Insight | Cloud + Data Centre Transformation

Microsoft

How to gain visibility and control across your security environment

IT security teams are often expected to monitor multiple portals and alert systems. This approach is cumbersome and fails to provide singular visibility and control of the IT environment from a security perspective. Learn about important trends in IT security — and a groundbreaking solution that lets you secure in wholly new ways.

Surveying the landscape

We're seeing an increase in cybercrime costs, data volumes, device counts — and in businesses asking for help.

Companies have an average of **47** different cybersecurity solutions deployed[1]

Worldwide data creation will grow from **33 ZB** in 2018 to **175 ZB** by 2025[2]

There will be more than **41 billion** IoT devices by 2027, up from about 8 billion in 2019[3]

58% of companies will be increasing their IT security budget by an average of **14%** in the next year[1]

55% of organisations work with external partners to reduce security risks[4]

The pressure is on

IT security leaders face a number of challenges securing the data centre, the corporate office, email systems, and everywhere in between.

- IT environments are complex with innumerable vectors of attacks
- The growth of endpoints and data volumes demand scalable security
- "Cloud first" initiatives are driving a need to address Security Operations Center (SOC) tools
- Point solutions offer limited scope and create integration challenges for managers (i.e., "tool fatigue")
- Finding and retaining key security talent is increasingly difficult
- Significant investments are required for effective and innovative in-house security operations

What about SIEM?

Amidst a complicated landscape, an intelligent SIEM solution can offer a unified platform for security teams to gain visibility, analytics, and control.

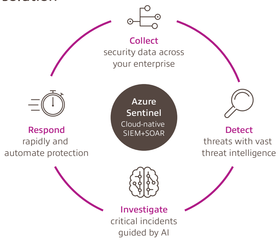
Security Information and Event Management (SIEM)

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

Microsoft Azure Sentinel: An advanced solution

Azure Sentinel™ is a SIEM and Security Orchestration Automation and Response (SOAR) solution built as a cloud service. It collects security data across your entire enterprise — users, devices, applications, and infrastructure deployed on-premises and in multiple clouds.

- Scalable and evergreen
- Consolidates tools required to run an SOC
- Reduces overall security costs
- Eliminates the need for hardware or virtual machines
- Enhances or replaces existing security tools



Secure smarter

It's never been a better time to improve your security posture. We can help you protect your organisation against threats, with intelligence and ease.

Why Insight for Azure Sentinel?

We are a top Microsoft partner and one of only 12 partners mentioned publicly by Microsoft to consult and deliver Azure Sentinel services.

18 Gold and Silver Microsoft competencies

Support from consultation through management of Microsoft® Security solutions

Azure Go Fast Partner and Azure Expert Managed Services Provider (MSP)

Microsoft partner for more than **25 years**

1,000+ Azure-focused engineers and service professionals globally

Get started today

Develop an actionable roadmap for deploying Azure Sentinel. Our Services for Azure Sentinel include an evaluation of your security environment, Azure Sentinel solution design, and a customised deployment plan that considers cost, sizing, and other critical factors.

Learn more

Insight | Cloud + Data Centre Transformation

Microsoft

Sources

[1] Ponemon Institute. (2019). The Cybersecurity Illusion: The Emperor Has No Clothes.
[2] IDC, The Digitisation of the World From Edge to Core, Doc #: US44413318, Nov. 2018. Sponsored by Seagate. [3] Business Insider Intelligence. (2019). Global IoT Executive Survey.
[4] PwC, CIO, and CSO. (2017). The Global State of Information Security® Survey 2017.