Microsoft Security

Protecting the digital estate:

An integrated approach for increased SOC efficiency

Today's complex IT environments require a more efficient, streamlined and integrated approach for the Security Operations Centre.

Contents

Key takeaways from this paper

An increasingly sophisticated and complex attack landscape makes it more challenging for SOCs to keep pace

Integrating XDR and SIEM systems increases security effectiveness and efficiency across the entire enterprise

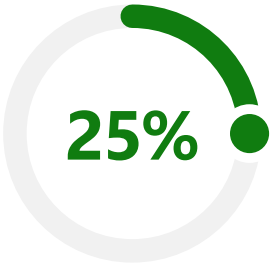
Automation and AI are critical components of the security tool kit, because they can **proactively detect and remediate threats**, freeing up Security Operation resources

A cloud-native security approach improves performance and scale for today's hybrid IT environments

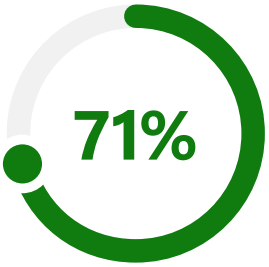
Introduction

Security teams are still feeling the impact of the sudden shift to remote work. CEOs are mandating improved user experiences to accommodate extended work-from-home policies, while at the same time asking CISOs to upgrade IT security to boost resiliency, according to the CIO Pandemic Business Impact Survey.

Meanwhile, threats are constant, and constantly evolving. According to the Microsoft Digital Defense Report, threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets. Terranova Security's 2020 Phishing Benchmark Global Report found that 25% of North American employees clicked on a link in a phishing simulation, and 71% of those employees also gave away their passwords – an indication that even the most common attacks continue to grow more sophisticated. Also, modern "kill chains" often contain a series of low-fidelity signals that are difficult, if not impossible, to manually detect and mitigate amidst the massive volumes of data the modern security operations centre (SOC) is tasked with monitoring. As threats increase, it's hard for overburdened SOC teams to keep up.



of North American employees clicked on a link in a phishing simulation.

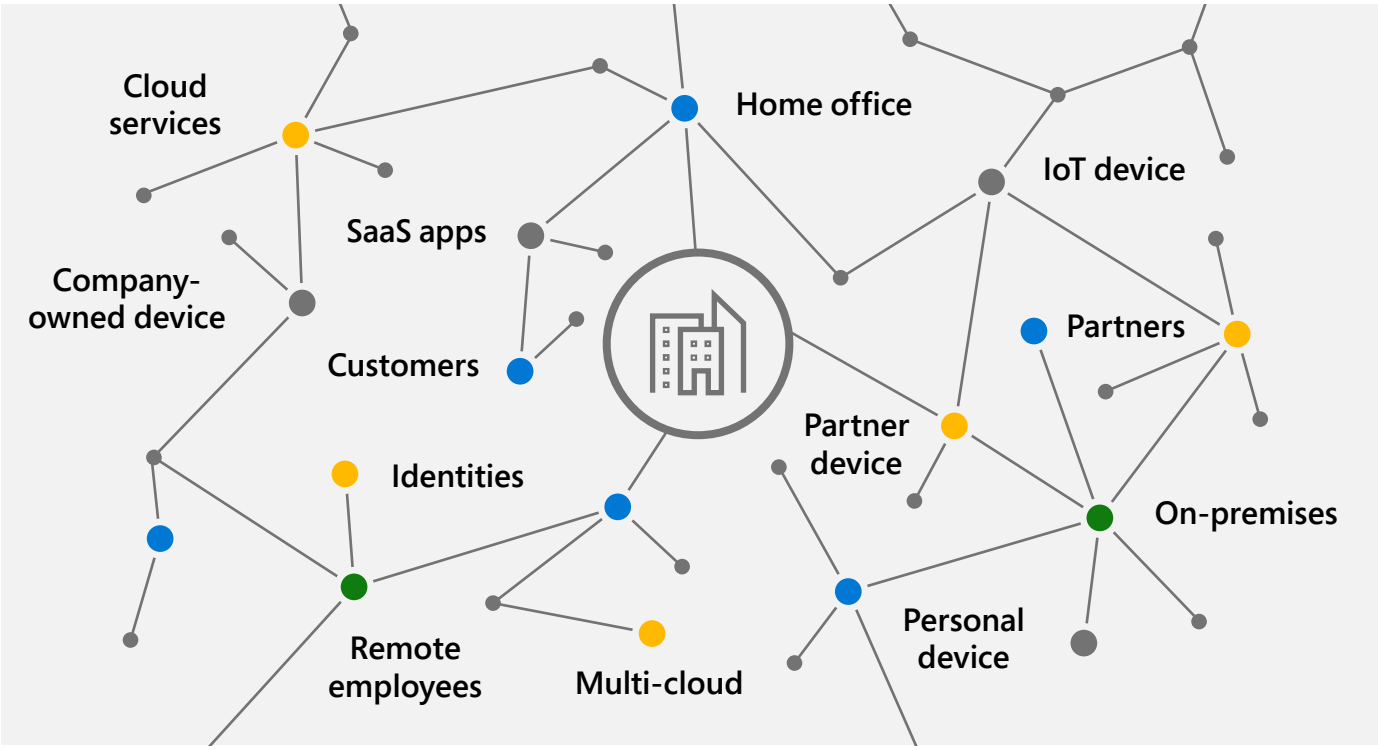


of those employees also gave away their passwords.

Today's patchwork of security tools provides pockets of protection but makes it difficult to integrate the breadth of security signals spanning the enterprise. As a result, it's hard for Security Operations teams to gain an enterprise-wide view of the entire kill chain – which explains why breaches can take months or longer to discover without the right security controls. Once attackers are inside and undetected, the damage can escalate quickly.

Allocating more resources to fill the gaps is not the answer, since finding enough skilled security professionals is an ongoing challenge. That leaves security teams stretched thin.

The expanding digital estate is difficult to manage and protect



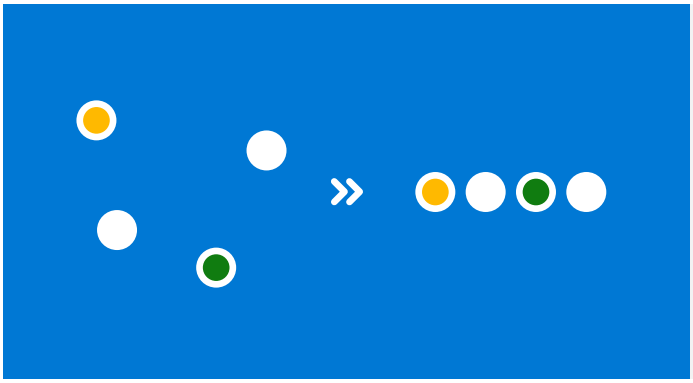
While the scope of today's security challenges may seem overwhelming at times, there's cause for optimism for CISOs looking to improve the efficiency and effectiveness of their security operations. The answer lies in an integrated, end-to-end approach to threat protection that will help SOCs:

- **Stop attacks before they happen** by reducing the attack surface and eliminating persistent threats.
- **Detect threats across domains** by integrating threat data for rapid and complete response.
- **Free up security team resources** with tools that can proactively hunt for sophisticated attacks across domains.

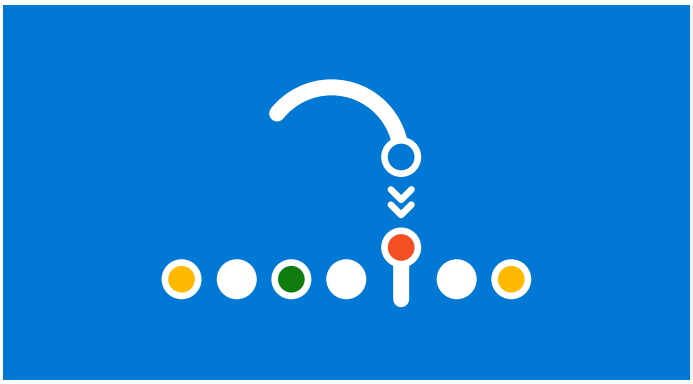
This approach is enabled by integrating extended detection and response (XDR) solutions with cloud-native SIEM systems and applying artificial intelligence (AI) and automation capabilities to help your SOC become more predictive, proactive and preventive against attacks across the enterprise.

The shift to integrated threat protection

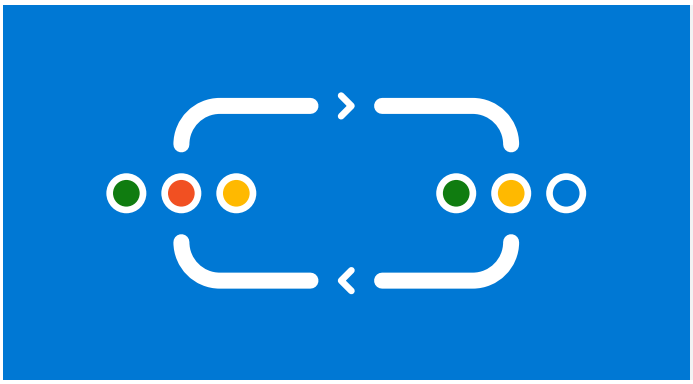
An integrated approach can help a SOC in three important ways:



Reduced complexity by consolidating tools to help streamline security while also strengthening your security posture.



Automated detection and correlation of alerts and pieces of data into manageable incidents.

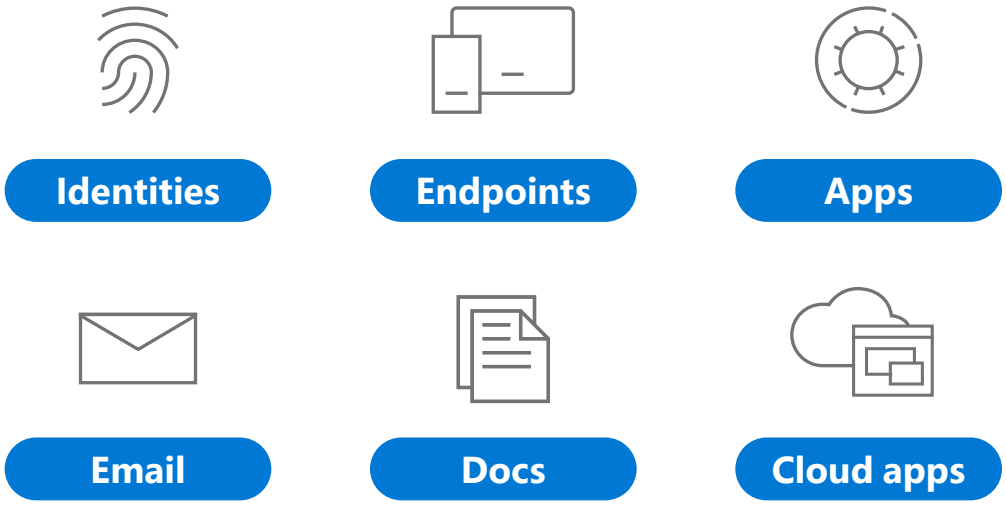


Automated “self-healing” capabilities, which give time back to SOC teams for threat hunting.

A cloud-native approach to threat protection provides the performance, scale and visibility required to take in all types of threats – to users, apps, data, devices and infrastructure – found across hybrid and multi-cloud environments. And it applies AI and automation capabilities to help SOC teams prioritise which threats are the most important. IDG's 2020 Security Priorities study found that 53% of organisations have launched or are piloting cloud-based SIEM solutions.

Integrated threat protection is critical because bad actors don't respect perimeters; they'll exploit any vulnerability they can find in devices, apps and users themselves. When they discover or create an opening, they'll use it as a starting point to move laterally until they find their target, often in the form of sensitive systems or data that they can take hostage or exfiltrate.

Attackers seek vulnerabilities across the organisation



For example, nation-state actor BISMUTH has been able to go largely undetected by taking advantage of low-priority alerts caused by cryptocurrency miners. Their goal: To establish continuous monitoring and espionage in order to exfiltrate useful information.

This level of sophistication and complexity is both staggering and alarming. That's why it's critical to align XDR and SIEM to correlate alerts, prioritise the biggest threats and coordinate action across the enterprise. Ultimately, these solutions provide SecOps efficiency and reduce the risk of costly data breaches. For example, integrating XDR and SIEM arms Security Operations teams with more context than ever, thanks to built-in AI capabilities. In addition, automation proactively deploys and enhances prevention techniques, while enabling teams to focus on more sophisticated tasks like threat hunting and creating custom tools that reduce response time.

Consider, for example, that a single, low-level signal may not garner much attention from a traditional SIEM. Using AI, however, a cloud-native SIEM could automatically compare that signal to signals from other sources throughout the organisation, correlating across multiple datasets to find multi-stage attacks.

The system would then normalise, analyse and correlate the data, while providing context about how the attack entered the infrastructure, along with the timeline of how it spread. This lets SOC teams visualise the breach – from a single console – and effectively address it.

By connecting the dots across on-premises systems and multiple clouds, SOCs gain critical visibility to help stop more attacks before they happen.

Strengthening security posture with intelligent, integrated threat protection

Microsoft Defender offers integrated, comprehensive security with extended detection and response (XDR) and built-in automation and AI capabilities. The product suite arms your SOC teams with the right functionality to stop even the most sophisticated, cross-domain attacks across Microsoft, third-party and custom-built apps.

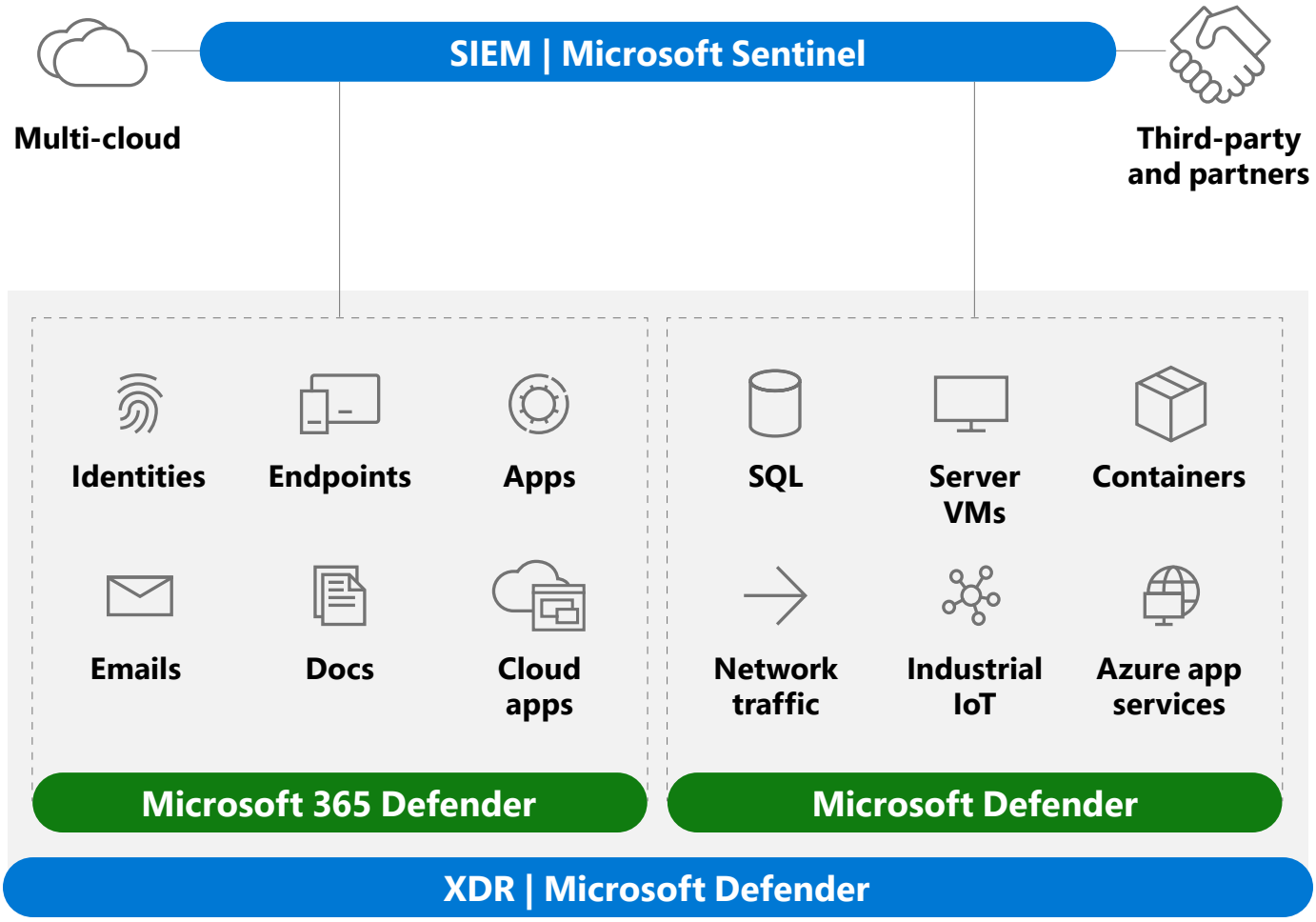
Microsoft 365 Defender addresses end-user and on-premises security across the Microsoft 365 ecosystem by securing identities, endpoints, email and applications. It uses artificial intelligence tools to consolidate alerts and remediate simple attacks.

Microsoft Defender addresses cloud and hybrid platform security by protecting dynamic and virtual services – including databases, virtual machines, containers and Internet of Things networks. It employs a visual console that illuminates secure and unsecure cloud resources. In addition, it includes protection for on-premises and multi-cloud SQL servers, as well virtual machines in third-party clouds.

Microsoft has connected Microsoft Defender with its cloud-native SIEM system, Microsoft Sentinel, to provide a comprehensive multi-cloud solution.

Microsoft Sentinel collates and integrates threat data from all security resources across the enterprise, including firewalls and existing tools, as well as third-party systems and platforms. Microsoft Sentinel helps reduce noise from legitimate events with built-in machine learning and knowledge based on the analysis of trillions of signals daily.

Stay ahead of attackers with a unified SecOps experience



Learn more about integrated threat protection with SIEM and XDR.

Take the next step

The attack landscape, coupled with the ongoing need for secure remote work, calls for a modern, integrated approach to threat protection. End-to-end integration empowers your organisation's defenders by putting the right tools and intelligence in the hands of the right people. With integrated SIEM and XDR solutions, defenders are armed with all the context and automation needed to stop even the most sophisticated, cross-domain attacks.

As a next step, consider an assessment to get a full picture of your security posture. Microsoft Secure Score helps CISOs understand their organisation's current state. It makes recommendations to improve threat protection and establishes key performance indicators to help enterprises monitor their progress.

Learn more about integrated threat protection with SIEM and XDR.

Microsoft

© 2022 Microsoft Corporation. All rights reserved. This document is provided 'as is'. Information and views expressed in this document, including URLs 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.