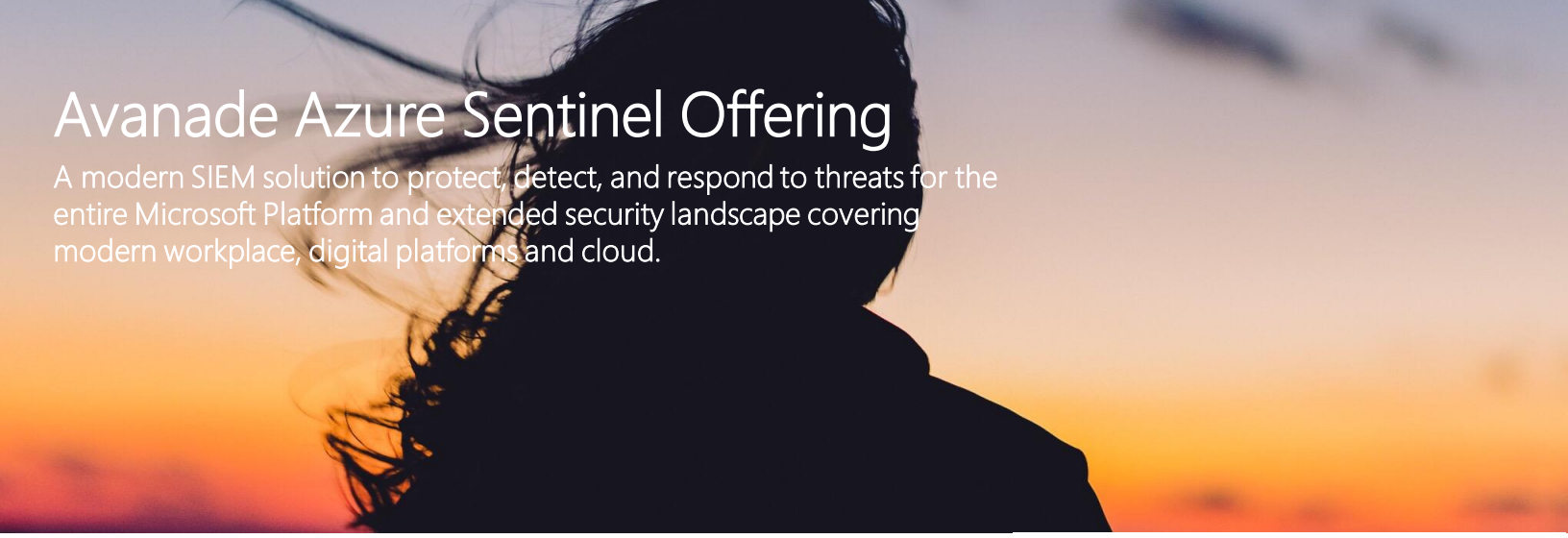


Avanade Azure Sentinel Offering

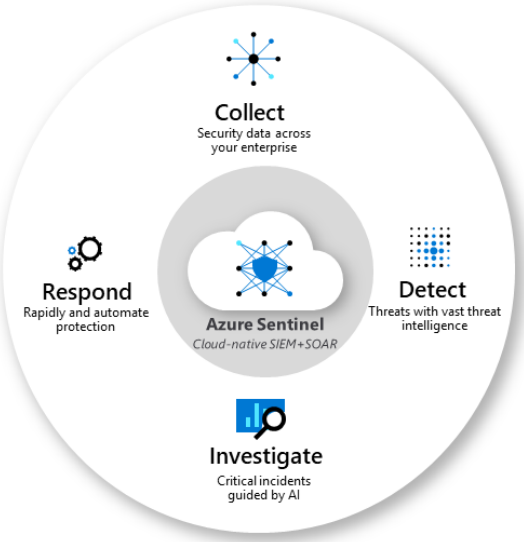
A modern SIEM solution to protect, detect, and respond to threats for the entire Microsoft Platform and extended security landscape covering modern workplace, digital platforms and cloud.

To truly defend your organization against cyber-attacks, you need to prepare for threats – both known and unknown – and ensure continuity in the face of disruption.

Security information and event management solutions built yesterday struggle to keep pace with today's challenges.

That's why Avanade uses – and helps customer use – Microsoft Azure Sentinel, a modern SIEM for entire Microsoft platform and extended security ecosystem covering modern workplace, digital platforms and cloud.

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting and threat response.



Why use Azure Sentinel?

- Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Implement in stages

- Define scope of work and build a minimum viable product (MVP)
- Integrate key Microsoft log sources and core infrastructure logs
- Monitor cyber activity through Security Operation Center (SOC)
- Automated threat management improves business continuity

Reduce alert fatigue by up to 90%

Security managed centrally

- One central location for reporting and alerting
- Visibility beyond the Microsoft stack
- Centralized threat intelligence providing earlier views on updated threats and recommended actions

Manage entire enterprise security centrally to save time

Quick ROI with Office 365

- Default connected Office 365 data
- Step-by-step guide to onboard quickly
- Implement rules, triggers and playbooks according to agreed upon use cases relevant for the client's business context
- Backed by Microsoft investment and innovation

Quick onboarding with free Office 365 data storage and analysis

 | www.avanade.com/security

avanade

Modern workplace and Azure security managed with Sentinel

Identity and Access Management

- Privileged Access Tier Model
- Analytics query on Tier 0, 1 & 2 security groups
- Playbook Logic App workflow for group membership changes alerts

Information Protection

- CASB: Microsoft Cloud App Security policies
- Cloud App Security alerts are sent to Sentinel as incidents
- Sentinel displays incidents in interactive graphical form to facilitate threat investigation

Threat Protection

- Third-party appliance data collection
- Analytics parses and queries Syslog to identify high severity attacks
- Playbook Logic App workflow to notify Security Operations about attacks
- Remediate immediate true positives related to remote working (Access, Malicious, External threats) & eliminate false positives.

Security Management

Our promise to you

Provide an end-to-end intelligent security solution

An offer to get you started

- Make security a business enabler
- Quick ROI and value realization
- Reducing the threat insights fatigue
- Deliver a more secure IT environment
- Enable a flexible, pay-as-you-go security solution
- Ensure proactive security management
- Take advantage of cloud services capabilities & scalability

Collect
- Visibility

Detect
- Analytics
- Hunting

Investigate
- Incidents

Respond
- Automation

How Avanade can get you started with Sentinel

- **Avanade can deliver a set of workshops, pilots and an engagement** based on our unique mix of business understanding in the security domain, deep Microsoft technology experience and our understanding of the client's environment.
- **Avanade can modernize the client's existing IT operations** by ensuring Azure Sentinel is optimized to provide client environment-specific, enterprise-wide insights, threat detection and intelligence capabilities.
- **Azure Sentinel can be set up to collect data across the PaaS and IaaS workloads**, detect & investigate threats and respond in a timely fashion.
- **Avanade can quickly deliver solutions** utilizing various Azure security monitoring technologies including Log Analytics, Kusto Query, Logic Apps, etc.
- **Avanade's Managed Security Service** brings top security talent, innovative technologies, and security-as-a-Service operating models, that help clients rapidly achieve operational resilience with scalable security and compliance operations

Why Avanade?

Microsoft Partner — Gold Security

Microsoft

Security Specialization

In designing and integrating the right Microsoft and third-party security solutions with a focus on security simplification without compromise

End-to-End Capabilities

Transform, evolve and secure the modern workplace via Evergreen Services along with cloud managed services.

250+ Active Clients

Across 25 countries powered by in-country and offshore capabilities

20/20 Microsoft Security Advisory of the Year

Leading partner in attaining MS-500 (Microsoft 365 Security Administration) & AZ-500 (Microsoft Azure Security Technologies)

 | www.avanade.com/security

avanade