Microsoft Security

Safeguarding the business with SIEM and XDR

Contents

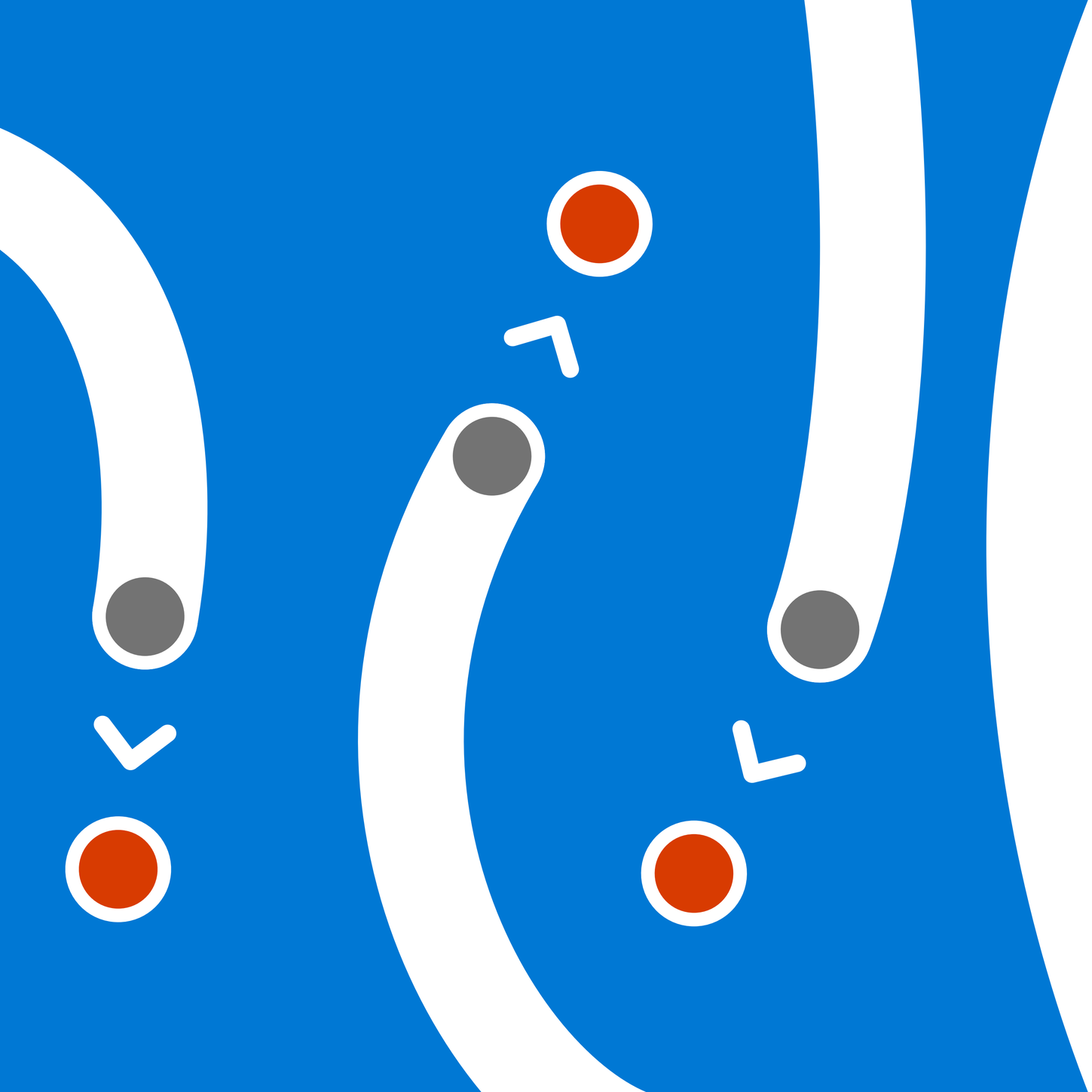
The shift to remote and hybrid work models over the past two years has left organisations more vulnerable to ransomware and other threats. Microsoft's Digital Defence Report notes a steady increase in ransomware 'encounter rates' for enterprises since the onset of the pandemic, reaching 100 million encounters in February 2021 alone.

SecOps teams have a much broader attack surface to protect because IT infrastructure now extends across multi-cloud, hybrid cloud and on-premises environments, and employees can access enterprise resources from virtually anywhere, using company-owned systems or unmanaged personal devices.

SecOps teams have responded to these trends by deploying multiple point products to protect against the broadening threatscape. These tools, while helping to safeguard specific workloads, assets or people, have also complicated the security challenge by forcing data and detection capabilities into multiple silos.

CISOs and their security teams need a better way to view threats across multi-cloud and on-premises IT environments to increase protection of resources and reduce the time it takes to detect and respond to incidents.

This eBook explores a critical next step in the evolution of security operations: Integrating cloud-native security information and management (SIEM) capabilities with extended detection and response (XDR).



What is XDR?

A full-featured XDR platform enables organisations to protect their digital ecosystem by collecting, correlating and analysing security telemetry from endpoints, networks, applications, cloud workloads and identity infrastructure.

The depth of information XDR consolidates helps SecOps teams uncover threats and attacks much faster than traditional, siloed detection and response platforms. SecOps analysts can leverage the cross-domain threat visibility and contextual alerts that XDR platforms provide to initiate quick and targeted responses.

XDR improves efficiency for SecOps teams by providing telemetry across integrated workloads. The technology helps reduce the number of alerts the security team must investigate by using correlation and behavioural analysis on consolidated threat data to eliminate false positives and low-fidelity alerts. The tools support automated investigation of threats and auto-remediation of compromised assets, often without the need for human intervention. Security teams can leverage the tailored recommendations and workflows available with XDR tools to implement proactive defences against identified vulnerabilities.

Microsoft 365 Defender and Microsoft Defender for Cloud offer cross-domain security as part of the Microsoft XDR solution. Microsoft 365 Defender helps organisations block a wide range of threats at the network perimeter, preventing intrusion. It also automatically collects, correlates and analyses threat and alert data from across the Microsoft 365 environment. This includes security telemetry from endpoint devices, email, applications and identities. The technology combines AI with automation to enable automatic attack mitigation and remediation of compromised assets.

Microsoft Defender for Cloud combines cloud security posture management with cloud workload protection capabilities. Defender for Cloud helps SecOps teams protect against cloud threats and continuously assess the security of their cloud environment. It issues alerts on detected threats to cloud workloads and resources, and then recommends customised mitigations for addressing the threats and hardening cloud assets against identified weaknesses.

Benefits of integrated SIEM and XDR

SecOps teams can capture even more value by layering XDR telemetry on a cloud-native SIEM platform. SIEM enables organisations to get more actionable information from security telemetrics by applying advanced analytics and threat intelligence to security information and event data gathered from across the enterprise IT infrastructure.

The Microsoft Sentinel cloud-native SIEM platform uses a correlation engine and AI-enabled behavioural analytics capabilities to condense vast amounts of data into alerts that are relevant to an organisation's security posture. Built-in orchestration and automation allow organisations to respond rapidly to detected threats and incidents.

SecOps analysts can use SIEM platforms like Microsoft Sentinel to compare internal security telemetry and log data with external intelligence to detect new threats and identify potential security breaches. The aggregated log data in SIEM platforms enables better forensics and investigations of past security incidents.

By feeding XDR data into SIEM, organisations can derive more value from both technologies. An integrated SIEM and XDR environment provides consolidated dashboards for viewing and managing threats across multi-cloud, hybrid cloud and on-premises 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 – minimising alert fatigue and false positives.

SIEM and XDR integration enhances the ability of SecOps teams to perform centralised, context-based threat detection, analysis and response. SIEM platforms offer log management and retention capabilities for XDR data, so it is 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.

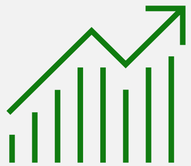
Organisations can also gain significant productivity benefits from connecting SIEM with XDR. A Forrester Consulting Total Economic Impact™ study found that Microsoft 365 Defender helped organisations reduce the number successful attacks and recover faster from breaches that did occur. The technology decreased the need for remediation efforts because fewer machines were compromised.

The Forrester study showed that, cumulatively, XDR helped organisations save USD 6.7 million in end-user productivity by ensuring less system downtime from security breaches. Security teams reported another USD 6.7 million in efficiency gains from:

A unified view of threat data.

Fewer false positives to chase after.

Automated response and remediation capabilities.



XDR helped organisations

save USD 6.7 million

in end-user productivity

Microsoft's approach to SIEM and XDR

Microsoft's vision for SIEM and XDR is to deliver an integrated offering that connects Microsoft Sentinel with Microsoft 365 Defender and Defender for Cloud. The technology also supports multi-cloud and multi-platform environments to ensure third-party data and signals are part of Microsoft SIEM and XDR.

Microsoft's goal is to combine the automated correlation from XDR with the power of cloud-native SIEM to help SecOps teams protect against attacks and keep enterprise data and resources safe from compromise.

Microsoft Sentinel

Microsoft Sentinel is Microsoft's cloud-native SIEM platform. It accelerates threat detection and response by collecting, correlating and analysing security log and event data at scale from devices, applications, users and infrastructure hosted in the cloud and on-premises.

Microsoft Sentinel enables organisations to detect threats they might have otherwise missed, by comparing internally gathered security telemetry with real-time external threat intelligence gathered from Microsoft sensors and other third parties. SecOps teams can leverage the AI and cloud security analytics capabilities in Microsoft Sentinel to hunt for hidden threats and signs of previous breaches in aggregated log data. The technology offers inline orchestration and automation capabilities for speeding up threat response and remediating compromised resources quickly and efficiently.

Microsoft aggregates security data – more than 24 trillion signals a day – from a broad and diverse spectrum of business environments and consumer devices. Microsoft Sentinel's correlation and analytics capabilities help organisations condense billions of daily security signals from across the enterprise technology stack into a manageable handful of legitimate events, and even fewer high-priority alerts that need to be investigated. This means SecOps teams can spend more time on proactive threat hunting and mitigation. The technology reduces complexity by enabling a unified, multi-domain view of the threat environment.

Microsoft 365 Defender

Microsoft 365 Defender offers XDR for email, documents, identities, apps and endpoints. It collects, correlates and analyses threat signals and alerts from across the Microsoft 365 environment including endpoint devices, email, applications and identities. Microsoft 365 Defender includes the following services to provide additional XDR depth:

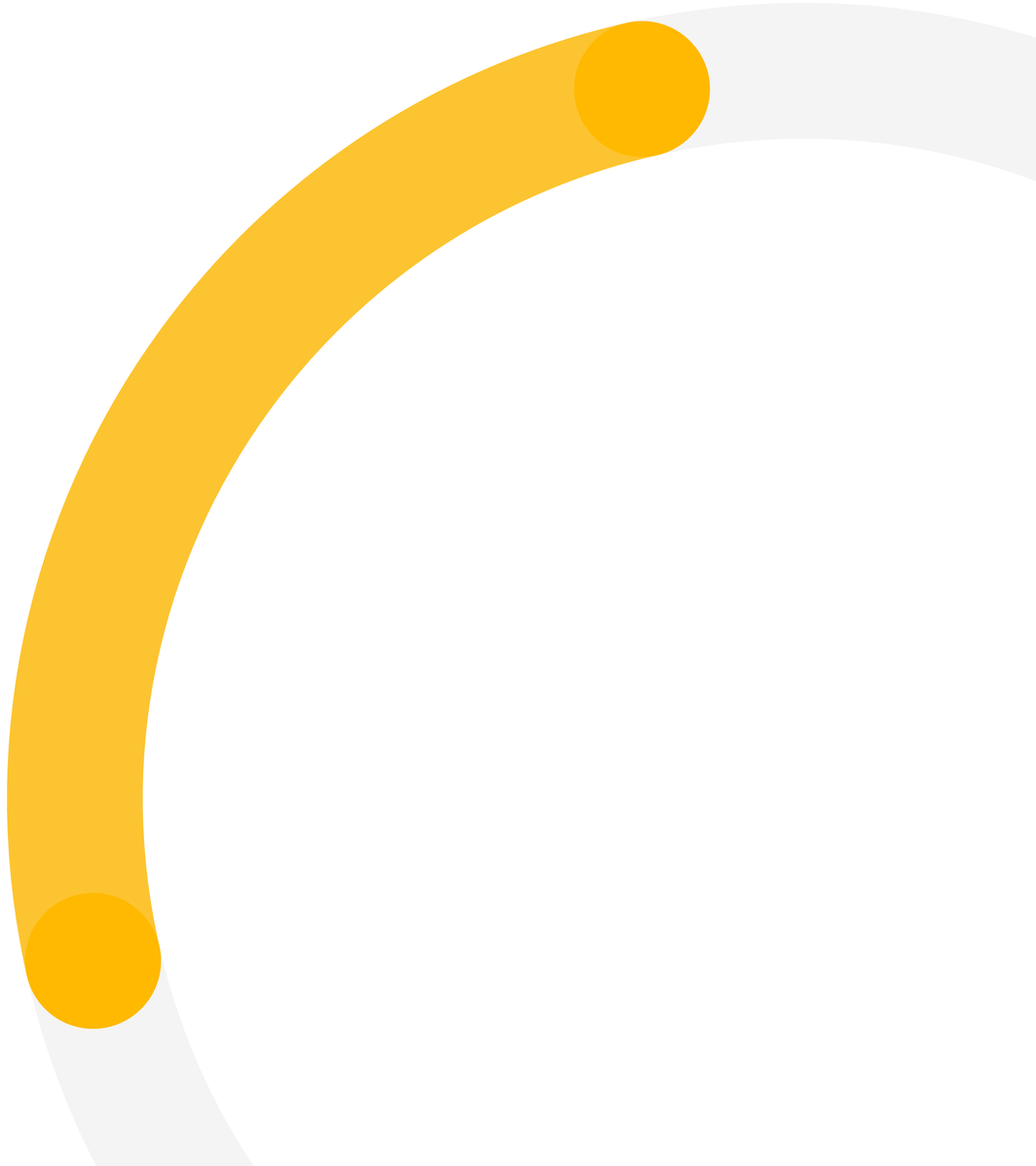
- **Microsoft Defender for Endpoint** analyses behavioural signals from Windows 11 endpoint environments to detect threats that signature-based threat detection tools might miss. It applies cloud security analytics to translate behavioural signals into actionable insights and threat detections, and recommends automated responses to advanced threats. Defender for Endpoint leverages Microsoft and third-party threat intelligence to identify threat actor tactics, techniques and procedures (TTPs) and to generate alerts when these artifacts are present in internally collected telemetry.
- **Microsoft Defender for Office 365** protects against email threats such as malicious links and attachments. Organisations can use it to protect Microsoft Exchange environments against broad, volume-based, known attacks. Defender for Office 365 offers capabilities for correlating attack patterns with known threat actor TTPs so security analysts can identify campaigns and mitigate them. The technology integrates capabilities for helping security teams identify, prioritise and investigate threats across the Office 365 environment. Inline incident response and automation capabilities allow security teams to quickly address detected threats and remediate compromised systems.
- **Microsoft Defender for Identity** helps organizations detect and respond to identity-based risks in cloud-based Azure Active Directory environments. It can be used to monitor users, entity behaviour and activities, and to protect user identities and credentials in Active Directory. Defender for Identity monitors on-premises Active Directory signals to detect and investigate compromised identities, credential misuse and potentially malicious insider actions. Defender for Identity offers user profile analytics and security reporting capabilities, so organisations have a better understanding of their attack surface.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides cloud security posture management and threat protection for workloads across Azure, AWS, GCP and on-premises. It helps assess and strengthen the security configuration of your cloud resources, manage compliance with critical industry and regulatory standards, as well as detect and respond to vulnerabilities and threats in the cloud or on-premises. It strengthens the security posture of cloud resources and provides the tools needed to harden resources, protect against cyberattacks and streamline security management.

Microsoft Defender for Cloud Apps is a cloud access security broker that works across multiple cloud environments including virtual machines, containers, databases and the internet of things. It helps organisations protect against threats to and from cloud apps and services by enabling discovery of all authorised and unauthorised cloud apps. It ensures that cloud apps are compliant with internal policy and industry/regulatory requirements by, among other things, enabling continuous monitoring of new and risky cloud apps.

The natively integrated capabilities in Microsoft 365 Defender and Microsoft Defender for Cloud enable comprehensive proactive and post-breach defences across Microsoft and third-party environments.



For example:

Defender for Office 365 provides proactive defence by detecting phishing emails and testing attachments to verify if it they are harmful – before they hit inboxes.

In the case of credential theft, **Defender for Identity** can spot attempts to misuse user credentials to elevate privileges or move laterally in a compromised network.

If a user opens a malicious attachment, **Defender for Endpoint** detects and blocks any malware that might be downloaded on the user device before it connects to the corporate network.

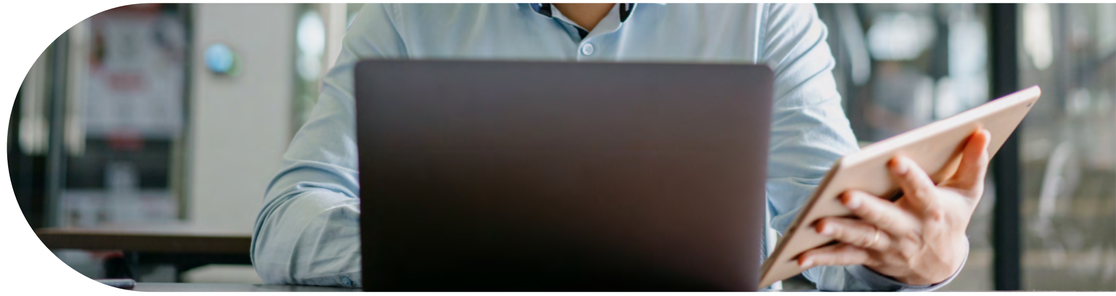
When an attacker uses a stolen identity to move laterally and tries to exfiltrate data from a cloud environment, **Defender for Cloud** apps can spot and stop the threat.

Integration for end-to-end visibility

Integrating Microsoft Sentinel with Microsoft's XDR solutions keeps incidents across endpoint and cloud environments bidirectionally synchronized and available in a way that enables rapid detection, analysis and automated response. For example, security teams can quickly verify if a threat they might have detected in an on-premises system is also present in their cloud infrastructure, or if a threat actor might have moved laterally from an on-premises environment to a cloud asset. Bidirectional synchronisation also means that when the status of a security alert changes in Microsoft Sentinel, it automatically changes in the Microsoft XDR environment.

The combination of Microsoft Sentinel and XDR enables better threat hunting across the enterprise. SecOps analysts can look at hot data in XDR and compare it against 10 years or more of SIEM information to determine, for instance, if they might have been previously breached. They can write one query and have it executed in both solutions to search for signs of lateral movement and malware persistence, or determine the full scope of a security incident.

Importantly, integrating the two platforms allows security teams to augment XDR telemetry with rich, real-time threat intelligence from Microsoft security researchers and third-party partners. By comparing external threat intelligence data with internal telemetry, SecOps analysts can quickly identity if threat actor activities and artifacts observed in the wild are present inside the organisation.



A clearer picture

A broader attack surface requires CISOs and their teams to continuously improve their ability to protect, detect and respond to threats. Layering Microsoft XDR telemetry from endpoints, email, apps, identities and cloud resources with cloud-native SIEM can help SecOps teams mitigate threats effectively, reduce the time it takes to detect and respond to attacks and minimise costly downtime from system disruptions caused by security incidents.

Learn more about how integrated threat protection can help stop breaches across your entire organisation.

Microsoft Security