Microsoft Security

# 3 Reasons to Shift to Integrated Threat Protection

# Contents

# Introduction

**The average enterprise now uses more than 30 different security tools, often disjointed and "bolted-on."**

Security is at an inflection point. Cyberattacks are becoming more sophisticated as organizations continue to grapple with challenges ranging from talent shortages and cost balancing to navigating the pressures of hybrid work.

Meanwhile, the security market is more fragmented and complex than ever. The average enterprise now uses more than 30 different security tools, often disjointed and "bolted-on," providing limited visibility and inadequate insights to security operations centers (SOCs).

Security and compliance leaders want a better understanding of the latest risks and threats, but they also need to know what's working, what isn't, and where they have gaps.

While the scope of today's security challenges may seem overwhelming, there's cause for optimism for CISOs looking to improve the efficiency and effectiveness of security operations. The answer lies in an integrated, end-to-end approach to cyberthreat protection, which will help organizations:

## Reason 1: Do more with less

**Consolidate point solutions and reduce security operations (SecOps) overhead.**

## Reason 2: Empower SecOps to focus on high-value tasks

**Use tools that increase efficiency and make even junior analysts more capable than ever.**

## Reason 3: Increase employee productivity

**Protect your organization in a way that lets your people be fearless as they create and innovate.**

This approach is enabled by integrating an extended detection and response (XDR) solution with a cloud-native security information and event management (SIEM) system that uses artificial intelligence (AI) and automation capabilities. The integrated solution can help your SOC become more predictive, proactive, and preventive against attacks across the enterprise.

## Reason 1

# Do more with less

**By consolidating tools with Microsoft's integrated solution, you can also save by paying for only what you use.**

Many organizations have approached security tooling with a focus on best-of-breed point solutions. Unfortunately, that approach can actually make it harder for security professionals to identify and respond to threats quickly. It can also end up having a negative impact on IT spending and end-user productivity.

As organizations look to do more with less, an integrated approach such as Microsoft's SIEM and XDR can help. It can reduce complexity by consolidating individual tools—and because it's cloud-native, an integrated solution can also improve performance and scale.

By consolidating tools with Microsoft's integrated solution, you can also save by paying for only what you use. You can also reduce the SecOps overhead required to manage solutions by increasing automation and integration.

> Starting the process of adopting new security tools is easy because you expect the gaps to be wide. Progressing from there, you will soon realize that tools from different vendors can potentially overlap in their mandate. Such an overlap might be desirable for checks and balances **but might also come at a hefty financial cost.**"
>
> **Jonathan Cassar**
> Chief Technology Officer, MITA

# $1.6 million

**saved annually from vendor consolidation**

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Microsoft SIEM and XDR. These were some of the key findings for a hypothetical composite organization with 8,000 total employees and 10 security professionals:

- **Saving almost $1.6 million annually from vendor consolidation**. The Microsoft SIEM and XDR investment enables the composite to reduce the cost of its prior SIEM ($560,000), the associated on-premises infrastructure (over $360,000), three XDR point solutions ($192,000), and the ongoing labor cost to manage these ($480,000).
- **Reducing the risk of a material breach by 60%.** With more efficient security investigation and response workflows, improved security response automation, and the increased ability to protect all computing environments, including multicloud protection, the composite reduces the risk of breaches with an annual impact of $1.6 million saved.
- **Generating a ROI of 207%.** The representative interviews and financial analysis found that a composite organization experiences benefits of $17.68 million over three years versus costs of $5.76 million, adding up to a net present value (NPV) of $11.92 million.

## Reason 2

# Empower SecOps to focus on high-value tasks

**It's critical to integrate SIEM and XDR to correlate alerts, prioritize the biggest threats, and coordinate action across the enterprise.**

SecOps teams are overwhelmed by the quantity of signals they have to analyze, including many low-fidelity signals that are difficult, if not impossible, to detect manually and mitigate. As threats increase, it's hard for an overburdened SOC to keep up, especially when trying to analyze data from multiple point solutions. Allocating more resources to fill the gaps isn't the answer, because finding enough skilled security professionals is an ongoing challenge.

That's why it's critical to integrate SIEM and XDR to correlate alerts, prioritize the biggest threats, and coordinate action across the enterprise, with advanced AI and automation to proactively detect and remediate threats.

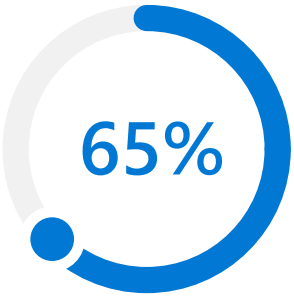
Consider, for example, that a single, low-level signal may not garner much attention from a traditional SIEM. But by using AI, a cloud-native SIEM can automatically compare that signal to signals from other sources throughout the organization, correlating across multiple datasets to find multistage attacks.

**Integrated SIEM and XDR frees up SecOps resources while also empowering even junior analysts with more capabilities and confidence.**

The system then normalizes, analyzes, and correlates the data, while providing context about how the cyberattack entered the infrastructure, along with the timeline of how it spread. This lets SOC teams visualize the breach—from a single console—and effectively address it.

> A lot of CISOs don't realize **the overhead they impose on their teams with 20 different panes of glass** or point solutions, and the associated annual costs... we've eliminated a lot of tool fatigue with a single vendor."
>
> **Terence Jackson**
> Chief Information Security and Privacy Officer, Thycotic

An organization shouldn't need deep expertise to unlock the value of a security solution. Integrated SIEM and XDR frees up SecOps resources while also empowering even junior analysts with more capabilities and confidence.




**The integrated approach of Microsoft SIEM and XDR reduced time to investigate threats by 65%.**

**The Forrester Total Economic Impact™ (TEI) study commissioned by Microsoft showed this kind of SecOps efficiency in its composite organization:**

- **Reducing time to investigate threats by 65% and reducing time to respond to threats by 88%.** Microsoft SIEM and XDR's integrated approach to security threat investigation and response makes these workflows more efficient for the composite organization's security professionals. They no longer need to jump through multiple tools to identify threats, while security automation features further enhance response workflows.
- **Reducing the time to create a new workbook by 90% and the time to onboard new security professionals by 91%.** Microsoft SIEM and XDR's integrated approach makes additional security professional workflows more efficient as well. As SIEM logs are integrated throughout the suite of solutions, workbook creation is nearly automated, while a singular login enables new security professionals to onboard nearly 16 weeks faster.

## Reason 3

# Increase employee productivity

**An integrated SIEM and XDR solution can help your organization improve productivity for end users.**

In addition to doing more with less and increasing SecOps efficiency, an integrated SIEM and XDR solution can help your organization improve productivity for end users.

As SecOps teams know, when you make security hard, people work around it. So, when end-user experiences hamper rather than help employees' productivity, that can leave an organization open to more security risks and higher costs. Weak or lost passwords, unsecured access via personal devices, or unfettered sharing of sensitive data are just some of the challenges.

> [In the past] we'd use blunt instruments when someone suspected an issue. We'd shut things down and close off access, which negatively affected our business. And it was very clear to everyone because things would temporarily stop working. In Microsoft Sentinel we have a scalpel with which we can surgically react to what's happening. **The business usually doesn't even know when we're responding to a threat**, and that's a really important measure of our success."
>
> **Rick Gehringer**
> Chief Information Officer, Wedgewood

**Almost**
# 68,000
**Microsoft SIEM and XDR improved productivity of other employees by almost 68,000 total hours annually.**

An integrated SIEM and XDR approach helps you deliver seamless user experiences that keep your people both productive and secure across all facets of their daily experiences. It can reduce negative impacts to productivity, such as having to turn off services or isolate and then reimage machines. But integrated SIEM and XDR can also create new opportunities for end-user productivity gains, such as with more self-service security support, better dashboards and reporting, and more responsiveness and faster boot times from running fewer security agents.

In the Forrester Total Economic Impact™ (TEI) study commissioned by Microsoft, the hypothetical composite organization with 8,000 total employees showed an increase in employee productivity by deploying Microsoft SIEM and XDR:

- **Improving productivity of other employees by almost 68,000 total hours annually.** Microsoft SIEM and XDR prevents negative impacts on other employees from inefficient security processes. For example, the composite saves 4,000 hours annually thanks to IT professionals' new ability to self-serve regarding security updates and recommendations. It also enables remote security-based troubleshooting on employee machines and reduces the number of security agents running on them, saving nearly 64,000 hours annually in end-user productivity.

Security has become an essential enabler of technological success. That's why organizations need security measures that build as much resilience as possible against modern attacks—to safeguard and enable the productivity and innovation that drive growth.

# Get integrated cyberthreat protection with SIEM and XDR

**This integration of industry-leading products delivers cyberthreat prevention, detection, and response in a single comprehensive solution.**

Microsoft offers the first and only integrated SIEM and XDR solution, providing end-to-end visibility across all clouds and platforms. This integration of industry-leading products delivers cyberthreat prevention, detection, and response in a single comprehensive solution.

Microsoft SIEM and XDR taps into the power of AI and automation, as well as deep, ongoing investments in cyberthreat detection and analysis—with expert insights and visibility into 43 trillion signals every day. With integration across these products, SOC teams are armed with more context than ever to hunt and resolve critical cyberthreats faster:

### Microsoft Sentinel

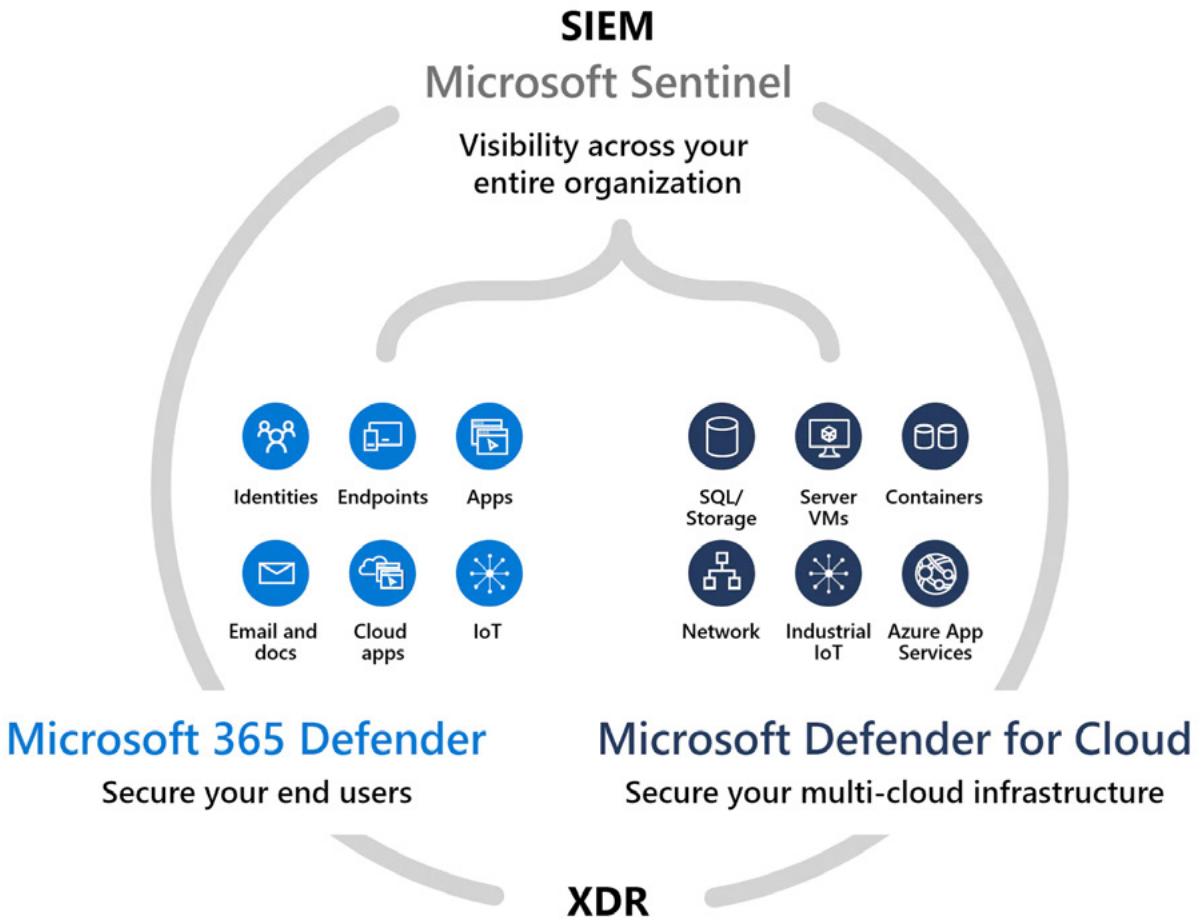
Get a bird's-eye view across the enterprise with Microsoft's cloud-native SIEM. Aggregate security data from virtually any source and apply AI to separate noise from legitimate events, correlate alerts across complex cyberattack chains, and speed up cyberthreat response with built-in orchestration and automation.

### Microsoft Defender XDR

Prevent and detect cyberattacks across your identities, endpoints, apps, email, data, and cloud apps with XDR capabilities. Investigate and respond to cyberattacks with out-of-the-box, best-in-class protection. Hunt for threats and easily coordinate your response from a single dashboard.

### Microsoft Defender for Cloud

Protect your multicloud and hybrid cloud workloads with built-in XDR capabilities. Secure your servers, storage, databases, containers, and more. Focus on what matters most with prioritized alerts.



# Don’t bolt security on. Build it in.

Put the right tools and intelligence in the hands of the right people. Defend against modern attacks with an end-to-end, cloud-native, integrated solution.

**Learn more about integrated cyberthreat protection with Microsoft’s SIEM and XDR solutions** >

Microsoft Security