4 Ways Microsoft Sentinel Addresses Top IT Security Concerns

Maximise the benefits and capabilities of your security investment.

Insight

Microsoft

Surveying the threat landscape

Finding the right combination of tools, technologies and skill sets is critical to running a successful Security Operations Centre (SOC). This is especially true since there has been a rapid increase in the volume of cyberattacks as of late. Now, take into consideration that the average cost of a breach caused by ransomware in 2021 was an outstanding $4.62 million.[1] That's a lot of potential damages. So, it's no surprise that the pressure is on for IT security teams around the world to improve response time and prevent future loses.

To combat this evolving trend, companies are expected to spend on average $24.4 million on IT security budget in 2022.[2] Those who are looking to house data on premises and in the cloud will need to reassess their existing solutions to ensure complete coverage across all operational locations, home offices, communication systems and everywhere in between.

The growth of endpoints and data volumes demands scalable security.

Point solutions offer limited scope and added integration challenges.

Finding and retaining key security talent has become more difficult.

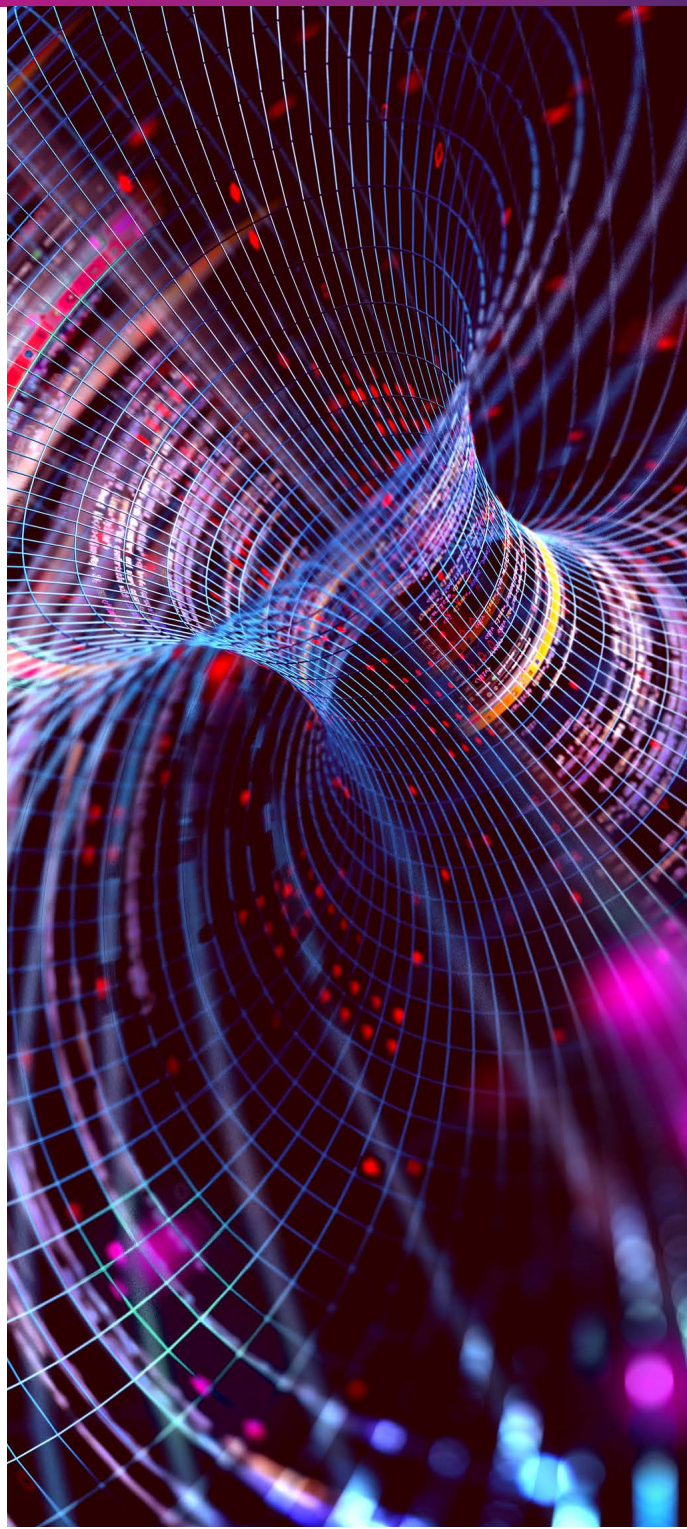
IT environments are only increasing in complexity with countless vectors of attacks.

Think about your data, users and systems.

Having full visibility is critical to detecting and thwarting potential damages, as well as being able to exploit multiple systems from a single starting point and gaining control of the entire IT environment. When it takes companies an average of 280 days to detect a breach, an innumerable amount of data, records and systems can be compromised before steps are even taken to combat the intrusion. One way to improve visibility and cut back on this roadblock is to implement identity and access management. Being able to track user behavior trends to uncover patterns can help businesses close the remediation window and address gaps that were previously unnoticed.

When implementing identity and access management, consider asking the following questions:

- How sensitive is your data?
- Who really needs access to specific files?
- When, and for how long, is access needed?
- Do you need to initiate a data classification program?
- Have you established user types?
- When was the last time you reviewed permissions?
- How are you verifying identities and access points?
- What alternatives have you considered to authentication?
- Would biometrics be a worthwhile choice?
- Have you noticed any blatant gaps or patterns?
- How might you transition your current approach to a more secure one?



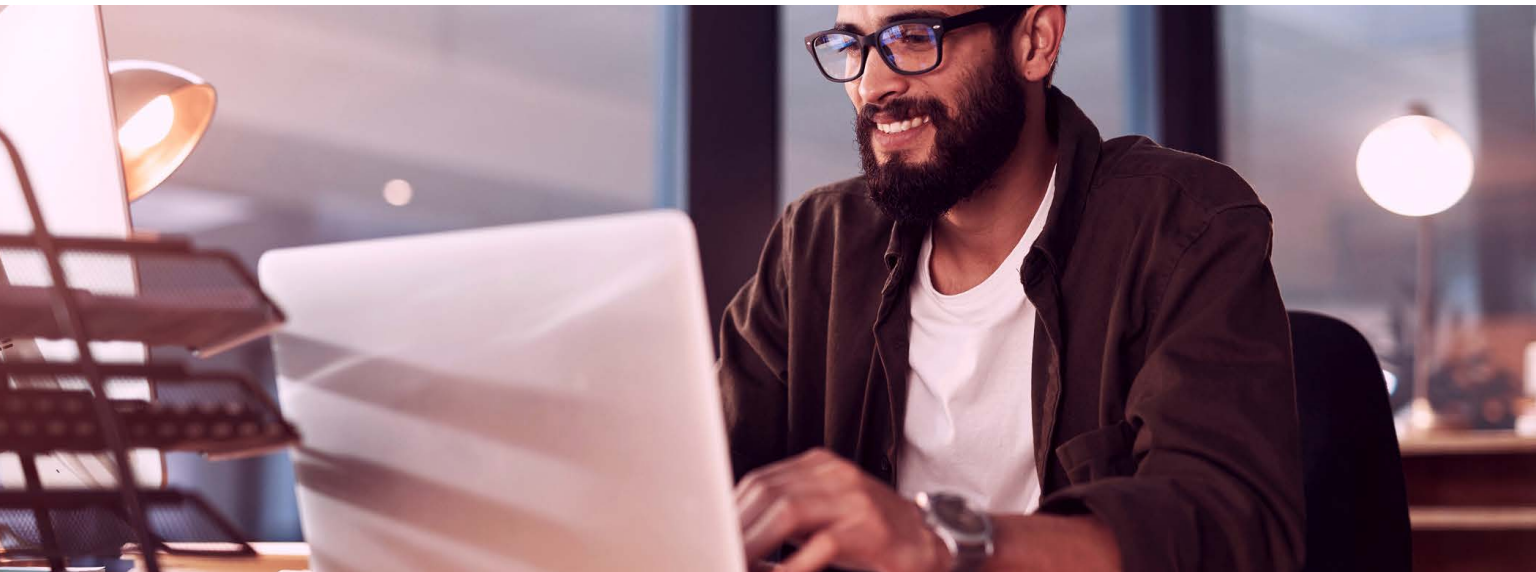
The makings of a modern security program

It may be helpful to note that 89% of companies have already adopted, or are planning to adopt, a multicloud approach.[4] If your business is part of this majority, you may have a diverse IT environment on hand. Being able to successfully track data, malicious hackers and more will improve the effectiveness of the prevention efforts made by your IT security team. Another key feature of a robust program is comprehensive governance that addresses ownership and accountability. By defining security objectives, roles and processes, businesses can better organise guidelines and training, as well as validate users and processes.

Another consideration to keep in mind is that 57% of the companies surveyed in "The State of IT Modernisation 2020" report said that upgrading security infrastructure and processes was a top obstacle in their pursuit of modernising their IT operating environments.[3] This is where a third-party partner may be able to provide added value through automation services.

Automation within the SOC delivers:

- Faster detection, response and remediation capabilities
- Fewer errors and reduced "alert fatigue"
- Security resources freed from repetitive tasks
- Improved user experience and satisfaction



Investing in a cloud-native SIEM solution

Microsoft Sentinel® is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) solution delivered as a cloud service. By leveraging its ability to provide intelligent security analytics for the entire environment, companies can stop threats before they cause harm. As a scalable, evergreen solution, Microsoft Sentinel will enhance or replace your existing security tools to boost visibility into your threatscape.

- Get a bird's eye view across your business.
- Streamline detection and response with Artificial Intelligence (AI).
- Eliminate security infrastructure setup and maintenance.
- Scale to meet evolving security needs.

As an added bonus, this solution reduces costs as much as 48% less and deploys 67% faster than traditional SIEMs.[5] As a result, companies can spend more time focusing on finding real threats quickly by cultivating more strategic security operations. So how exactly does it work? How does it use AI and machine learning to detect, analyse and investigate threats? We'll dive into the four-step process on the next page.

4 steps to next-generation security operations

1. Collect

Businesses today host documents, data, records and more on a multitude of devices, applications and infrastructure, both on premises and in multiple clouds. Plus, all these sensitive files are being accessed by users at virtually anytime, from anywhere. Microsoft Sentinel® collects data at cloud scale, aggregating infrastructure and security devices such as firewalls.

2. Detect

Finding regular occurrences and cyberattack patterns can help businesses lock in on threats. Analytics and unparalleled threat intelligence even help companies uncover previously undetectable threats and minimise the chances of false positives. Imagine being able to monitor and correlate millions of anomalies at once and then quickly pull value from the report. That's what this solution delivers.

3. Investigate

Tapping into decades of cybersecurity work at Microsoft, Microsoft Sentinel hunts suspicious activities at scale with guidance from AI — eliminating the need for hardware or virtual machines. It learns from daily logs how to cut through the noise, so security teams can focus on the essential signals.

4. Respond

With built-in orchestration and the automation of common tasks, businesses can respond to incidents rapidly. By leveraging intelligent technology, your IT security team will not only save time, but improve accuracy too. For instance, playbooks triggered by analytics or automation rules can be run within Microsoft Sentinel to streamline response time and block malicious actors.

Why Insight for Microsoft Sentinel?

At Insight, we believe there's never been a better time to improve your security posture, especially with the rise of remote and hybrid work. Lean on our years of experience to protect your company against evolving cyberthreats. Together, we'll help your business obtain a flexible, scalable solution leveraging cutting-edge AI and machine learning capabilities. The goal: improved security, visibility and control of your entire IT environment.

We're a top Microsoft partner and one of only 12 partners mentioned publicly by Microsoft to consult and deliver Microsoft Sentinel® services:

- 18 Gold and Silver Microsoft competencies
- More than 25 years as a Microsoft partner
- 1,000+ Azure-focused engineers and service professionals
- An Azure Expert Managed services Provider (MSP) and largest Azure partner
- Microsoft Security 20/20 award winner for the Azure Security Deployment Partner of the Year category
- Support throughout and consultation services delivery

About Insight

Insight Enterprises, Inc. is a Fortune 500 solutions integrator with 11,500 teammates worldwide helping organisations accelerate their digital journey to modernise their business and maximise the value of technology. We enable secure, end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 33+ years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class e-commerce experience, realising the digital ambitions of our clients at every opportunity.

Insight®

uk.insight.com

Sources:

[1] IBM Security. (2021). Cost of a Data Breach Report.

[2] Channel Futures. (February 2022). The High Cost of Ransomware.

[3] Insight. The State of IT Modernisation 2020.

[4] Flexera. (March 2022). 2022 State of the Cloud Report.

[5] Forrester. (November 2020). The Total Economic Impact™ of Microsoft Microsoft Sentinel. Cost Savings and Business Benefits Enabled By Microsoft Sentinel.

MKT6231