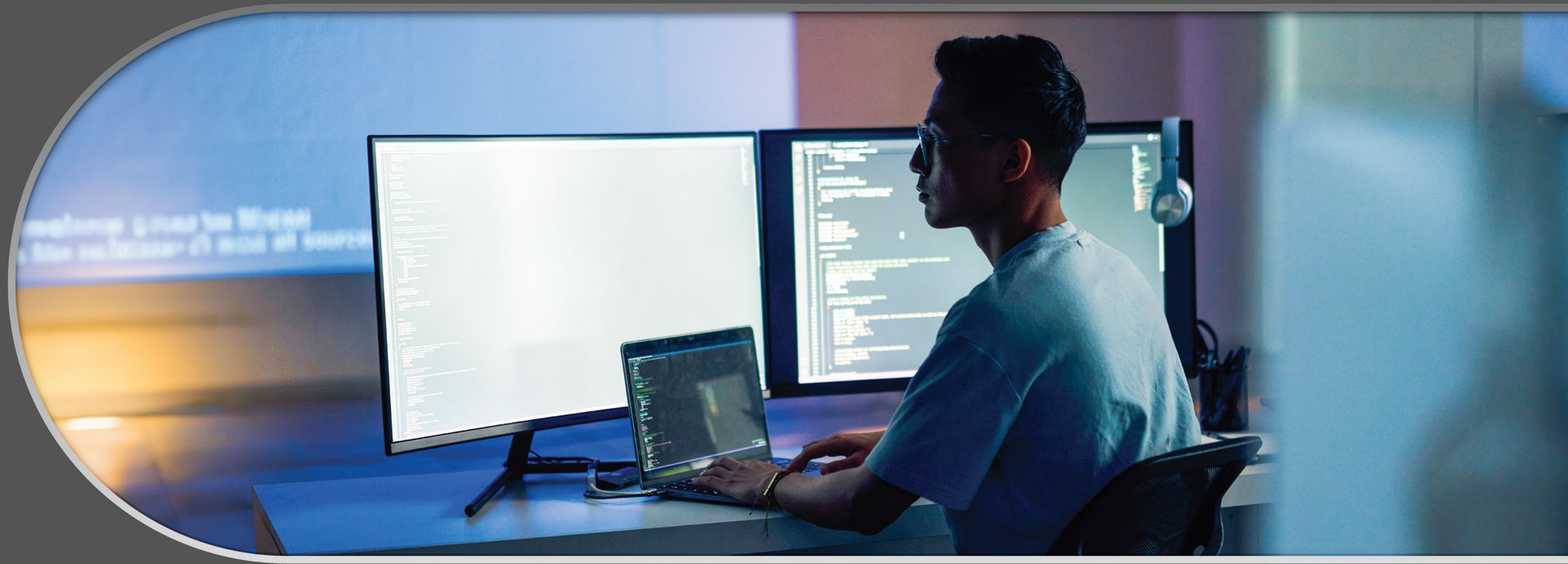
Microsoft Security

3 Reasons to Ditch the Point-Solution Approach

A CISO's guide to more proactive and efficient security operations



Contents

Executive summary

The evolving cyberthreat landscape, expanding digital estates, and cost constraints have made it difficult for Chief Information Security Officers (CISOs) to choose between two strategies: using best-of-breed tools to address the most pressing challenges, or prioritizing tooling that focuses on integrating with your existing portfolio while making it easier to adopt new technology in the future. For a long time, the best-of-breed strategy was the default strategy for CISOs. However, cyberthreats and tooling have changed. Organizations have accumulated an unwieldy array of security tools, impeding the proactive work security teams desperately need to do. The next generation of tools interoperate, speeding security teams' work so they can spend more time on prevention.

In this cyberthreat climate, an approach that prioritizes disparate, best-of-breed point solutions makes it harder to reach your goals. A unified approach can improve your overall security and help you get ahead of emerging cyberthreats.

Reason 1

Complexity traps security operation (SecOps) teams in a reactive spiral.

Too many tools keep analysts scrambling to get ahead. They end up spending too much time detecting and remediating threats and too little time on proactive measures.

Reason 2

Siloed best-of-breed tools impede a full view of the cyberthreat landscape.

A lack of visibility into cyberthreats across your entire digital estate allows sophisticated cyberattackers to evade detection.

Reason 3

Proactive security requires speed that siloed tools can't provide.

Fragmented security tools make it harder for SecOps teams to respond quickly to and protect against risks such as ransomware attacks and business email compromise (BEC).

The case for a unified approach.

The best way to make proactive security possible is to ditch your legacy point solutions and replace them with an industry-leading, unified security operations platform. By combining the capabilities of extended detection and response (XDR), security information and event management (SIEM), exposure management, and generative cybersecurity AI, the unified SecOps platform empowers security teams to address current incidents quickly, so they have time to focus on fortifying your organization against new and emerging cyberthreats.

The power of one: Why cybersecurity needs a paradigm shift

As a CISO, the responsibility for preventing a breach ultimately rests with you and your strategic choices. Over the years, CISOs have had to frequently make quick decisions to adapt to the rapidly changing cyberthreat landscape. This has led many organizations to accumulate a diverse portfolio of tools that address specific types of threats that were being prioritized at the moment. Unfortunately, this approach has resulted in another, equally pressing problem: security teams are saddled with a sprawling set of fractured tools, making their work more difficult.

A CISO's objective is always to protect the organization by adopting the most robust technology and strategies while controlling costs. This can be difficult to achieve when you're confronted with a high-stakes tug of war between competing priorities. To name just a few:

- Finding an organization-wide solution versus solutions focused on specific areas.
- Reacting to a current cyberthreat versus taking on a broader security modernization effort that will increase efficiency and resilience in the long run.
- Getting consensus within your organization versus enforcing adoption of what's needed.

A recent Microsoft survey of data security professionals illustrated just how paradoxical the question can be. Of the respondents, 80% agreed or strongly agreed that a comprehensive data security platform with integrated solutions is superior to using multiple best-of-breed solutions that have to be manually integrated and managed. Yet 55% of those same participants said they preferred the best solution available over fully integrated solutions.[1] Unraveling this contradiction requires CISOs to redefine "best-of-breed" for the current cyberthreat climate. If your multiple, disparate solutions create gaps that elevate your risk exposure while making it more difficult to detect an active attack, is it truly better?

This e-book explores the top three reasons why a best-of-breed approach can keep you from achieving your organization's security goals, and how a unified approach can help you overcome those challenges.

Complexity traps SecOps teams in a reactive spiral

It can be challenging to manage the overload analysts experience from a daily deluge of cyberthreats—especially with the ongoing shortage of skilled cybersecurity talent. To further complicate the situation, SecOps teams face multiples of everything: incident queues, lists of assets, response playbooks, and tools.

A fragmented view of threats means teams must switch between numerous portals to stitch alerts together. Among the many alerts, some may be redundant. But which ones? And which ones are the highest priority? Without fully connected tools, these are questions that take a lot of time and effort that could be better used on higher-value work.

Complexity forces SecOps into a reactive posture rather than a proactive one. They spend a great deal of time trying to distinguish false positives from real alerts in their queue, which requires a lot of skill and makes it time-consuming to uncover the full scope of an incident. They also don't have the time or capability to look for advanced persistent threats that evade detection. Too little time is spent on preventative measures because sifting through alerts, weeding out those that are redundant or of low-value, identifying high-priority threats, then correlating them all into incidents is a labor-intensive process. Understanding the full scope of an incident so that it can be fully remediated and prevented in the future simply takes too much time and manual work. **Through no fault of their own, SecOps teams end up fending off cyberthreats in the moment without reducing the risk of future cyberattacks.**

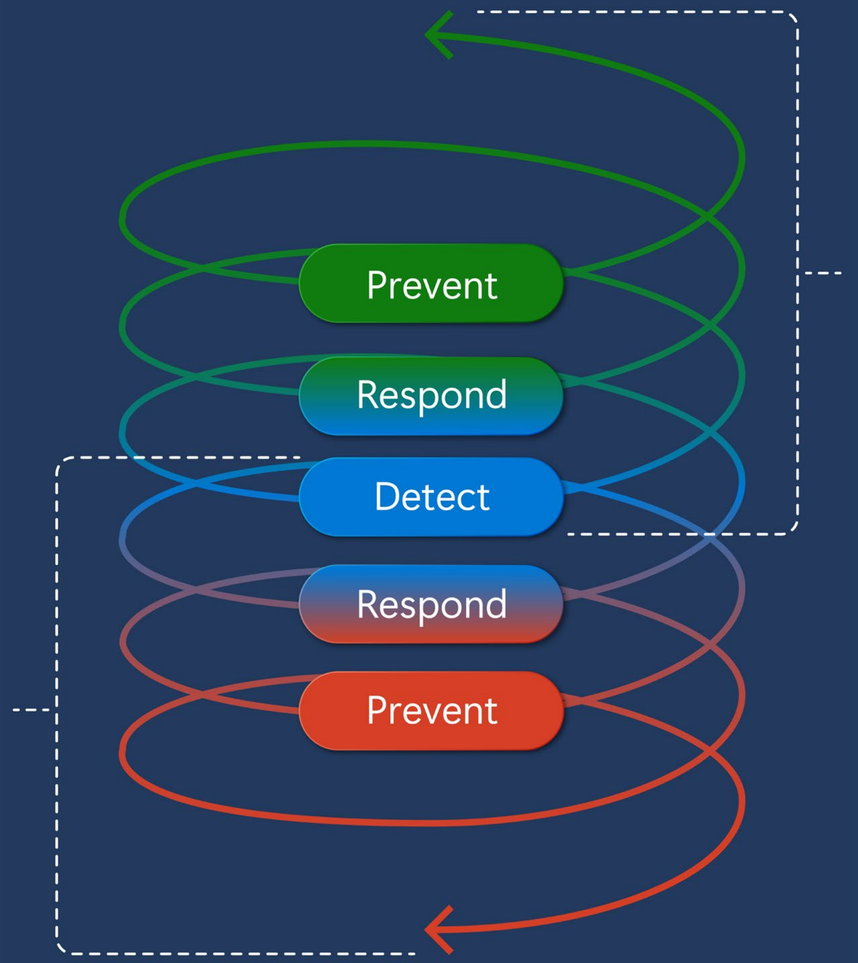
CISOs everywhere need to place a heavy emphasis on prevention to keep organizations safe in the current cyberthreat climate. But the need to keep up as cyberthreats become more sophisticated and dynamic is what prompted the accumulation of so many point solutions in the first place. With so many tools to manage, the rapid evolution of cyberattackers' tactics, and ever-growing digital estates, security teams can't get ahead of their incident queues. The lack of unity traps them in a reactive cycle when it could be a proactive one.

Point-solution approach

Detect › Repeatedly switch between portals to:
- Sift and weed out low-value alerts manually.
- Stitch alerts into prioritized incidents.
- Detect in-progress attacks across the entire cyberattack chain.

Respond › Scramble to:
- Recognize complex attacks spanning multiple layers.
- Respond quickly and thoroughly.
- React in time to avoid a serious breach.

Prevent › Lack the visibility or time to:
- Analyze all signals the SOC receives every day.
- Reduce vulnerabilities across the digital estate.
- Implement policies that prevent repeat attacks.



Unified approach

Prevent › Regain time to:
- Proactively manage your security posture.
- Engage in threat hunting and guard against repeat attacks.
- Model attack paths to prevent access to critical assets.

Respond › Use advanced capabilities to:
- Automate low-value tasks and resolve incidents quickly.
- Use AI speed to avoid a serious breach.
- Give junior analysts step-by-step remediation guidance.

Detect › Use unified dashboard and end-to-end visibility to:
- Automatically disrupt in-progress attacks.
- Streamline triage across multicloud, multiplatform environments.
- Uplevel SOC efficiency and reduce analyst overwhelm.

Siloed best-of-breed tools impede a full view of the cyberthreat landscape

The digital estate you're charged with protecting likely includes multiple clouds and platforms, widely distributed endpoints, workloads, apps, services, and human and nonhuman identities. All CISOs face the same problem: getting visibility into all of it. That's the key to understanding your true cyberthreat exposure, and it can be extremely difficult to achieve using disjointed tools.

Coverage gaps and poorly connected tools that aren't able to effectively share data can also impede your ability to understand the full scope of a cyberattack. Cyberattackers weave a complex web that spans multiple security layers across the entire cyberattack chain. For example, a cyberattack may start with a phishing email, gain access to an individual's device, and move to a cloud app before trying to exfiltrate data. Too many alerts, incidents, and asset lists spread across multiple portals and dashboards make it harder to gain an end-to-end view across these domains, allowing cyberthreat actors to more easily evade your defenses.

The result is that most organizations have significant exposure to cyberthreats that they don't know about or struggle to effectively address. And when a cyberattack does occur, they often don't have the insights necessary to help prevent a similar attack from happening again. Cyberattackers work hard to find gaps in your defenses and cover their tracks. A best-of-breed approach can create security silos and overworked teams—exactly the conditions cyberattackers need to thrive. Without a unified approach to ingesting and analyzing anomalies across multicloud and hybrid environments—including endpoints, cloud workloads, apps, and services—SecOps teams constantly find themselves playing catchup. They:

- **Struggle to prevent repeat attacks.** Without visibility into full cyberattack chains, it's difficult for security teams to understand them and implement policies to prevent them.
- **Struggle to detect in-progress attacks.** When teams spend most of their time correlating alerts between tools, they're often unable to act in time to prevent a serious breach.
- **Struggle to investigate and respond efficiently.** When there are visibility gaps, analysts must fill them manually, consuming valuable time.

Proactive security requires speed that siloed tools can't provide

To take a proactive stance against modern cyberthreats, you need speed. Without it, you won't have sufficient resilience against modern cyberthreats. In today's cyberthreat climate:

72 minutes is the median time it takes for an attacker to access your private data if you engage with a phishing email.[2]

One hour and 42 minutes is the median time for an attacker to begin moving laterally within your corporate network after a device is compromised.[2]

With a best-of-breed approach, you miss out on opportunities that one end-to-end platform can provide. Siloed tools force analysts to manually triage alerts and fill the gaps. Not only is this difficult to do fast enough to stop in-progress attacks, but it also requires years of experience to do effectively. Junior analysts often struggle to quickly gain the necessary speed and acumen.

And the entire team ends up spending too much time on low-value tasks, such as triaging alerts across multiple tools, instead of the high-impact work, like threat hunting, that yields results. This is a critical disadvantage when both resources and security talent pools fall short.

Organizations also lose time because of the lack of coordination between security operations center (SOC) teams and security teams that are using disparate tools. An endpoint detection and response (EDR) solution can help bridge the gap between those responding to cyberthreats and those defining policies for endpoints. XDR extends insights beyond endpoints to identities, email, and cloud apps, and an integrated SIEM solution provides a single portal for all detection and response. Without a unified platform that integrates these tools, much of the coordination is complex and manual because teams have to use different portals to review lists of assets and incident queues. In this way, a best-of-breed approach results in inefficiencies that can be costly.

Finally, having an overly diverse portfolio of tools also threatens to keep organizations from taking advantage of one of the latest security innovations: generative cybersecurity AI. Generative AI automates investigation and response and offers step-by-step recommendations that help accelerate incident detection and response. But in order to work effectively, this technology needs the data and threat intelligence connectivity of a unified platform.

With a unified platform, teams get the insights necessary to prevent, detect, and disrupt cyberthreats such as ransomware and BEC attacks across emails, endpoints, identities, workloads, and cloud apps in near-real time. In the current cyberthreat climate, that immediacy is a must-have.

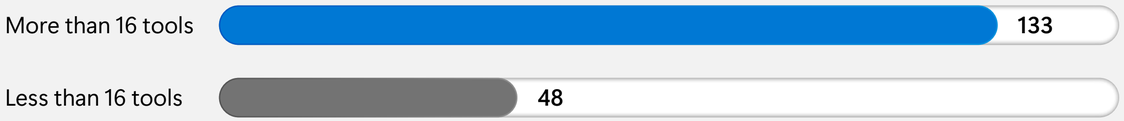
The case for a unified approach

Having more tools may be creating a false sense of security among security decision makers. According to a Microsoft survey, those who use more than 16 tools are more confident in their security posture: 61% say they are confident compared to 56% of those with fewer tools.[1] **However, those with more tools also experienced more data security incidents in the past year with an average of 133 incidents for those with more than 16 tools compared to 48 incidents for those with fewer tools.[1]**

Fortunately, an increasing number of CISOs are realizing that having a greater number of best-of-breed tools is not improving their security. Instead, analysts need more intuitive workflows that allow them to get ahead of their queues and spend more time adapting your defenses to the specific needs of your business. According to Gartner®, "By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric design practices to minimize cybersecurity-induced friction and maximize control adoption."[3]

Confidence in security posture

Data security incidents per year



"By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric design practices to minimize cybersecurity-induced friction and maximize control adoption."[3]

Gartner®

A strategic shift to a unified approach can move your organization out of the reactive spiral and into a proactive one.

One Gartner® senior analyst further said that, "CISOs must review past cybersecurity incidents to identify major sources of cybersecurity-induced friction and determine where they can ease the burden for employees through more human-centric controls or retire controls that add friction without meaningfully reducing risk."[3]

A strategic shift to a unified approach can move your organization out of the reactive spiral and into a proactive one. This means that analysts can spend more time on remediation instead of triage, and dedicate ever more of their bandwidth to prevention. This not only improves your security posture, but it can also save as much as USD1.6 million annually in vendor consolidation.[4]

With technology that automates routine tasks and lightens analysts' workloads, the unified approach provides visibility into cyberthreat signals, threat intelligence, and tooling that allows SecOps teams to disrupt cyberthreats in near-real time. Automatic attack disruption significantly enhances a security team's ability to get ahead of serious cyberthreats. The advantages of having automatic attack disruption for your SecOps teams are measurable:

3 minutes is the average time it takes to disrupt a ransomware attack with attack disruption.[2]

92% of targeted devices have been saved by attack disruption in ransomware disruption cases, involving both remote and local encryption.[2]

With a holistic strategy, security teams have the breathing room to reclaim more time for proactive work.

It’s time to streamline your security operations

The pressures CISOs and their SecOps teams face today were the inspiration behind the Microsoft unified SecOps platform. By providing end-to-end visibility and bringing together the full capabilities of SIEM, XDR, exposure management, generative AI, and threat intelligence, it empowers SecOps teams with:

- Intuitive features that work across use cases, such as stopping phishing, malware, and ransomware, detecting insider threats, and protecting privileged accounts.
- Step-by-step instructions created by generative AI that are built into the analyst experience to speed their work and uplevel their skills.
- Automation to help analysts investigate effectively, respond quickly, and focus on high-value tasks.
- The option to add on the powerful identity protection and response capabilities of Microsoft Entra ID.
- The cost benefits of consolidating vendors and tools.

It’s time to stop accumulating separate tools and dashboards and embrace the power of one. One integrated platform combines best-of-breed tooling with the convenience of a unified solution to empower your team to take a proactive approach to security.

Prepare for the future with a unified approach.

Explore your deployment options:

Learn about Microsoft's unified security operations platform

Source:
[1] Microsoft Data Security Index: Trends, insights, and strategies to secure data, Microsoft, October 2023.
[2] Microsoft releases its second edition of Cyber Signals tracking ransomware's new business model, Microsoft Stories Asia, August 23, 2022.
[3] Gartner Identifies the Top Cybersecurity Trends for 2023: Security Leaders Must Pivot to a Human-Centric Approach to Establish an Effective Cybersecurity Program. Gartner, April 12, 2023.
[4] The Total Economic Impact™ Of Microsoft SIEM And XDR, a commissioned study by Forrester Consulting, August 2022. Results are for a composite organization based on interviewed customers.