SERVICE DESCRIPTION

# Accelerators for Microsoft Security

## Overview

Trustwave's Accelerators for Microsoft Security (**"Service"**) provide Client with a roadmap to accelerate value and security outcomes from Microsoft Security products. Trustwave will review Client's Microsoft Security capabilities with the aim of improving security maturity and to identify potential cost-saving initiatives.

The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

## Service Features

The Service includes one (1) or more of the following accelerators (one (1) or more, **"Accelerators"**, and each, an **"Accelerator"**). The applicable Accelerator(s) will be indicated in a SOW or Order Form between Trustwave and Client.

### Accelerators

**Accelerator for Microsoft Defender XDR**

The Accelerator for Microsoft Defender XDR provides Client with a roadmap to accelerate value and security outcomes from Microsoft Defender XDR. Trustwave will conduct the following reviews as part of the Service:

- **Security Entitlements:** Evaluate current security entitlements to understand what has been purchased and determine alignment with security needs.
- **Security Configurations:** Assess existing security configurations within each Defender XDR service to identify areas for improvement.
- **Use & Operation of Security Tools:** Review current use and operation of security tools with a view to improving their effectiveness.
- **Financials:** Identify redundancies and opportunities for rationalization in the Defender XDR technology stack to identify potential cost savings.

The Microsoft Security products covered under the Accelerator for Microsoft Defender XDR are:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Servers

- Microsoft Defender Vulnerability Management

### Accelerator for Microsoft Sentinel

The Accelerator for Microsoft Sentinel provides Client with a roadmap to accelerate value and security outcomes from Microsoft Sentinel. Trustwave will conduct the following reviews as part of the Service:

- **Workspace Architecture:** Assess workspace architecture to understand current deployments and identify areas for improvement.
- **Data Sources:** Evaluate data sources and log source types to understand data connections.
- **Roles & Permissions:** Assess roles and permission for users, groups, and services to evaluate excessive privileges.
- **Threat Intelligence:** Evaluate threat intelligence enablement to assess coverage and threat hunting capabilities.
- **SIEM Content:** Evaluate SIEM use cases, analytics, and threat hunting to assess comprehensiveness.
- **SOAR Playbooks:** Review inventory of playbooks, dashboards, and reporting metrics to assess level of coverage and provide recommendations for enhancement.
- **System Auditing:** Evaluate past auditing results against existing processes to assess effectiveness of changes.
- **Defender XDR Connectivity:** Evaluate connectivity to Defender XDR services to identify areas for optimization.
- **Financials:** Evaluate current usage against cost model to identify potential cost savings.

The Microsoft Security product covered under the Accelerator for Microsoft Sentinel is:

- Microsoft Sentinel

### Accelerator for Microsoft Copilot for Security

The Accelerator for Microsoft Copilot for Security provides Client with a roadmap to accelerate value and security outcomes from Microsoft Copilot for Security. Trustwave will conduct the following reviews as part of the Service:

- **Environment:** Assess the environment based on best practices pertaining to permissions and access controls, as well as Defender XDR scope, to identify areas for improvement.
- **Promptbooks:** Plan and analyze core security operations detection, triage, and response promptbooks.
- **Use & Operation:** Review current use and operation of Copilot for Security to identify potential improvements to its effectiveness.
- **Use Cases:** Identify potential use cases security teams can benefit the most from through Copilot for Security.

The Microsoft Security product covered under the Accelerator for Microsoft Copilot for Security is:

- Microsoft Copilot for Security

For Trustwave to provide the Accelerator for Microsoft Copilot for Security, Client must procure Security Compute Units (SCUs) from Microsoft. Trustwave will coordinate with Client to determine the number of SCUs required to provide the Service.

## Tools and Methodologies

Trustwave will combine industry-standard, Microsoft-native, and proprietary tools to perform the Service to provide a comprehensive and effective review process.

## Deliverables

Trustwave will produce the following deliverables as part of the Service:

- **Gap Analysis:** Analysis highlighting gaps between current and optimal security configurations.
- **Recommendations:** Suggestions for additional security capabilities or features for evaluation.
- **Cost-Benefit Analysis:** Prioritization of recommendations based on a cost-benefit analysis.
- **Prioritized Roadmap:** Prioritized roadmap for implementing recommendations, with consideration for impact and ease of implementation.
- **Implementation Proposal:** Proposal for implementing recommended changes.
- **Executive Summary:** Summary of key findings and proposed implementation plan.

# Delivery and Implementation

Trustwave will work with Client to assess and determine areas of improvement for Client's Microsoft Security capabilities:

## Discovery

Trustwave will work with Client to gather information that describes Client's Microsoft Security environment. This includes:

- Completing preparatory work and outlining requirements for the Service.
- Conducting a kick-off with stakeholders to discuss objectives and delivery expectations, including escalation paths and governance.
- Developing a project plan with key activities, milestones, and timelines.
- Obtaining systems access with appropriate permission levels.
- Collecting relevant information on existing security tools.

### *Client Obligations*

For Trustwave to provide the Service, Client will:

- Provide contact details for and access to Client stakeholders and escalation points and remain available for communication from Trustwave;
- Attend a kick-off and provide logistics support for booking meetings and arranging access to required personnel;
- Coordinate with Trustwave to discuss concerns and perceived threats, objectives, and delivery expectations, as well as develop a project plan; and
- Provide Trustwave with access to systems with appropriate credentials, as reasonably requested by Trustwave.

### *Trustwave Obligations*

As part of providing the Service, Trustwave will:

- Establish engagement roles and responsibilities for stakeholders;
- Deliver and facilitate a kick-off at a date and time agreed between Trustwave and Client;

- Coordinate with Client to discuss concerns and perceived threats, objectives, and delivery expectations, as well as develop a project plan;
- Collect current state data and information from Client's systems; and
- Develop a report giving details on the kick-off and outcomes.

## Analysis

Trustwave will examine applicable data and information and coordinate with Client stakeholders to assess Client's current Microsoft Security capabilities:

### Accelerator for Microsoft Defender XDR

For the Accelerator for Microsoft Defender XDR, analysis includes:

- Evaluating security entitlements and configurations.
- Assessing previous security incidents.
- Reviewing Client's Microsoft Secure Score and associated security metrics.
- Assessing compliance controls based on security features available in Defender XDR.
- Reviewing security tool usage and operations, identifying redundancies and opportunities for rationalization.
- Identifying Microsoft services outside of Defender XDR that Client is not currently using but which may help enhance Client's security maturity.
- Conducting knowledge transfer for the assessed Defender XDR functions for Client stakeholders.

### Accelerator for Microsoft Sentinel

For the Accelerator for Microsoft Sentinel, analysis includes:

- Assessing workspace architecture.
- Evaluating data sources and log source types, including roles and permissions.
- Analyzing threat intelligence enablement and capabilities.
- Reviewing SIEM content (e.g., use cases, analytics, threat hunting) and inventory of SOAR playbooks.
- Reviewing SOC efficiency dashboards and reporting.
- Assessing previous security incidents.
- Evaluating system auditing capabilities and effectiveness of changes.
- Evaluating connectivity to Defender XDR services as well as third-party technologies.
- Assessing usage costs and determining where costs can be optimized.
- Assessing compliance controls based on security features available in Sentinel.
- Conducting knowledge transfer for the assessed Sentinel functions for Client stakeholders.

### Accelerator for Microsoft Copilot for Security

For the Accelerator for Microsoft Copilot for Security, analysis includes:

- Assessing the environment based on best practices pertaining to permissions and access controls, as well as Defender XDR scope.
- Identifying potential plugin enablement for Microsoft products and services.
- Assessing previous security incidents.
- Reviewing dashboards, reporting, and security metrics.
- Assessing compliance controls based on security features available in Copilot for Security.
- Planning and analyzing core security operations detection, triage, and response promptbooks.

- Identifying and assessing potential use cases for Copilot for Security, including planned, new, or existing deployments.
- Assessing SCU requirements based on security operations and planned usage.
- Conducting knowledge transfer for the assessed Copilot for Security functions for Client stakeholders.

### *Client Obligations*

For Trustwave to provide the Service, Client will:

- Provide feedback on Trustwave findings, as requested by Trustwave;
- Participate in and understand materials explained during meetings, including discussions on inspections and controls analysis; and
- Attend knowledge transfer programs conducted by Trustwave.

### *Trustwave Obligations*

As part of providing the Service, Trustwave will:

- Assess current state data and information from Client's systems;
- Review findings with Client and obtain feedback as required; and
- Deliver and facilitate knowledge transfer programs for Client stakeholders.

## Reporting

Trustwave will produce a roadmap that Client may utilize to accelerate Microsoft Security capabilities and improve security maturity. This includes:

- Conducting a gap analysis highlighting gaps between current and optimal security configurations.
- Developing recommendations for additional security configurations or features to improve Client's security maturity.
- Conducting a cost-benefit analysis to prioritize recommendations.
- Developing a prioritized roadmap for implementing recommendations.
- Developing a proposal for implementing proposed changes.
- Summarizing key findings and proposed implementation plan for Client stakeholders.

### *Client Obligations*

For Trustwave to provide the Service, Client will:

- Review Trustwave's deliverables and attend review sessions conducted by Trustwave; and
- Support the identification of appropriate owners for Trustwave's findings and recommendations.

### *Trustwave Obligations*

As part of providing the Service, Trustwave will:

- Present deliverables to Client for review and feedback; and
- Conduct project close-out, confirming delivery of key activities and deliverables.

# Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable SOW or Order Form between Trustwave and Client.