avanade

Future Fit Managed Extended Detection and Response

Protect against advanced cyberthreats
with a Microsoft powered MXDR service

Microsoft Security

Table of Contents

03
How effective is your current security model?

04
Managed Extended Detection and Response Approach

06
Unify your security tools

08
Build cyber resilience

09
Case study: Healthcare provider

10
Why Avanade

How effective is your current security model?

Strengthen your security posture to defend against constantly evolving security threats

In recent years, it has become harder to keep up with emerging threats. With rapid digital transformation, a shortage of skilled security resources, and the exponential increase in sophisticated cyberattacks, security teams everywhere are facing immense pressure. It is no longer enough to just focus on preventing security breaches. Organizations must find ways to stay ahead of threats and keep their environment secure.

Continuous security monitoring, detection, and response

Avanade blends the power of people, process, and automation with Managed Extended Detection and Response (MXDR) so organizations can meet these security challenges head-on. MXDR extends across the Microsoft ecosystem, on-premises, and the cloud, detecting and responding to advanced cyberattacks throughout an organization's IT infrastructure.

Stay ahead of threats

Find and resolve hidden threats before they cause damage or loss.

Unify your security tools

Integrate Microsoft tools with Avanade MXDR for comprehensive security operations center (SOC) monitoring.

Build cyber resilience

Reduce downtime, exposure, and risks.

75%
of workers will continue to split time between home and traditional office locations by 2026.[1]

57%
of organizations claim they are impacted by the global cybersecurity skills shortage.[2]

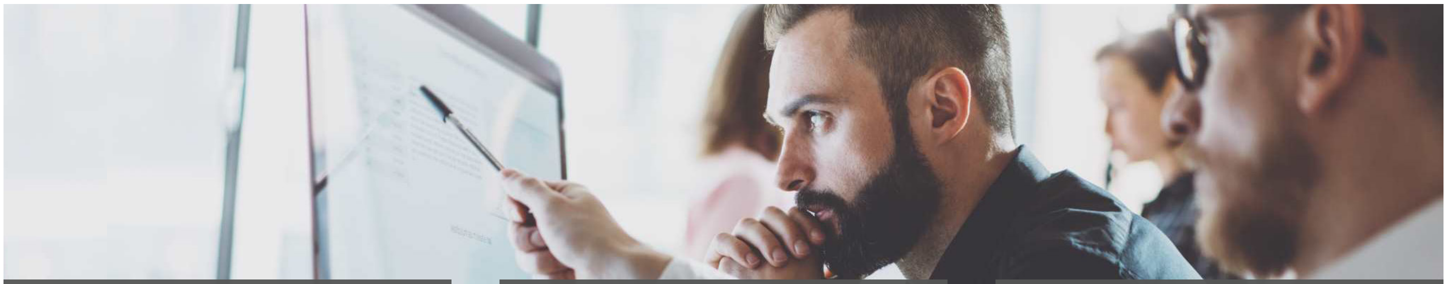
82%
of security leaders have been surprised by a security event, incident, or breach that evaded a control they thought was in place.[3]

Stay ahead of threats

Detect and stop attacks before they happen

To defend your organization against cyberattacks, you need to prepare for threats and ensure continuity in the face of disruption. You can stay ahead of threats with Avanade's managed detection and response service with Microsoft Sentinel, which helps you proactively find and mitigate cyberthreats before they disrupt your business while limiting the impact of security incidents that occur. And you can prioritize threats through automation and risk assessment capacity and support. With continual monitoring, minimize the time from detection to response – automate alert triage and threat remediation faster than traditional Security Incident Event Monitoring (SIEM).

Avanade's approach to Managed Security Services



Manage

End-to-end management of Microsoft Security product portfolio leveraging our cost-effective and highly certified and skilled Microsoft Security capabilities.

Defend

Maximize the Microsoft Security product portfolio capabilities to defend your environment for internal and external threats.

Evolve

Recognize maximum ROI and gain continuous value from your Microsoft Security investment through platform evolution.

Managed Extended Detection and Response (MXDR) Services

Future-fit and cost-effective security monitoring and managed extended detection response at scale across endpoints, identities, email, and the cloud. Rapidly deploy MXDR and migrate from legacy SIEM and MDR solutions quickly and smoothly into our MXDR services.

Next Generation Cloud Security

Transform cloud security into a fast, frictionless, cost-effective, and proactive function that deploys policy to mitigate the risk of misconfiguration as well as deploying advanced defenses to protect from external attack across any cloud or hybrid environment.

Identity and Access Management

End-to-end services for identity and access management (IAM) provide the latest automation and security capabilities to protect your human, service, and privilege identities from advance threats, while also optimizing and strengthening your IAM processes and defenses.

Data Protection

Robust and end-to-end data protection services protect structured and unstructured via holistic data classification, data loss prevention, and threat protection capabilities for Microsoft 365 E3 and E5. We help you maximize your investment in Microsoft products and realize improved defenses through full adoption of your E3 and E5.

Secure Applications and Platforms

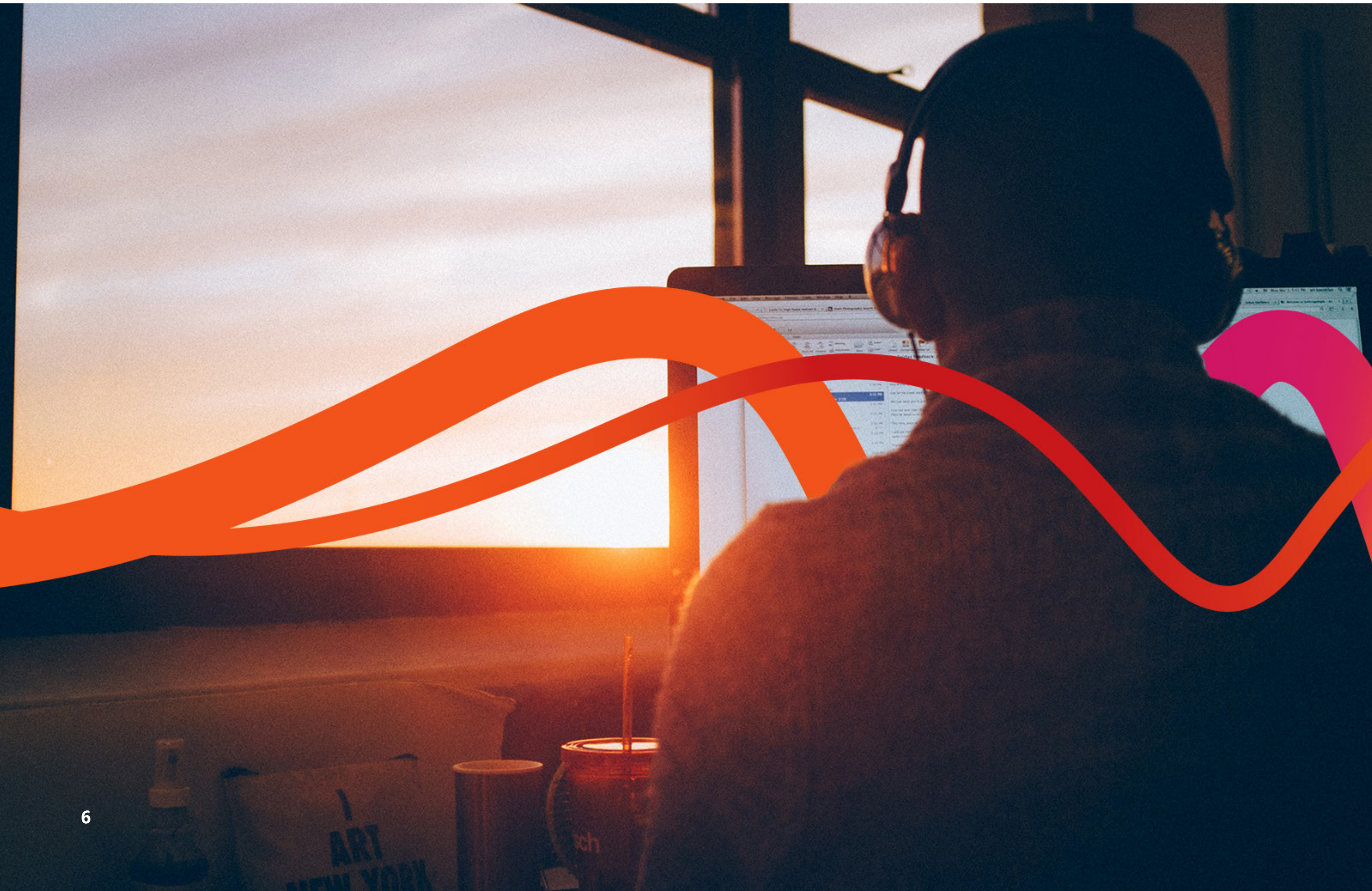
Shift your security left with application and platform security services that proactively identify and mitgate risk prior to production deployments and actively defend your critical applications and platforms from advanced threats.

Unify your security tools

Leverage the best of Microsoft security capabilities

Many organizations have implemented multiple security tools, resulting in increased complexity and risk. It is hard for businesses to know where to look for threats and what to prioritize. The abundance of disparate tools results in alert fatigue and management overheads, leaving organizations vulnerable to threats and attacks.

Onboard and connect services to Microsoft Sentinel to protect, detect, and respond to threats for the entire Microsoft platform and extended security landscape. You can gain cost-effective security monitoring at scale using Microsoft Sentinel SIEM to deploy advanced analytics and automate threat responses. Strengthen your security posture across your entire IT infrastructure and gain a comprehensive and holistic view of your security. And enhance your critical capabilities with governance monitoring, incident response, and threat intelligence applied with machine learning and AI.



Avanade’s end-to-end, fully orchestrated capabilities

Threat Intelligence

Provides insight into threats impacting similar industries and geographies and adversary Tools, Techniques, and Procedures (TTPs).

Advanced Security Analytics

Process and analyze log data from security controls, network infrastructure, and endpoints to identify events of interest.

Threat Monitoring

Perform 24/7 alert monitoring and analysis, identifying and escalating incidents.

Threat Hunting

Identify compromises through targeted, proactive discovery across the kill chain, identifying known and unknown threats.

User Behavior Analytics

Apply machine learning to identify anomalous user activity to support threat identification.

Endpoint Detection & Response

Detect, analyze, and remove threats from endpoints, such as servers and laptops, leveraging Avanade-provided or client EDR solutions.

Incident Response

Perform incident triage, prioritization, and response to notable events (e.g., disable user accounts, quarantine hosts, etc.).

Tailored Use Cases & Playbooks

Develop and continuously refine rules, triggers, and response playbooks, applying threat hunter methodology and feedback.

Microsoft powered MXDR

- Optimize your SOC using predictive threat intelligence, automated remediation, and power of the cloud.
- Provide a comprehensive and holistic view of your security using Microsoft Threat Protection stack and on-premises log collection sources.
- Manage security using Managed Detection and Response including threat detection, threat hunting, threat analysis and remediation, and playbook automation.

Build cyber resilience

Shift from reactive to proactive security

Security teams everywhere are understaffed and overwhelmed. Many organizations don't have the skills, resources, and scale to ensure comprehensive around-the-clock security. Security teams are struggling to validate and prioritize high volumes of notifications and false positives because they are understaffed with certified security professionals, causing reactive responses and important security concerns to be missed.

Shift to an adaptive security model that rapidly prevents, detects, and remediates security threats to build cyber resilience. Modernize your SOC and augment your SOC team's capability with automated investigation and response so they can prioritize other tasks. All while accelerating your threat analysis and reducing human error through innovations in intelligent systems. With Avanade MXDR, you can gain additional security and visibility for recently deployed services and infrastructure with a key focus on protecting endpoints from ransomware. And develop and continuously refine rules, triggers, and response playbooks, applying threat hunter methodology and feedback.

Case study: Healthcare provider

Situation

A healthcare provider had a maturing platform and outdated tools that did not adequately address its security and operational needs.

Result

Avanade implemented a set of digital identity, application security, and threat protection services integrated into an SOC and SIEM solution. By providing this service, it allowed the client to focus on its core business by offloading the monitoring, incident management, and maintenance of attack surface reduction controls.

Solution

Avanade built a SIEM and Security Orchestration Automation Response solution powered by Microsoft Sentinel. This extended the current Defender for Cloud monitoring of alerts using playbooks, workbooks, and over a dozen analytical rule sets with defined thresholds for alerts and custom reports.

Why Avanade

At Avanade, we're the experts for helping you secure your Microsoft and hybrid IT ecosystems. Our security services provide a holistic approach through advisory, implementation, and managed services.

Recognized as the Zero Trust Champion winner at the Microsoft Security Excellence Awards, we provide proven methodologies, deep expertise, and leading-edge technology.

20+ years
of experience helping clients secure their organizations

45% of Global 500 companies
are clients

Thousands of
security risks mitigated per year

1 million+
endpoints managed

30 million+
digital identities managed

Winner of Microsoft Global Partner of the Year 17 times

Global Security Center of Excellence
bringing global expertise to our clients

Security analytics that handle billions of events daily

Running some of the largest SIEM Deployments in the world

- State-of-the-art MXDR capabilities across global SOC and 24/7 coverage
- Established Managed Security Services and outsourcing partner as an Azure and Microsoft 365 Defender Expert
- Advanced SOC services coverage with MXDR integration
- Powered by our parent Accenture Security – a Forrester MSS Quadrant Leader

Take the next step

Take the first step and book an Avanade Discovery Workshop. We will work with you to understand your business drivers, existing infrastructure, and processes to come up with a holistic assessment of your security landscape and risks. From there, we create a roadmap to help you realize your security vision over the long term.

Visit Avanade.com/security for more information

LEARN MORE

Find Avanade on the Microsoft Commercial Marketplace

READ MORE

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Global System Integrator (GSI) Award

Microsoft Security

Excellence Awards 2022

Microsoft Intelligent Security Association

WINNER

Avanade

Zero Trust Champion

[1] Top Network Practices to Support Hybrid Work | Gartner

[2] The Life of Cybersecurity Professionals | ESG Global, ISSA

[3] Security Leaders Peer Report | Business Wire

Microsoft Security

avanade