


# Extending SIEM

How to get the most  
from your security stack

The graphic features several overlapping geometric elements: a yellow diagonal bar on the left, a blue diagonal bar on the right, a green curved bar at the bottom, and a central white circle with an orange dot. A grey circle is partially visible on the right edge.

# Contents



## Introduction

Page 03

### 1 Having too many solutions adds costs and complexity

Page 05

### 2 Identify which cloud-based services you can consolidate with an integrated solution

Page 08

### 3 Get more from your SIEM with XDR

Page 11

### 4 Integration and synchronization provide broader threat context

Page 14

## Integrated threat prevention, detection, and response with Microsoft SIEM and XDR

Page 17

# Introduction

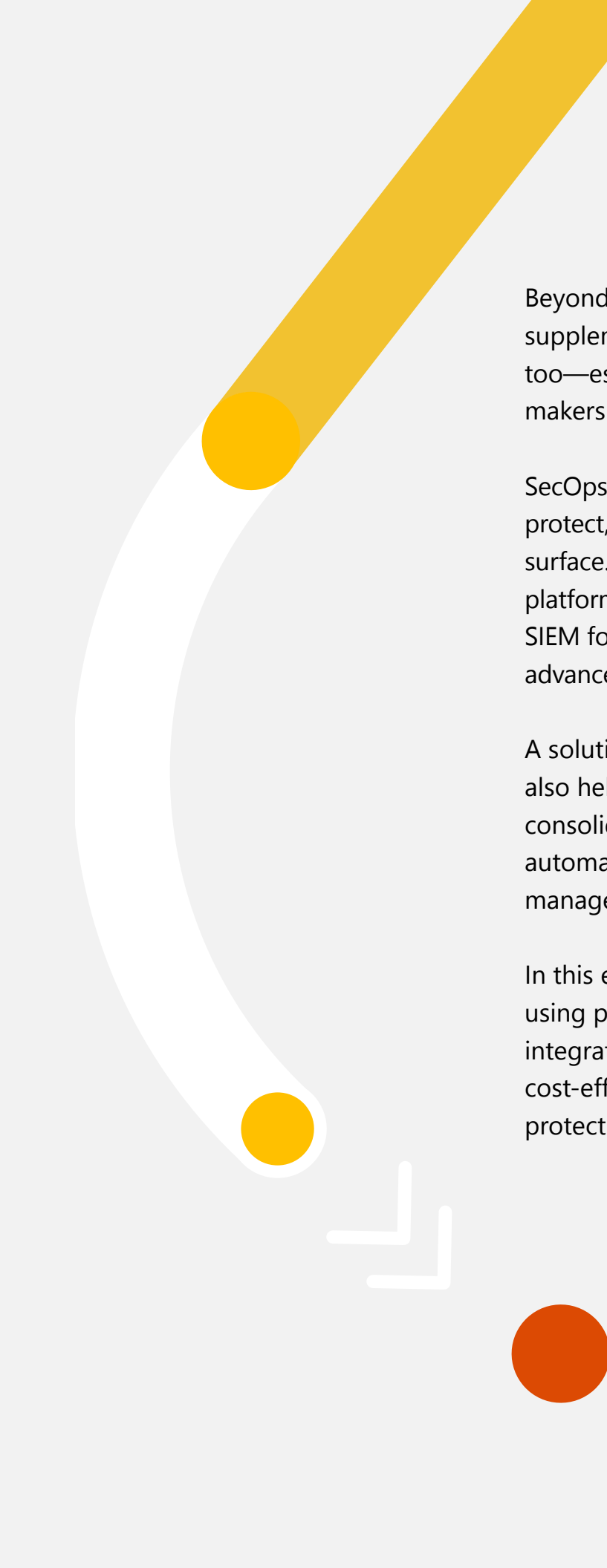
**For more than a decade, SecOps teams have relied on security information and event management (SIEM) systems to monitor and analyze security alerts across their digital infrastructure.**

As the volume and sophistication of cyberattacks have grown, security teams added a myriad of tools to their SIEM systems in an attempt to increase visibility into vulnerabilities and active threats.

Through it all, SIEM systems have remained a powerful addition to the SecOps toolbox. Organizations continue to invest heavily in the solution. According to a [Gartner report](#), "the SIEM market grew from \$3.41 billion in 2020 to \$4.10 billion in 2021, a 20% annual growth rate compared to a 3.9% decline the previous year."<sup>1</sup>

As organizations move more of their IT stack to the cloud, cloud-based security tools are following. A variety of cloud-based services can supplement SIEM solutions with specific security management functions, helping SecOps teams identify issues, close vulnerabilities, and respond to active threats. But these services have also added layers of complexity and unfiltered noise that may actually increase risk instead of reducing it.





Beyond increased complexity and risk, this sprawl of supplementary services can have a financial impact, too—especially at a time when security decision-makers are feeling more pressure to cut costs.<sup>2</sup>

SecOps teams need a better option to identify, protect, and defend against an ever-changing attack surface. Extended detection and response (XDR) platforms are a way to strengthen a cloud-native SIEM for greater threat protection, smarter telemetry, advanced automation, and increased efficiency.

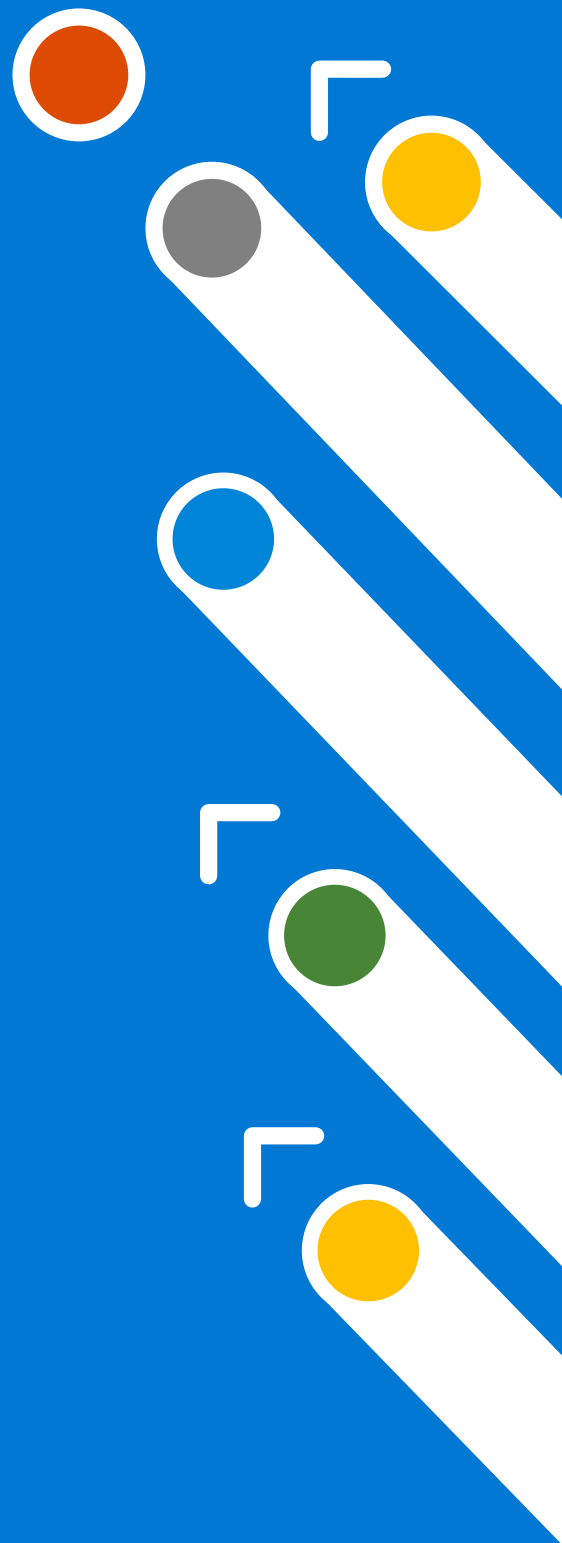
A solution that integrates SIEM and XDR can also help organizations do more with less, by consolidating individual tools and increasing automation and integration in ways that reduce management overhead for SecOps.

In this e-book, we examine the challenges of using point solutions with SIEM and explain how integrating SIEM with XDR can make SecOps more cost-effective and manageable, while improving protection across the enterprise.

1

## Having too many solutions adds costs and complexity

A patchwork of security tools and strategies makes it difficult to meet the demands of today's distributed enterprise. One-off security solutions can be costly to maintain, time-consuming to deploy, and inevitably contribute to a daunting mix of consoles and reports that are tough to monitor and manage.



**Reducing complexity in security infrastructure has become increasingly important. According to a [Gartner survey](#), “75% of organizations are pursuing security vendor consolidation in 2022, up from 29% in 2020.”<sup>3</sup>**

Having fewer tools enables more seamless integration with SIEM and better-coordinated detection and response. All the components of the security stack can work together more easily, to find and remove sophisticated adversaries wherever they lurk.

Given the enormous amount of security signal generated by the digital ecosystem, modern solutions also need built-in artificial intelligence (AI) and automation to process routine tasks and filter high-value alerts out from all of that noise. SIEM needs to evolve beyond visibility and log data to offer SecOps teams a more proactive approach to identifying and mitigating threats, while also automating many tasks and offering a simplified level of management that reduces risk.



**3 out of 4**

Three out of four organizations were pursuing security vendor consolidation in 2022.

Moving to a cloud-native SIEM is an important step in that direction. Integration with an extended detection and response (XDR) solution can improve the efficiency and cost-effectiveness of security operations even further. A Forrester Consulting [Total Economic Impact™ \(TEI\) study](#) commissioned by Microsoft found that organizations deploying integrated Microsoft SIEM and XDR saw significant cost savings and an increase in security operations efficiency. These were some of the benefits for the composite organization representative of interviewed customers:

- Microsoft SIEM and XDR reduced the cost of a legacy SIEM solution, associated on-premises infrastructure, and ongoing management staffing, saving almost \$1.6 million annually from vendor consolidation.
- Microsoft SIEM and XDR reduced the cost of material breaches by \$3.9 million over three years.



## 207% ROI

Microsoft SIEM and XDR generated a net present value (NPV) of \$11.92 million and an ROI of 207% over three years.

## 2

# Identify which cloud-based services you can consolidate with an integrated solution

As enterprise perimeters expanded beyond the corporate walls, SecOps teams added third-party tools and services to augment SIEM. But as organizations now look to reduce costs, complexity, and risk, many of these solutions can be consolidated by a more comprehensive, integrated solution.





**Many common cloud-based services can augment SIEM configurations. They offer important features that can help a SIEM system improve protection, but integrating and managing them presents its own set of challenges.**

That's why the following tools and services are a good first place to look when considering where to consolidate.

### **Examples of tools and services to consider for consolidation with an integrated solution**

#### **Cloud Access Security Broker (CASB)**

A CASB serves as a "blanket" on top of a cloud-native SIEM. It collects log information from multiple sources and exposes anomalous events and threats, making the SIEM cloud-aware and giving it the information needed for remediation.

#### **Cloud Security Posture Management (CSPM)**

CSPM automates the identification and remediation of risks across cloud infrastructures and also applies best practices for cloud security in multicloud environments.

#### **Cloud Workload Protection Platform (CWPP)**

CWPPs target the unique protection requirements of workloads in modern hybrid, multicloud environments. They help security teams discover and protect workloads in on-premises and public cloud environments.





### **Endpoint Detection and Response (EDR)**

EDR determines if malware has been installed on an endpoint device and finds ways to respond. Once installed, EDR solutions collect data from many different sources and store it in a central database.

### **Network Detection and Response (NDR)**

NDR applies AI and security research to detect and respond to cyberattacks in real time, keeping a watchful eye on hidden attacker behaviors in workloads in the cloud and hybrid cloud, as well as in on-premises enterprise networks.

### **Vulnerability Management**

Vulnerability Management is a continuous, proactive, and often automated process that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches.

### **Data Loss Prevention (DLP)**

DLP provides a balance between protection and productivity, ensuring the proper access controls are in place and policies are set to prevent actions such as improperly saving, storing, or printing sensitive data.

### **Secure Web Gateway (SWG)**

SWG is a web security service that filters unauthorized traffic from accessing a particular network. The goal of a SWG is to zero in on threats before they penetrate a virtual perimeter.

## Get more from your SIEM with XDR

A cloud-native SIEM solution provides valuable insights, giving SecOps teams a comprehensive command-and-control experience across the entire enterprise. It can collect and analyze data across the entire organization to detect, investigate, and respond to incidents that cross silos. It can also enhance SecOps efficiency with customizable analytics and built-in automation.



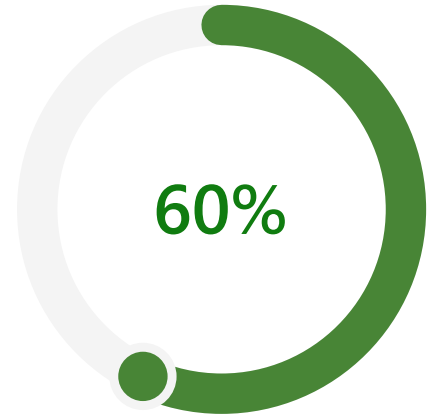
**Instead of layering on multiple point solutions that add counterproductive complexity, CISOs should consider integrating XDR as a more effective complement to SIEM, helping to gather and process telemetry from across the IT stack in a single dashboard. XDR provides depth of knowledge into specific threats, while SIEM provides broad visibility for managing security operations from a bird's-eye view.**

XDR takes security management beyond endpoints to help SecOps teams investigate attacks by examining specific resources across platforms and clouds. XDR applies threat intelligence to aggregated data to more effectively identify trends, allowing SecOps teams to more quickly spot vulnerabilities, detect attacks, and respond using auto-remediation. The technology can help reduce the number of alerts that the security team must investigate by using correlation and behavioral analysis on consolidated threat data, eliminating false positives and low-fidelity alerts.

Microsoft's XDR solution includes Microsoft 365 Defender and Microsoft Defender for Cloud, which automatically collects, correlates, and analyzes security signals and threat alert data involving endpoints, users, applications, the internet of things, and cloud workloads. It uses AI and automation capabilities to stop attacks faster and remediate affected assets.



A commissioned Forrester Consulting [Total Economic Impact™ \(TEI\)](#) study found that organizations deploying integrated Microsoft SIEM and XDR reduced the risk of a material breach by 60%, reduced time to investigate threats by 65%, and reduced time to respond to threats by 88% for the composite organization representative of interviewed customers.



Microsoft SIEM and XDR reduced the risk of a material breach by 60%.

Because of its depth of functionality and automation capabilities, XDR also can help CISOs address the pressing challenges of the cybersecurity talent gap. An [\(ISC\)2 Cybersecurity Workforce Study](#) puts the global cybersecurity talent workforce gap at 3.4 million people. With skilled security professionals in high demand, SecOps teams are often overwhelmed with alerts and a backlog of incidents that need to be investigated and potentially remediated.

The Forrester Consulting [TEI study](#) found that for the composite organization, Microsoft SIEM and XDR reduced the time to create a new workbook by 90% and onboard new security professionals by 91%. Improved threat investigation and response time saved another \$2.7 million over three years.

Microsoft is recognized as a Leader in the 2022 Gartner® Magic Quadrant™ for SIEM

Microsoft also had the highest “Ability to Execute” in the [2022 Gartner Magic Quadrant for Security Information and Event Management report](#).<sup>4</sup>

Various industry analysts consistently named Microsoft a leader in security, compliance, identity, and management. [Learn more](#)

# 4

## Integration and synchronization provide broader threat context

Integrating SIEM and XDR allows systems to share even more incidents, schema, and alerts, giving SecOps teams a unified view and the ability to seamlessly drill down into individual incidents for more context. Together, Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender offer broad and deep visibility across organizations while improving SecOps efficiency and response times.



**Connectors allow organizations to stream data from the Microsoft XDR solution into Microsoft Sentinel so SecOps teams can view, analyze, and respond to Defender alerts—and the incidents they generate—in a broader organizational context.**

For example, a team using Kusto Query Language (KQL) to explore log analytics in Microsoft Sentinel can use that same query in Microsoft 365 Defender to look at performance-related data or follow up on an alert. Information between the two systems is synchronized in both directions, so security analysts can easily move from one tool to the other to identify, remediate, and close an incident. When an incident containing a security alert is closed in one system, the corresponding alert in the connected system is closed automatically.





By feeding XDR data into SIEM, organizations get more value out of both technologies. An integrated SIEM and XDR environment provides a single dashboard for viewing and managing threats across multicloud, on-premises, and hybrid environments. It allows for billions of pieces of signal data from XDR and other sources to be reduced to thousands of alerts and tens of incidents, thereby minimizing alert fatigue and false positives for SecOps teams.

Integration helps SecOps teams perform centralized, context-based threat detection, analysis, and response. SIEM platforms offer log management and retention capabilities for XDR data, so it's available for threat investigation and forensic analysis. This can enable better insight into past security incidents so measures can be taken to prevent the same events from happening again.



# Integrated threat prevention, detection, and response with Microsoft SIEM and XDR

Attacks are escalating in frequency and sophistication, and legacy tools can no longer keep up with the evolving threat landscape. CISOs need a more effective, comprehensive solution, especially as many are feeling organizational pressure to do more with less.

Microsoft's vision for SIEM and XDR is to deliver a single, integrated solution to help SecOps teams stop attacks and keep their organizations safe. Microsoft SIEM and XDR solutions extend beyond native and hybrid models to provide the depth of automated correlation from XDR, integrated with the breadth of a cloud-native SIEM—to reduce complexity, lower costs, and improve risk posture.

**Find out how integrated threat protection can help your security team do more with less.**

[Learn more >](#)

The advanced security and compliance features in Microsoft 365 E5 can provide up to 60% savings over comparable multi-vendor standalone solutions.<sup>5</sup>

[See how many point solutions you could remove from your balance sheet with Microsoft 365 E5 >](#)

<sup>1</sup> Gartner, "[Magic Quadrant for Security Information and Event Management](#)," Pete Shoard, Andrew Davies, Mitchell Schneider, October 10, 2022.

<sup>2</sup> March 2022 survey of 501 US Security Decision Makers commissioned by Microsoft from agency Vital Findings.

<sup>3</sup> Gartner Press Release, "[Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022](#)," Sept 13, 2022.

<sup>4</sup> Gartner, "[Magic Quadrant for Security Information and Event Management](#)," October 10, 2022.

<sup>5</sup> Illustrative comparison based on web direct/base price for Microsoft 365 E5 compliance and security add-ons to Microsoft 365 E3 (\$24/user) vs. multi-vendor prices based on publicly available estimated pricing for other vendor solutions (\$63/user).

GARTNER is registered trademark and service mark of Gartner, Inc. and MAGIC QUADRANT is a registered trademark of Gartner and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



©2023 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.