



Microsoft Threat Protection Engagement



Grant Thornton Overview – Microsoft Services

Grant Thornton leverages best-in-class industry tools to provide a full suite of deployment, integration, and managed security services. We help customers focus on what is relevant, eliminating false positives, performing effective triage before issuing an alert, and risk prioritization to ensure limited budgets are spent in the most effective way. Our team acts as an extension of the customer's organization, working collaboratively with our customers to help strengthen their cyber defenses.

GT Experience



Deeply Qualified Teams

Our teams bring the right mix of technical expertise and operational acumen to align your Microsoft investment with your overall program goals and objectives.



Experienced Staff

Our team members are comprised exclusively of Microsoft certified Engineers and Analysts dedicated to providing implementation and monitoring services support to our customers for Microsoft's entire product suite.



Lessons Learned

Our services and recommendations are based on lessons learned in the field performing this work, not theories. Our integration and monitoring services experience guide success by avoiding items that sound good but don't work and the reason why.



Insight Into Cyber Risks

Purpose built content and models to align implementations to leading risk areas such as insider threat, cyber fraud, and cyber operations automation.



Security

Specialist
Cloud Security
Threat Protection

Grant Thornton Alliance with Microsoft

Grant Thornton brings a wealth of experience in the design, review, and deployment of Azure Security services. Furthermore, we are actively involved in and acknowledged by Microsoft’s Security Designation and Specialization programs.

Grant Thornton Capability Areas	Sample Azure Security Products Grant Thornton can support
Identity & Access Management (IAM) Services	 Entra ID  Authenticator  Privileged Identity Management  Identity Protection  Conditional Access
Threat Protection Services	 Sentinel  Defender  Log Analytics Workspace
Cloud Security Services	 Azure Firewall  Key Vault  DDoS Protection  Defender for Cloud
Information Protection (IP) Services	 Information Protection  Data Loss Prevention  Unified Data Governance

Engagement Overview

Designed as a four-week engagement, the Threat Protection engagement uses specialized trials and subscriptions for identifying threats and vulnerabilities in a customer environment and will help define clear next steps and the best ways to mitigate risks.

Kick-off Meeting

- Introduce the Threat Protection Engagement, discuss the upcoming activities, align expectations and establish timelines.

Define Scope

- Define and finalize the engagement scope and required configuration settings for the engagement tools.

Change Management

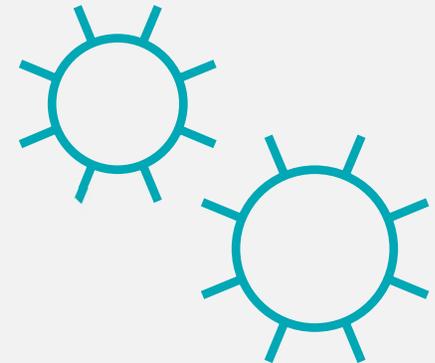
- Customer to go through their change management process and obtain approval for configuration changes as per defined scope.

Microsoft 365 Security Configuration

- Deploy and configure the Microsoft 365 tenant and Microsoft 365 Security.

Microsoft Sentinel Configuration

- Deploy and configure Microsoft Sentinel.



What we'll do during the engagement



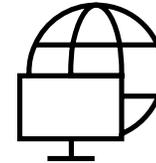
Analyze your priorities and requirements for deployment of Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) systems.



Define scope & deploy Microsoft Sentinel and Microsoft Defender XDR in production environment, integrating them with Microsoft and 3rd party solutions.



Discover threats to cloud and on-premises and across email, identity, endpoints and data and demonstrate how to automate responses.



Discover and prioritize vulnerabilities and misconfigurations across your organization.



Plan next steps on how we can work together.

Threat Protection Engagement Approach

1. Engagement Setup

2. Engagement Execution

3. Results and Outcome



STEP 1



Our goal is to ensure project goals and criteria align with customer goals and expectations.

Key Activities:

- **Define Engagement Objectives:** Establish specific goals for the engagement, identify stakeholders and define roles and responsibilities between Grant Thornton & customer staff.
- **Define Scope of the Engagement:** Review in-scope Microsoft products, data sources to be ingested into Microsoft Sentinel, and different types of policies to configure in Microsoft Defender XDR for Microsoft Defender for Endpoint, Office 365, Cloud Apps, Vulnerability Management and Entra ID Protection.
- **Define Customer Responsibilities:** Establish key customer responsibilities for a successful engagement including but not limited to providing access to customer tenant & relevant stakeholder to oversee and own the process from the customer side.

Deliverables/ Outcomes:

- ✓ Kickoff slide deck
- ✓ Customer questionnaire

Threat Protection Engagement Approach

1. Engagement Setup

2. Engagement Execution

3. Results and Outcome



STEP 2



Our goal is to prepare cloud environment and identify threats and risks in the environment.

Key Activities:

- **Integration of Microsoft Sentinel:** Deploy a dedicated log analytics workspace for this engagement and Configure data source ingestion into Sentinel via connectors and the Syslog agent VM
- **Integration of Microsoft Defender:** Deploy Defender XDR suite products which includes Microsoft Defender for Endpoint, Office 365, Cloud Apps, Vulnerability Management, and Entra ID Protection
- **Configuration of Defender and Sentinel:** Configure analytics rules, playbooks, and threat hunting use cases
- **Configure Vulnerability Scanning & Entra ID Protection policies**

Deliverables/ Outcomes:

- ✓ Deployment review with customer staff

Threat Protection Engagement Approach

1. Engagement Setup

2. Engagement Execution

3. Results and Outcome



STEP 3



Our goal is to document findings, prioritize actions, and improve security posture over time.

Key Activities:

- **Documentation and Reporting:** Document findings from incidents and alerts in Defender and Sentinel, including identified top threats and recommendations for mitigating identified risks. Provide a detailed report to the customer, highlighting engagement results, prioritized recommendations, and actionable steps for improving organization's security posture.
- **Engagement decommissioning & closeout:** Remove trial licenses or any engagement specific configuration from the customer's tenant. Discuss follow on engagement work with the customer.

Deliverables/ Outcomes:

- ✓ Engagement report highlights top risks and recommendations
- ✓ Follow up engagement plan

Contact Us



John Pearce

Principal

T +1 703 637 4071

E John.Pearce@us.gt.com



Don Sheehan

Managing Director

T +1 703 847 7642

E Don.Sheehan@us.gt.com



"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the independent network of GTIL member firms provide services to their clients, as the context requires. GTIL and each of its member firms are not a worldwide partnership and are not liable for one another's acts or omissions. In the United States, visit [grantthornton.com](https://www.grantthornton.com) for details.
© 2024 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd