




Do what matters

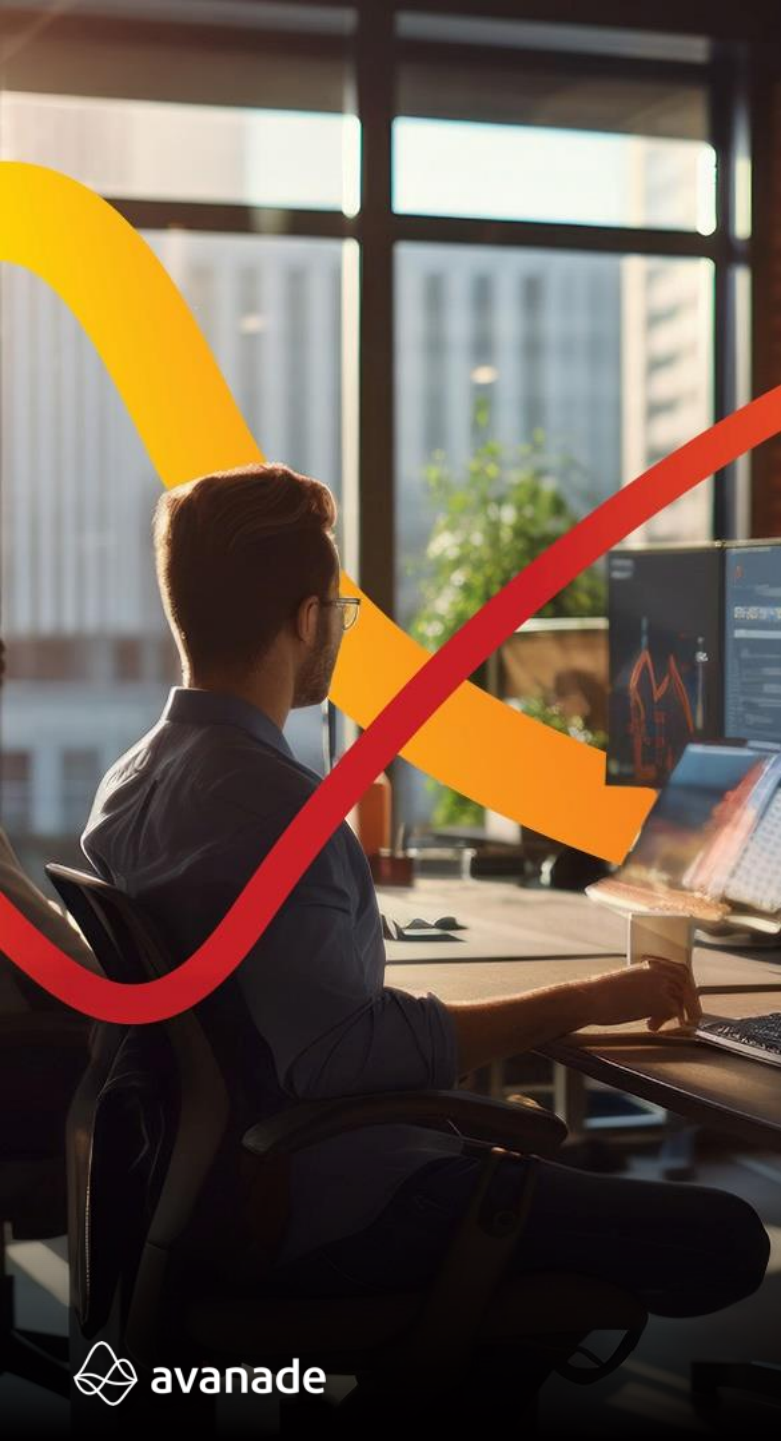
Unify threat protection

Stay ahead of evolving threats

A man with a beard and glasses is looking at a computer screen. The screen displays lines of code, including "Auto-Selecting P...", "Auto-Selecting IP...", "Pyl Monitor: 2.0.0", "Press F2 to Show...", and "Keyboard Error". The background is dark with some blurred lights.

“ 83% of businesses say that complex, interconnected cyber risks are emerging more rapidly, and 77% agree that risks are more difficult to detect and manage. ”

– Accenture Risk Study, 2024



Organizations are struggling to keep pace with fast-moving cyber threats

Too much noise

Massive quantities of data moving at high speed, coupled with a huge rate of alerts, is overwhelming security teams and making it difficult to validate and prioritize threats.

Talent shortages

A global shortage of skilled security resources, alongside overworked and overstretched security teams, means that organizations aren't able to respond rapidly to complicated attacks.

Complexity

Organizations have too many security tools with complex integration. This fragmented market of point solutions and lack of integrated experience drive inefficiencies – and impede the creation of a robust security platform.

To stay ahead of shifting threats, organizations need to simplify their security management

Many organizations still rely on traditional approaches to threat hunting that utilize a range of advanced tools and highly skilled teams.

But this approach comes with challenges. The talent shortage and fragmentation across security tooling, coupled with the storm of threat-related data, is leaving organizations scrambling to stay on top of the rapidly evolving threat landscape – and creating vulnerabilities ripe for breach.

50,000

The number of threat alerts that organizations experience annually¹

81%

of security executives agree that staying ahead of attackers is a constant battle, and the cost is unsustainable.²

80%

C-Suite executives believe their organizations lack sufficient protection against cyberattacks in this digital era.

Sources:

1. Forrester, "[The Total Economic Impact™ Of Microsoft SIEM And XDR](#)"
2. Accenture, "[State of Cybersecurity Resilience](#)"

The power of unified threat protection for your operations

Avanade's unique approach to threat protection integrates Copilot for Security alongside Microsoft Sentinel and Defender, utilizing built-in AI to improve detection and response capabilities.

Forrester's Total Economic Impact™ (TEI) study shows that firms deploying Microsoft Sentinel and Defender together realize:

~1.6M

annual savings from vendor consolidation

The Microsoft SIEM and XDR investment enables organizations to reduce the cost of their prior SIEM (\$560,000), the associated on-premises infrastructure (over \$360,000), XDR point solutions (\$192,000) and the ongoing labor cost to manage these (\$480,000).*

75%

improved efficiency and productivity

An integrated approach to security threat investigation and response makes workflows more efficient for security professionals – who no longer need to use multiple tools to identify threats – while security automation features further enhances response workflows.

60%

reduction in risk of material breach

With more efficient security investigation and response workflows, improved security response automation and the increased ability to protect all computing environments, organizations can reduce the risk of breaches – an annual impact of \$1.6 million saved.*

*Based on savings from a composite organization

Source: Forrester, "[The Total Economic Impact™ Of Microsoft SIEM And XDR](#)," August 2022.



65%

reduction in the amount of time it takes for a security professional to investigate threats



91%

faster onboarding of new security professionals across various tools

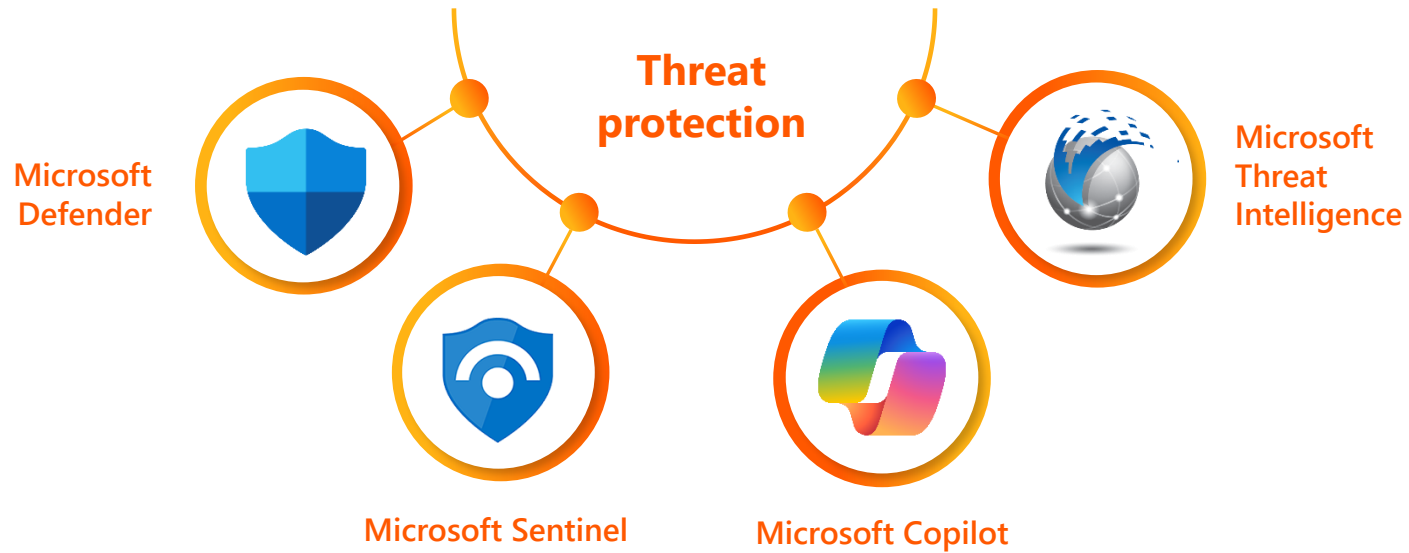
Source: Forrester, "[The Total Economic Impact™ Of Microsoft SIEM And XDR](#)," August 2022,




The power of unified threat protection for your people


88%

less time analysts spend responding to each threat – down from days to hours



 **Optimize and reduce costs**

- Maximize security investments and simplify security management
- Leverage automation and efficient threat models to reduce security costs
- Drive up to 60% annual savings from vendor consolidation

 **Address the talent gap**

- Enhance your team's productivity and overcome the shortage of skilled resources for SOC monitoring
- Drive up to 65% reduction in investigative time

 **Build cyber resilience**

- Secure your cloud and on-premise environments as you scale your business
- Drive up to a 60% reduction in risk of material breach

 **Rapidly respond to security incidents**

- Investigate and respond to incidents faster through improved visibility
- Enable up to 88% reduction in response time to attacks

Stay protected with the full power of Microsoft Security

Why Avanade for threat protection?



1,000+ Avanade security practitioners worldwide

- #1 for Security certifications – Accenture / Avanade have the highest number of Microsoft Security certified people – 2x the next Global SI
- We have the scale, reach and expertise to help you achieve your goals faster and more efficiently



First-mover learnings and insights

- We are deeply aligned with Microsoft, partnering to help design and build new technology and as early clients to experiment with and deploy Microsoft capabilities within Avanade
- As 1 of 5 members of the Microsoft Design Advisory Council Member for Copilot for Security, we actively work with Microsoft to shape Copilot for Security and are one of the first organizations to use it within the enterprise – enabling us to share these learnings with our clients



Market-ready solutions and services, fueled by AI

- We are the first Microsoft partner to combine Microsoft Sentinel, Defender for Endpoint and Copilot for Security into one unified solution
- Our quick start approach delivers value within weeks by rapidly onboarding all three key components to achieve end-to-end, real-time visibility into threats in the multi-cloud environment
- Expand capabilities with fully managed operational model and functional Copilots via our Managed Extended Detection and Response Service (MXDR)



The leading Microsoft Security Services partner

- Avanade holds 4 Microsoft Security specializations:
 - Threat Protection
 - Cloud Security
 - Identity and Access Management
 - Information Protection Governance
- We are 1 of 4 firms worldwide named a Microsoft MxDR partner



Recognized for our commitment to exceptional outcomes

- IDC Leader in the Cybersecurity Worldwide MarketScape 2024
- Two-time winner of Microsoft's Zero Trust Champion Award
- Winner of the MISA Diversity in Security Award



Next steps

To help you get started on your threat protection journey, we begin with a cyber portfolio evaluation (CPE) exercise that focuses on your operational threat protection readiness.

1

Plan and design

1 week

Hold CPO workshop to understand the current state, use cases and requirements and identify and prioritize deliverables across Sentinel, Defender and Copilot for Security deployments.

2

Build, test, pilot and deploy

5-7 weeks

Rapidly deploy all integrated components, including rules, playbooks and agreed use cases. Perform validation and testing activities and generate ROI and migration roadmap with three key capabilities for quick wins highlighted.

3

Threat protection optimization

Transition to ops team or perform workshop and analysis activities to map the value of additional XDR components to further threat protection optimization.

Ready to start evolving your approach to threat protection?

Schedule your follow up discussion today.