entire IT system, resulting in extreme financial loss, damaged reputation and countless additional fallout. Having the most up-to-date cybersecurity in place is vital to detect, stop and respond to attacks in real time.

Particular concern in today's hybrid world surrounds Artificial Intelligence (AI).

The rise of AI in cybersecurity is rapidly evolving, and hackers are utilising its tools and reliance on the cloud for advanced cyberattacks.

You'll want to employ solutions that protect every part of your IT environment, including:

Endpoint security: Keep your devices safe from cyberthreats and malware — wherever you use them.

Email security: Unlock tools such as firewalls, encryption and filtering to make it difficult for hackers to gain entry to your internal systems.

Application security: Minimise the risk of threats, breaches and code hijacking.

Identity and access management: Enforce appropriate access to critical systems for your workforce and customers.

2. Innovative devices and lifecycle management

Devices are essential to business operations, with billions in use today. Maintaining high workforce productivity (and improved profits) requires the right tools at the right times, and having modern, fast devices will increase employee satisfaction and retention. However, managing the device lifecycle can consume the bulk of your budget. In fact, PCs continue to make up the largest capital component in the annual IT budget for many enterprises.

So, how can you find and utilise the right tools without breaking the bank? A technology partner can eliminate the time and hassle of managing multiple hardware vendors, ensure maximum uptime and lifespan, improve user experience and reduce device total cost ownership. We'll talk more about the benefits of choosing the right partner below, but first, let's look at software optimisation.

3. Software and process automation

In today's constantly evolving digital space, having the right software to support your work is crucial to success. This is especially important if new employees are joining your organisation from a fully remote setting. With devices that are ready to go and equipped with the right software, your team will onboard with ease, and you'll save time (and resources) from the start.

The right tools can also automate repetitive processes, eliminate redundancies and free team members to focus on important tasks. With today's optimisations, you'll see improvements in:

Productivity: Business applications can streamline your operations and improve efficiency, collaboration and performance.

Creativity: Your team can produce unparalleled work with feature-rich platforms for designing, editing, drafting and more.

Networking: Powerful networking applications keep your users and devices connected across your business.

Operating systems: With an efficient, robust operating system, you can seamlessly manage hardware and software resources.

Applying advanced technology tools in these areas can lead to pivotal optimisation for your business, but staying up to date with trending tech can be a job in and of itself. New technology is increasingly complex, and we're dealing with an expanded surface area — more devices, a dispersed workforce and accelerated cloud migration. That's where a technology partner comes in.

Choosing the right technology partner

We've covered how utilising technology can optimise your business cost processes and more — but what if you could take it one step further and optimise the entire process?

When finding the right technology for your business, you might spend valuable time juggling vendors for the right product, only to be left with no issue support, maintenance, licensing assistance and overall partnership. Procuring software, for example, can come with a host of challenges: unused products, auditing issues, duplicated technologies, wasted resources and more.

A full-service technology partner, like Insight, will subvert these challenges and bring you improved efficiency, effectiveness, compliance and strategic alignment. When you're looking for the right partner, you'll want to ask a few key questions:

- Do they have an extensive breadth of capabilities?
- Do they offer end-to-end solutions?
- Do they provide a seamless marriage of products and solutions?
- Are they adept in modern services and devices that support digital transformation?

The ideal technology partner will not only help you find the right technology, but will also provide unmatched benefits before, after and along the way. Through Insight, you'll find optimised software costs, better forecasting for future needs, consistent compliancy and greater asset visibility. Our powerful tools and deep partnerships become your crucial advantage.

With advanced technology — and the right partner — optimisation is within reach. **Get started with Insight**.

About the author

Bob Bogle

Regional Vice President & GM Corporate Technology Sales, Insight

CASE STUDY

The University of Sydney Deploys Cloud-Based Courses in One Week

Insight and Citrix quickly creates an online learning environment.

By teaming with Insight and Citrix, The University of Sydney quickly created an online learning environment for students who were unable to return to campus locations to study.

Enabling students to learn safely

We’ve all heard someone utter the phrase, “It turned my world upside down”. Almost never do we hear someone say that, in just seven days, an innovative IT team designed, procured, implemented, tested and rolled-out an enterprise global solution that set things right again. However, the IT team at The University of Sydney did exactly that in providing remote students with rapid-fire education alternatives.

“During a time of rapid change and uncertainty in Higher Education, Insight is proud to be able to support The University of Sydney in the rapid procurement and deployment of a leading edge solution to a very modern problem,” explains Alex Nikolaidis, Account Manager, Education NSW & ACT at Insight.“It speaks to the depth and trust that exist between The University of Sydney and Insight that this was able to be achieved so quickly”

Connecting students and staff across the globe

The University of Sydney is committed to delivering a great student experience. A longstanding relationship with Insight as the IT partner of choice, and strategic partner with Citrix, the university's IT team deployed an entire digital environment that enabled remote access to coursework, apps and data. Technologists on the ground in China then tested the system to ensure its viability. "The great thing about the Citrix platform is that we built it directly in the cloud," explains Jordan Catling, Associate Director of Client Technology at The University of Sydney. "Our implementation took seven days and is entirely scalable."

The idea was to address the immediate challenge first: to build capabilities for students, followed by providing tools for staff and faculty. The team's goal was to provide a range of agile tools, while avoiding being prescriptive as to how those tools should be used. This would ultimately enable greater innovation. "We wanted to provide a secure, high-quality student experience by supporting the diverse ways in which different individuals consume information," Jordan says.

The team has provided more than 100 course-specific applications and SaaS apps that students can access regardless of the type of device or location. The student experience is as good as – and sometimes better than – what a student would have when using locally installed apps on a physical computer.

> *"During a time of rapid change and uncertainty in Higher Education, Insight is proud to be able to support The University of Sydney in the rapid procurement and deployment of a leading edge solution to a very modern problem."*
>
> **Alex Nikolaidis**
> Account Manager, Education NSW & ACT
> Insight Enterprises Australia

Industry
Education

Location
Australia

- Insight Enterprises Australia leveraged strategic partnership with Citrix to provide a solution for an online learning environment, designed, implemented, tested and deployed within 7 days.
- Citrix solution makes it easier than ever before to onboard students and faculty.
- Enables students to work from anywhere, on any device, at any time and provides remote PC access.
- Computers can be configured from a single image in minutes, enabling virtual access to software.
- Data security is enhanced by keeping data only in the data centre while embedded security means access is strongly controlled and user context is governed by policies set by the IT team.

> *"With a focus on multidisciplinary research and teaching, The University of Sydney wanted to provide our staff and students with a broad set of tools that enable disciplinary depth as well as breadth. "*
>
> **Jordan Catling**
> Associate Director of Client Technology,
> The University of Sydney

Insight and Citrix empowers students in virtual labs and classrooms

Many of the statistical, scientific or technical apps that The University of Sydney students use put high computational demands on physical computers. Virtualisation with Citrix allows the university to run these intensive apps in the cloud. "A physical computer might take up to two minutes to load one of our statistical programs," Jordan clarifies. "Running it on the Citrix Cloud management platform, we can see responsiveness in 20 seconds."

The university has now enabled student access to virtual labs, and, thanks to Insight and Citrix in combination with other tools such as Zoom, students can attend virtual classes.

The Citrix-based Virtual Research Desktop is a great example of a virtual lab that delivers high-powered resources so researchers can perform their work more easily. The Faculty of Medicine and Health provides students with healthcare-related tools regardless of the teaching hospitals in which they operate. Not only can students now access information easily in the hospitals, they can also rely on Citrix to complete coursework as they are in transit to and from various medical facilities.

Citrix content collaboration capabilities allow students and staff to securely share data. In the past, transmitting massive volumes of data slowed down the system and took up valuable space on servers. Citrix solved that problem.

Not only is The University of Sydney now enabling students to work from anywhere, on any device, at any time, it is also providing remote PC access. This is something that some staff find particularly appealing. Users are able to connect to their physical desktop computers via a Citrix Virtual agent – without actually needing to be on site.

> ***"A physical computer might take up to two minutes to load one of our statistical programs. Running it on the Citrix Cloud management platform, we can see responsiveness in 20 seconds."***
>
> **Jordan Catling**
> Associate Director of Client Technology, The University of Sydney

Closed borders create barriers and innovation

As the Covid-19 pandemic hit Australia and the rest of the world many students from The University of Sydney were unable to return to campus to continue their studies due to closed international borders and "stay at home" orders.

The University of Sydney worked closely with their IT partner of choice - Insight Enterprises Australia, to help provide a solution for an online learning environment, designed, implemented, tested and deployed within 7 days! Leveraging strategic partnerships Insight engaged Citrix to develop the solution.

Insight and Citrix, a strategic partnership

Monitoring performance to ensure a consistently great experience

The Citrix solution also helps IT gauge the consistency of the online staff and student experience. Using Citrix Analytics, IT can monitor performance in remote locations to determine if latency is an issue and adjust to make the user experience even better.

The university's IT team implemented an underlying foundation of Citrix networking technology to ensure performance is consistently high. This is achieved by prioritising and routing network traffic based on geography. The Citrix network capitalises on the nearest available resources.

Forward-thinking goals

The University of Sydney's IT team had several goals in mind that could serve the university now and in the future.

- Providing a set of highly responsive, flexible, robust, and scalable tools that are natural to use.
- Provide the user base with tools that encourage innovation, without being prescriptive in their use.
- Establishing and maintaining business partnerships that enable the exchange of innovative ideas.

Global Partnerships and Local Partners

"No matter the size of the company, successfully managing work mobility securely is a crucial component to productivity in today's technology-driven world. The deep connection we share with Citrix to deliver complete workspace solutions results in reduced operational costs for IT and a high-quality end-user experience for our clients,"

Bob Kane
Senior vice president of productt marketing, Insight Enterprises

"The great thing about platforms like Citrix is that they are feature-rich, flexible and scalable, so we can embrace leading-edge ways of educating students and researching complex global problems"

Jordan Catling
Associate Director of Client Technology, The University of Sydney

Trending Tech

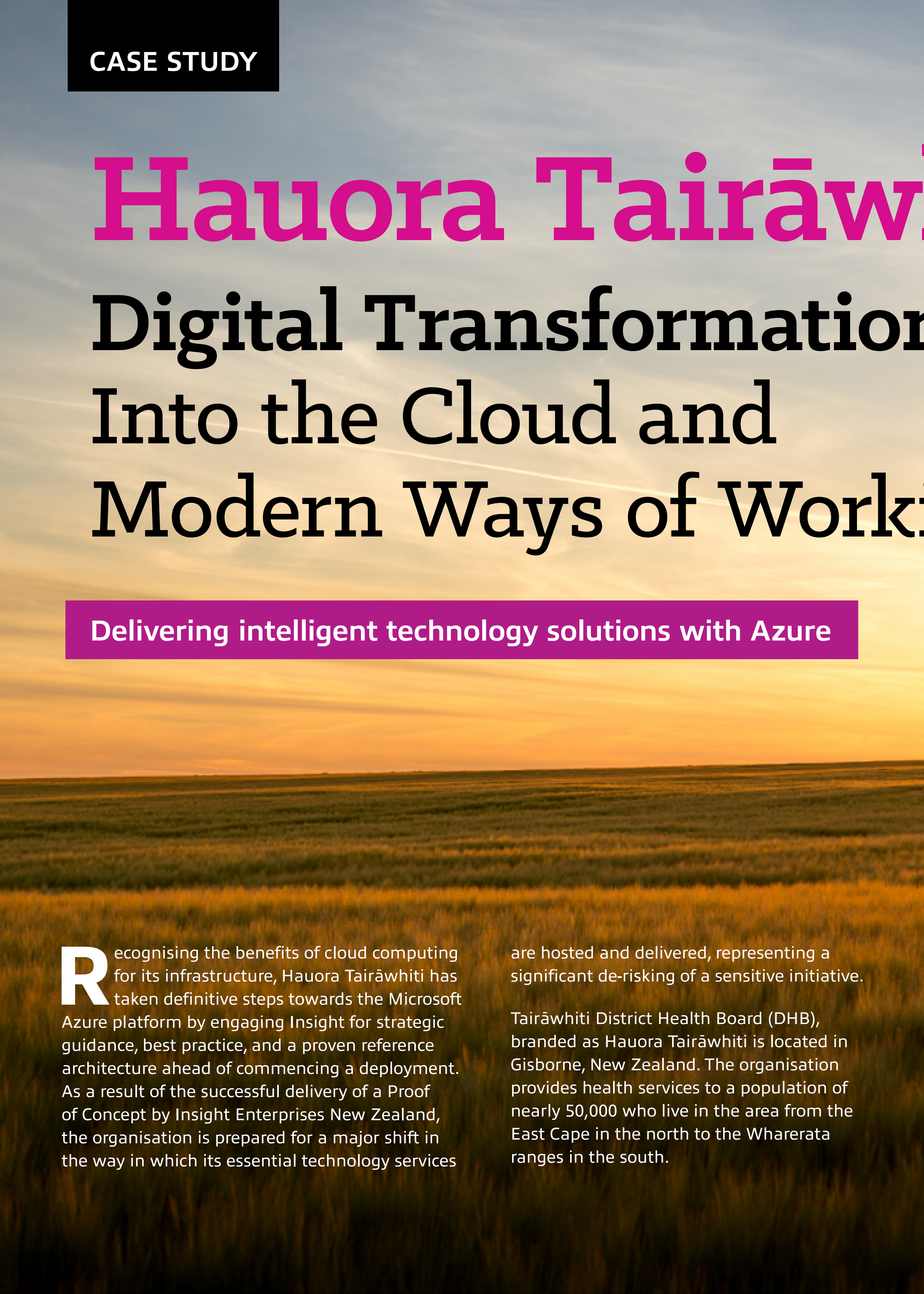
Drive business success with devices designed to boost productivity and security.

Surface Duo

Unlike other devices, the Surface Duo optimises both Google Play and Microsoft Office 365® applications that are best for dual-screen use. Need more visibility? Simply span apps across both screens or view them side by side.

With cloud-based management and enterprise-level chip to cloud security, the Surface Duo is perfect for handling and protecting your business's devices, identities and data. The Surface Duo has protection built in at every layer with integrated firmware, hardware and software so you're always protected.

Learn more HERE



Hauora Tairāw

Digital Transformatio Into the Cloud and Modern Ways of Worki

Delivering intelligent technology solutions with Azure

Recognising the benefits of cloud computing for its infrastructure, Hauora Tairāwhiti has taken definitive steps towards the Microsoft Azure platform by engaging Insight for strategic guidance, best practice, and a proven reference architecture ahead of commencing a deployment. As a result of the successful delivery of a Proof of Concept by Insight Enterprises New Zealand, the organisation is prepared for a major shift in the way in which its essential technology services are hosted and delivered, representing a significant de-risking of a sensitive initiative.

Tairāwhiti District Health Board (DHB), branded as Hauora Tairāwhiti is located in Gisborne, New Zealand. The organisation provides health services to a population of nearly 50,000 who live in the area from the East Cape in the north to the Wharerata ranges in the south.

hiti’s
n Journey

ing

> *“These benefits apply to Azure for our infrastructure services. We can easily meet the challenge of making applications available for an increasingly mobile workforce, and Azure is a preferred platform owing to pre-existing Government arrangements with Microsoft,”*
>
> **Natacha Blattes**
> Project Manager, Hauora Tairāwhiti

A further consideration, she adds, is that the Hauora Tairāwhiti technology department staff are well versed with Microsoft (if not specifically Azure) and can therefore upskill with ease owing to a familiar environment.

Situation

Like many local government entities, most of the technology services relied upon by Hauora Tairāwhiti are based on legacy onpremise platforms, confirms Project Manager Natacha Blattes. "While we recognised the need to look at migrating to the cloud - including services and applications – there are a lot of moving parts. As a DHB, we must be mindful of the necessity for security, the unacceptability of any disruption to business as usual, and the complexity of relying on legacy systems built up over the previous decades."

Like every public office, Hauora Tairāwhiti must work within the recommendations of the New Zealand government, which requires agencies to accelerate their adoption of public cloud services — in a balanced way — so they can drive digital transformation. Not only does a move into the cloud represent substantial and ongoing operational improvements, including flexibility, scalability and ease of access, it also represents an opportunity for every department to leave legacy technology in the past while benefiting from the latest advances and continual upgrades.

Solution

With Insight already engaged for delivery of its Microsoft 365 Foundations, it was further engaged for the delivery of the Azure Proof of Concept. This included conducting an environment discovery for recommendations supporting Hauora Tairāwhiti's transformation strategy, fundamental adoption framework and best approach for a productised Azure environment using best practices.

A well-architected cloud solution allows for greater control of information, system costs and ease of delivery. Through the standardisation of governance and controls surrounding these services, Hauora Tairāwhiti can be certain of achieving the desired benefits, while mitigating attendant risks.

> *"However, while moving to Azure is obvious on paper, it's a lot more challenging in practice, particularly as we have to make the move safely and securely. We recognised early on that a successful transition will depend on partnering with the right provider"*
>
> **Natacha Blattes**
> Project Manager – Hauora Tairāwhiti

and it is worth noting that our digital transformation has multiple components and building blocks, of which Azure is only one. There is also the necessity to deliver that transformation while maintaining daily operations and risk-managing existing systems," she explains.

Throughout the delivery, says Blattes, the Insight team distinguished itself by a willingness to transfer knowledge and create appreciation for the advantages available in an appropriately delivered Azure platform. *"The team is forthcoming with information and very clear on the benefits. They are also highly approachable, responding with accuracy and enthusiasm to any issues raised, while demonstrating deep knowledge of, and enthusiasm for, Azure technology."*

Insight’s teams delivered three primary engagements in the delivery of the Azure Proof of Concept, beginning with ‘Envision’

Envision

In this phase, Insight hosted whiteboard-based workshops where Hauora Tairāwhiti staff members learned more about Microsoft Azure and how it provides an underlying platform for current and future initiatives. Cloud Adoption Framework patterns and tools were introduced, while Insight reviewed business motivations, people, processes and technology pillars with Hauora Tairāwhiti, delivering key design decisions informing an Azure Adoption Roadmap document.

Azure Landing Zones

This fed into the creation an ‘Azure Landing Zones’, the output of multi-subscription Azure environments accounting for scale, security, governance, networking, and identity. Azure Landing Zones enable application migration and greenfield development at enterprise-scale and encompass all platform resources required for Hauora Tairawhiti’s application portfolio.

Migration Assessment and Pilot Migration

The final step in the engagement, the Migration Assessment and Pilot Migration, addresses a key component of transformation – the creation of a comprehensive strategy and migration plan. The Azure Migration Assessment identifies pilot workloads and action plans, followed by migration activities including infrastructure deployment, application remediation, and phased migration events.

Results

The primary outcome of the engagement is an Azure reference architecture and the Azure Landing Zones, Microsoft’s reference architecture and approach for optimising Azure capabilities while respecting existing security and governance policies. Blattes explains: *“Ahead of an actual migration, the work delivered by Insight serves as a solid foundation on which we will build, as various streams are identified and prioritised for a shift into the cloud.”*

She adds that the Proof of Concept served as a validation of the decision to move into Azure, which now leaves Hauora Tairāwhiti ready to execute when the time comes. *“With the scope of the engagement taking in the end-to-end Azure adoption experience, we are now in a position where the platform is ready for building and migrating workloads as we expand on our cloud journey.”* In addition to lasting artefacts including documentation and workshop outcomes, Blattes says the value delivered is best described as a capability uplift for the DHB’s technical staff.

> *“We now have skills we didn’t previously possess. That means we are ready to go from on premise into the cloud with a high degree of confidence.”*

But that move won’t be made without support; such is the success of the engagement that Hauora Tairāwhiti has renewed its partnership with Insight.

Insight®

au.insight.com