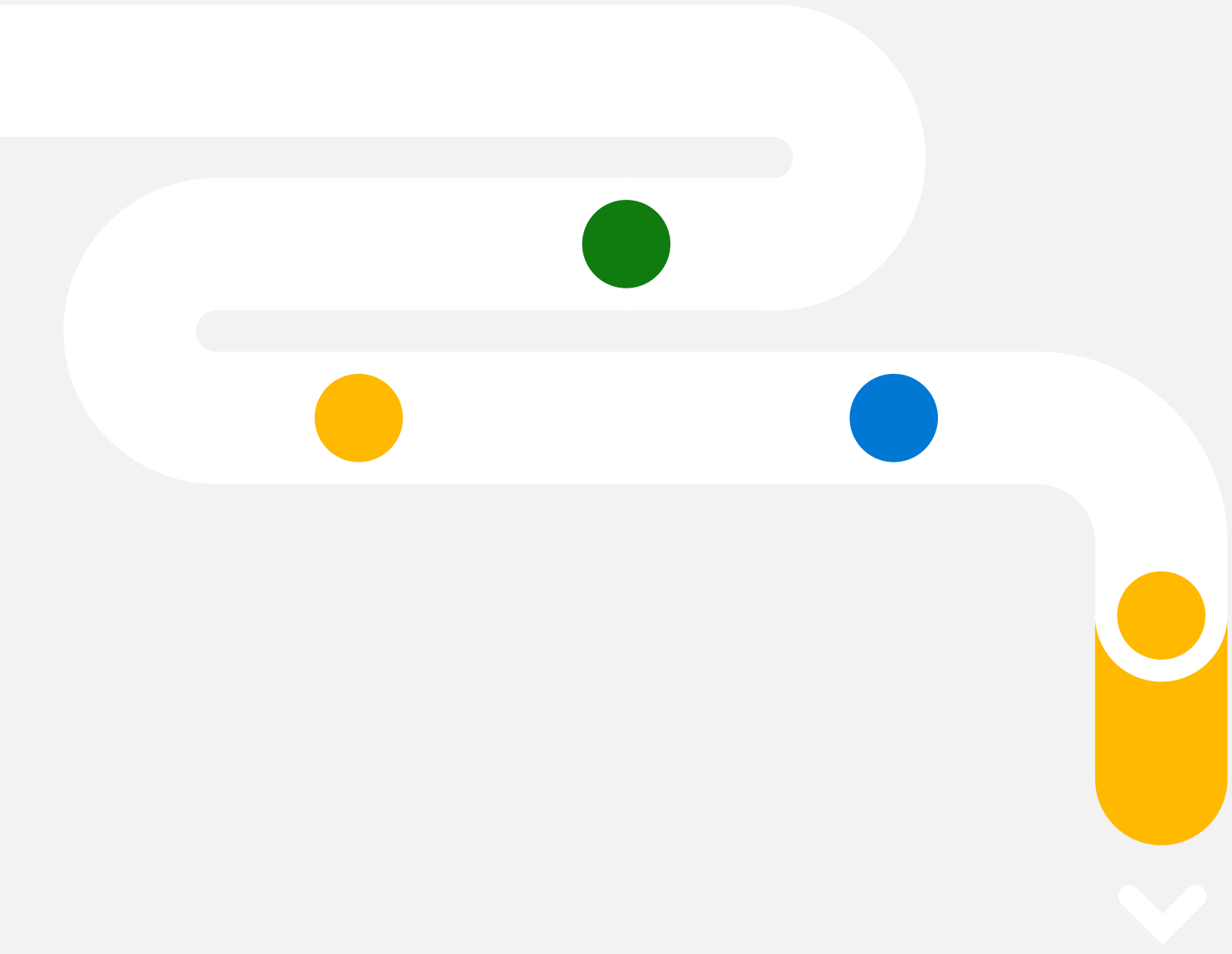
Microsoft Security

How a consolidated security stack can reduce your risks and costs

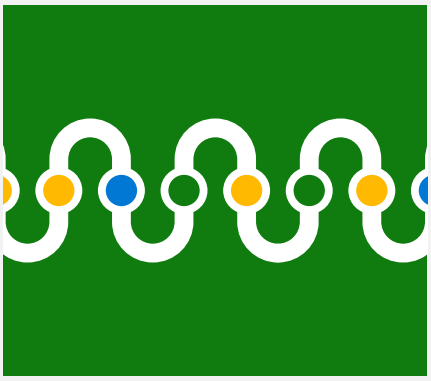


Contents

Introduction

Even before the global pandemic introduced new security challenges to organizations, CISOs were dealing with a complex security landscape. Technology stacks for security have evolved into a jumbled mix of point solutions as security teams address multiple threat types from a variety of endpoints, apps, services, and networks. As CISOs pivot to prioritize around post-COVID-19 security strategies, it's a good time to revisit ways to streamline and strengthen security environments. Rather than cobbling together individual point solutions, consider a more integrated approach that provides comprehensive protection and enhanced capabilities for today's workers, with tools that take advantage of intelligence and automation capabilities to simplify management and reduce risk.

Consolidate security with a more cost-effective solution



Deliver unified end-user experiences for greater security

Reduce cyber risk with integrated, best-in-class protection

Consolidate security with a more cost-effective solution

As the security landscape evolves, with new threats cropping up almost daily, security teams face a heavy burden to keep pace. In some cases, technology has added to the challenge instead of mitigating it. A complex mix of siloed, single-point security solutions are time-consuming to deploy and inevitably lead to a patchwork of consoles and reports that are difficult to monitor and manage across the enterprise. In a study by Forrester Consulting, 59% of organizations acknowledged the challenge of correlating security alerts from disparate technologies to detect threats. "Reducing the number of disparate security point solutions that must interact with each other—particularly older, legacy ones—brings complexity down to a manageable level," the study notes[1].

In addition to reducing complexity, a consolidated solution can improve your overall security posture by filling gaps created by a lack of integration across the technology stack. For example, a separate study by Forrester Consulting found that organizations deploying Microsoft Defender for Office 365 P2, which provides a holistic, integrated approach to security, reduced the likelihood of a security breach by 60% and decreased the time required for investigation and remediation of security incidents by 89%.

[1]"Security Through Simplicity," Forrester Consulting, December 2018.

60% decrease in time required for investigation and remediation of security incidents

89% reduction in the likelihood of a security breach

Another benefit of vendor consolidation is improved cost management—a critical consideration in these extraordinary times, when every dollar counts. In a recent study by CIO, 75% of IT leaders expect IT budgets to remain flat or decrease in the next 12 months, and 45% expect to be spending more time on cost control and expense management in the months ahead.

Customer perspective

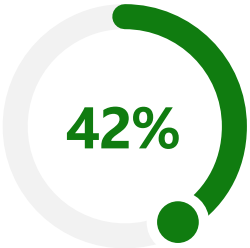
"We recognized the best-in-suite value of Microsoft 365 E5 not just from a security perspective.... We realized we could get everything we needed with one license. If we had used separate vendors, it would absolutely have cost more, in addition to the complexity of managing multiple products and contracts."

— Doug Howell, Director of IT, The Little Potato Company

Deliver unified end-user experiences for greater security

CISOs have long known that security is only as strong as individual users across the organization. More than two-thirds (68%) of organizations in a recent survey by Cybersecurity Insiders believe they are vulnerable to insider attack, and less than half (42%) said their ability to monitor, detect, and respond to insider threats is very or extremely effective.

of organizations in a recent survey by Cybersecurity Insiders believe they are vulnerable to insider attack



said their ability to monitor, detect, and respond to insider threats is very or extremely effective.

Insider risk includes the unintentional leaks that may occur due to overly complex security tools and policies. The shift to remote work makes it imperative to provide easy-to-use tools for securely accessing data, apps, and systems from any location.

Modern security tools provide strong, secure access to applications while removing the traditional friction points that can inhibit productivity. A seamless single sign-on experience provides quick access from anywhere to the dozens of applications users need daily to perform their job duties. And it can save users an average of 10 minutes per week and save the organization $2.9 million annually, according to Forrester Consulting.

Multi Factor Authentication (MFA) is one proven method to address the dreaded password reuse issue. It's well known that users often reuse passwords across multiple accounts, which flies in the face of good security hygiene and also puts an organization at greater risk of a security breach. Passwords were tied to 80% of breaches in 2019, according to the 2020 Verizon Data Breach Investigations Report.

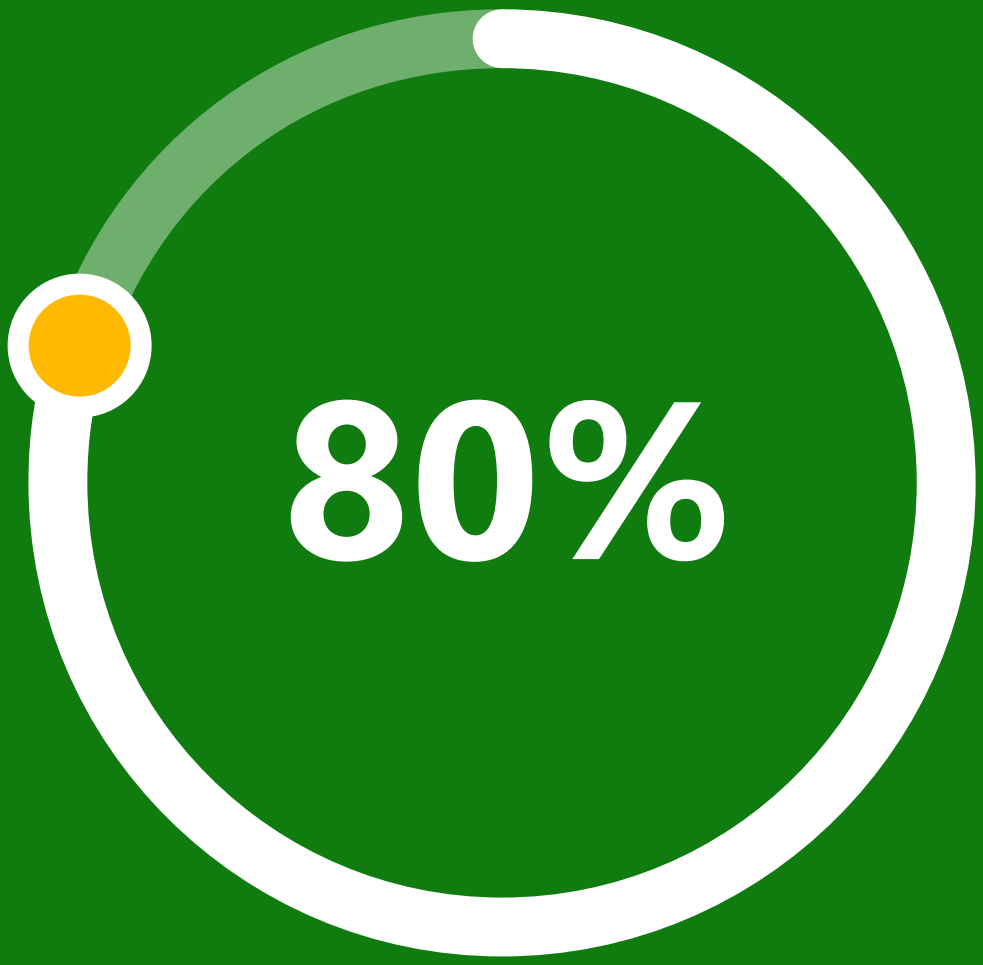
Another option that's gaining favor is to remove the password entirely. Passwordless methods such as Microsoft Authenticator, Windows Hello, and FIDO2 security keys provide a simpler and more secure authentication experience across the web and on mobile devices. Based on the FIDO2 standard, these methods enable remote users to authenticate easily and securely without requiring a password. Windows Hello uses biometrics, providing a convenient option that is three times faster than using a password.

MFA and passwordless access are just two examples that represent a broader shift from perimiter-based defense to identity-based management and a Zero Trust security model. Using identity as the control plane lets organizations treat every access request as untrusted until the user and device are fully verified.

Customer perspective

"If you make security hard, people may work around it. With Microsoft 365, we get native capabilities, visibility into our operational environment, and simplicity for all employees."

— Simon Hodgkinson, Group Chief Information Security Officer, BP



of breaches in 2019 were tied to passwords

Reduce cyber risk with integrated, best-in-class protection

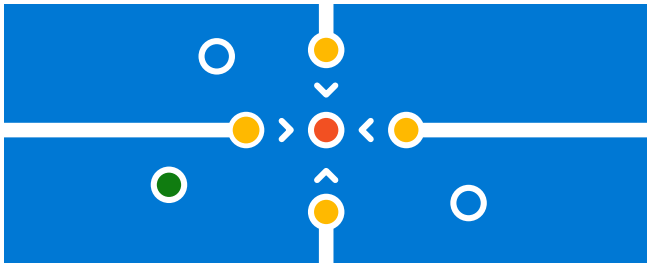
Poor security posture is often rooted in complexity. Security teams have historically struggled to keep up with threats and signals across a patchwork of poorly integrated solutions that fail to cover the breadth of workloads, clouds, and devices that businesses run on. A consolidated tool set can improve your organization's overall security posture by reducing complexity and integrating protection across the enterprise. An integrated solution will also help security teams more effectively deploy and leverage automation and AI technologies to further improve protection.

Automation is critical for modern threat protection, in part because it can help correlate, consolidate, and analyze an often-unwieldy volume of alerts for anomalous behavior, particularly now that much of the workforce is outside the office. For example, the AI and automation capabilities in Microsoft 365 Defender reduce alert triage and correlation by 50x on average, empowering teams to more quickly detect and respond to threats.

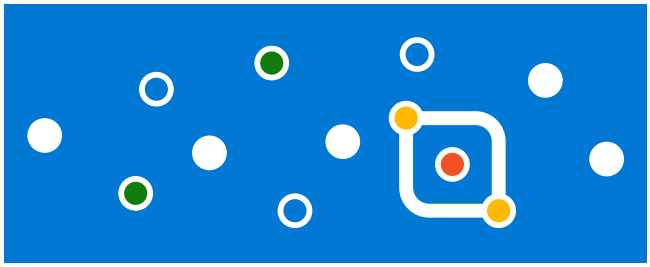
The cloud has given rise to a new generation of modern security tools that simplify the defender experience by combining signals and automating responses to catch threats that would otherwise go unchecked. The most important emerging tools are cloud-native Security Information & Event Management (SIEM) and Extended Detection and Response (XDR). Most vendors only offer one or the other.

Microsoft offers a unique approach that empowers security professionals with both cloud-native SIEM and XDR tools from a single vendor. This brings a new level of integration that gives defenders the best of both worlds: end-to-end visibility across all of their resources and intelligent alerts built with a deep understanding of individual resources, enhanced with human and machine intelligence.

Microsoft 365 Defender provides best-in-class real-world detection according to a MITRE ATT&CK evaluation, which found that the Microsoft solution provides:



Nearly 100% complete coverage across emails and docs, endpoints, identities, and apps across kill-chain stages.



Leading out-of-box visibility into attacker activities to dramatically reduce manual work for the security operations center.

Microsoft SIEM and XDR solutions can help reduce "alert fatigue" significantly—as much as 90% in some Microsoft evaluations.

Customer perspective

"Going with a best-of-platform security approach from Microsoft was the right choice because of the rapid innovation across the platform."

— Erik Passchier, Global Head of IT Infrastructure, Rabobank

Microsoft

Summary

A point-solution approach to security may provide access to the latest and greatest security tools, but it has also created levels of complexity that can actually hinder your team's ability to defend against constantly evolving threats. Now, however, organizations no longer have to make the difficult tradeoff between best-ofbreed and integrated solutions. A best-of-platform approach to consolidation reduces complexity and costs while improving visibility across the organization. Better visibility, supported by AI and automation capabilities, makes it easier to identify vulnerabilities and quickly mitigate threats to reduce risk. Strong, seamless, end-to-end security will also provide a better experience for the workforce. Microsoft has created a suite of tools and services that help protect your organization against cyberthreats with built-in automation and intelligence. It combines best-of-breed capabilities with end-to-end integration to provide strong security while enabling employees to remain productive. Gartner has named Microsoft a Leader in five Magic Quadrants, including Access Management, Unified Endpoint Management (UEM) tools, and Endpoint Protection Platforms[2].

Customer perspective

"The analysts were saying that when you combined the Microsoft security products you get better visibility than with point solutions. Since that was the exact problem I was facing, it convinced me to try the Microsoft platform."

— Eric Walters, Department Manager, Cybersecurity & IT Infrastructure, Burns & McDonnell

Learn more