AVERTIUM

AVERTIUM SOLUTIONS FOR MICROSOFT SECURITY

MDR FOR DEFENDER FOR ENDPOINT

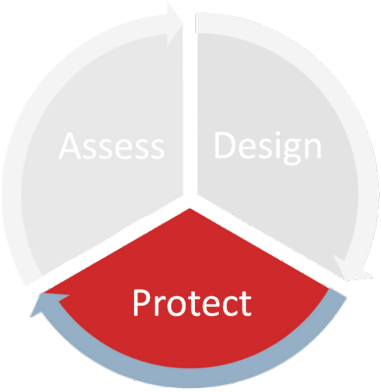
UNLOCK ADVANCED THREAT DETECTION

Avertium can help you maximize your Microsoft Security investment. We are an extension of your team, helping you both design your Microsoft Security strategy and put it into action. Our **Assess - Design - Protect** approach makes you more secure, compliant, and efficient.

- ✓ **MICROSOFT CERTIFIED:** Certified Avertium security professionals: Microsoft Security Operations Analyst, Azure Security Engineer Associates, and 365 Security Administration.
- ✓ **COMPREHENSIVE MICROSOFT XDR PROTECTION:** Identity, O365, Cloud Apps, and Endpoint.
- ✓ **24/7/365:** True 24/7/365 monitoring, management, and human response to security incidents.

Avertium can lead the implementation of Microsoft Defender for Endpoint and transition to **PROTECT** your security operations with a fully optimized MDR solution.

Avertium's MDR for Defender for Endpoint includes telemetry with Fusion Engine and the human element of highly skilled security professionals who provide monitoring, alerting, threat identification, incident management, and response. Avertium's Threat Response Team also provides custom intelligence and incident response expertise to ensure you are prepared for multiple scenarios beyond automation.



PROTECT

v /prəˈtekt/
24/7/365, fused defense operations that continually improve with vulnerability management, Microsoft integrations, threat intelligence, and reoccurring tuning and testing.

Avertium provides a more advanced MDR security solution utilizing Microsoft Defender for Endpoint, with the capability identify and neutralize threats able to elude common organizational security controls. This service adds experienced, high-skill-level analysts with a more comprehensive roster of innovative security tools at their disposal.

APPROACH

RESPONSE

- Fully managed Microsoft Defender for Endpoint: Configuration, deployment, and management
- 24/7/365 monitoring, management, and human response to incidents
- Investigation of events and triage of actionable alerts
- Enhanced analysis of events and alerts for trend detection

ACCOUNT TEAM

- Onboarding Manager
- Service Delivery Manager
- Threat Response Team

REPORTING

- Monthly touchpoints with SDM's
- Vulnerability Flash Notices and Threat Reports
- Aggregate relevant threats in a single feed, via OpenCTI

THREAT EXPOSURE

- Map rules to Microsoft Sentinel MITRE ATT&CK® framework analytics
- Tailored Threat Intelligence

FUSION ENGINE INTEGRATION

- Cyber fusion telemetry between Microsoft DFE and your other operations
- Threats flow from Sentinel to Fusion Engine, correlating with our Threat Intelligence Platform

CAPABILITIES

- Measurably enhanced coverage and confidence in security posture
- Real-time analytics and advanced correlation with two, US-based Cyber Fusion Centers
- 24/7/365 escalation of critical and high-severity security incidents
- Security framework and compliance aligned MDR
- Greater incident fidelity: reducing noise to isolate true positive alerts
- Reduced Total Cost of Ownership
- Threat Intelligence Reports and Flash Notice with in-depth analysis of threat actors, attack campaigns, and zero-day vulnerabilities
- Reduce alert fatigue and thus, reduce risk
- Incident triage and guided response through the dedicated Threat Response Team with isolated containment of high-risk incidents of attack and compromise

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection

Member of
Microsoft Intelligent Security Association
Microsoft

OUTCOMES

Combine Microsoft Defender for Endpoint with Avertium's Expertise to identify and neutralize even the most advanced security threats.

MORE SECURE

24/7/365 monitoring along with your dedicated Service Delivery Manager (SDM) who will review, discuss, and consult with you on tactical, strategic, and technical requirements, helping you monitor your environment, perform regular health checks and updates, and respond to threats rapidly.

MORE COMPLIANT

We look at the bigger picture of how the configuration, optimization, deployment, management, and maintenance of your MDR solution can proactively support your compliance requirements.

MORE RETURN ON INVESTMENT

Our comprehensive, Cyber Fusion approach streamlines security operations, reduces the risk of an incident, and lowers the total cost of ownership (TCO) of your MDR investment.

ABOUT AVERTIUM

Avertium is a cyber fusion company with a programmatic approach to measurable cyber maturity outcomes. Organizations turn to Avertium for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive approach to cybersecurity. That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**