MANAGED CLOUD PROTECTION - SERVICE GUIDE

Last Modification Date: 12/19/2023
Exported and Shared on: 03/15/2024

For additional information, visit www.intervision.com

CONTENTS

1 SERVICE DESCRIPTION

Managed Cloud Protection covers malware and intrusion detection, prevention, and containment for designated cloud workloads, storage, networks, applications, and containers. This includes managed Trend Micro Cloud One (Apex One) software agents and licensing, managed services via trained and focus cybersecurity experts, alerting of malware issues, and reporting of malware protection activity.

This managed service is provided for devices or applications in a cloud environment. The service is designed to have all qualified workloads and applications covered; a partially covered environment is not acceptable.

2 SERVICE DETAILS

This service is designed to provide malware, exploit, and intrusion protection for cloud resources as well as managed support of the Trend Cloud One platform, policies, and alert output:

- Provides managed software to protect cloud workloads, storage, networks, applications, and containers from malware, intrusions, and exploits
- Trend Micro Cloud One software and platform troubleshooting and support
- Alerting and ticketing for compromise related incidents
- Remediation guidance for detected compromises
- Ongoing operations by knowledgeable Security Operations Center staff
- Trend Micro Cloud One software updates
- Trend Micro Cloud One administrative support with 24/7/365 coverage
- Activity and summary reporting

3 IMPLEMENTATION

The rollout of the Trend Micro Cloud One platform has multiple steps to help ensure a successful deployment. However, this may vary depending on unique client environments or requirements. Below is the typical implementation process:

- Customer* provides details on environment (cloud provider, operating systems, types of segments to protect, etc.).
- InterVision SOC creates test groups/policies and provides Trend Micro Cloud One installation direction.
- Customer deploys Trend Micro Cloud One test software to a test environment for a short period of time
- InterVision SOC reviews the test policy findings, including any initial detections or customer reported issues (performance slowdown, application failures, etc.).
- InterVision SOC provides recommendations for allowlists/exclusions to the customer.
- Customer approves change list, and InterVision SOC makes the necessary changes.
- InterVision SOC moves existing install base to standard policies.
- InterVision SOC provides customer with new installation directions to deploy standard software to the rest of the customer environment.
- Customer deploys software to the rest of their environment and then removes any other protection software still in place.
- InterVision SOC provides reports of where Trend Micro Cloud One has been installed.
- Upon successful implementation, InterVision SOC will move into normal Managed Cloud Protection runtime state with 24/7 production support.

**InterVision Managed Cloud Services, Professional Services, or Help Desk may augment Customer IT where appropriate when those services are consumed alongside Managed Cloud Protection.*

4 SUPPORT

InterVision maintains a 24/7 operations center (InterVision SOC) which serves as the designated administrative contact for Trend Micro Cloud One support. The technical support model provides unlimited support for the customer-designated IT contact (eg. IT Director, InfoSec Director, System Admin, etc.). Direct end-user support is not included but may be obtained through InterVision HelpDesk services.

Phone, email, and ticket-based support activities include:

- Trend Micro Cloud One Software Troubleshooting and Support
- Policy management
- Allow-listing assistance
- Initiating deep scans
- Malware incident response –
    - Details of the event
    - File investigation
    - Recommend remediation actions
    - Malware infection root cause analysis
- Platform administration and troubleshooting
- Open and escalate issue with software to vendor
- Standard reporting per client requirements
- InterVision portal and InterVision portal access

Endpoint remediation such as manual file removal or operating system re-installation/reimaging is not included in this service. Complimentary services such as Managed Cloud Services, Help Desk, and Professional Services are available for these additional remediation capabilities.

5 INTERVISION SERVICE PORTAL

The InterVision service portal provides for the creation, tracking, and review of service tickets. All service ticket information is available via this portal and enables tracking of implementations, changes, releases, and general support issues. The InterVision Services portal is accessible via https://support.hostedcafe.com[1].

6 ALERTING

Managed Cloud Protection attempts to block or quarantine malware, intrusions, and exploits, however, new threats such as unseen zero-day attacks may evade software detection. The service will alert upon critical or high risk events representing potential compromises via the ticketing system. These critical alerts are sent to both the 24/7 Operation Center and to the customer simultaneously.

Other non-critical events that are considered informational and do not require actions are collected and available through generated reports.

7 REPORTING

Managed Cloud Protection offers many operational, event, and activity reports for scheduled email delivery. These vary based on service usage (workload/storage/application/network/container) and policy and include, but are not limited to:

- Utilization by module
- Events by module
- Total incidents over time
- Versioning

1 https://service.hostedcafe.com/

- Threats detected by engine (Anti-Malware, Web Reputation, Device Control, Firewall, Intrusion Prevention, etc)

Custom reporting may available on an as needed basis based on scope.

8 ROLES & RESPONSIBILITY MATRIX

	InterVision	Customer	Extended (Professional or Managed Cloud Services)*
General			
Provide client escalation contacts and procedures		X	
Provide install base information (segments, OS, machine count, etc.)		X	
Installation and Configuration			
Provide licensed software	X		
Install software on machines		X	X
Set up initial Cloud One platform and workload policies	X		
Provide change management for Cloud One platform and workload policies	X		
Identify which applications, sites, and IPs to exclude or allow-list		X	
Configure exclusions, exceptions, and allow-listing	X		
Create/Manage Application, Network, File Storage, or Container Policies	X		
Monitoring and reporting			
Provide access to InterVision monitoring portal	X		

	InterVision	Customer	Extended (Professional or Managed Cloud Services)*
Manage incident notification profiles	X		
Provide ticket based notification for all high severity malware incidents	X		
Provide reporting for overall malware activity	X		
Provide pre-defined reports on schedule or demand.	X		
Operations			
Provide workload agent software updates to InterVision supported versions**	X		
Deploy/apply software updates to covered servers***	X		
Software vendor management	X		
Update exclusion lists per client requirements	X		
Update policy with new indicators of compromise	X		
Initiate a deep scans	X		
Update policies per client request	X		
Enable proactive isolation of compromised endpoints	X		
Infection and Remediation			
Malware quarantine and exploit blocking (software)	X		

	InterVision	Customer	Extended (Professional or Managed Cloud Services)*
Root cause analysis of malware/ exploits that are not quarantined or blocked	X		
Provide information relative to nature of malware infection	X		
Advise client on remediation actions for malware not quarantined	X		
Trouble shoot endpoint devices not checking in or running scans		X	X
Reimage endpoints machines infected by malware		X	X
Incident Response or Forensics for larger scale malware outbreaks			X

* Extended services are optional services that can be provided with incremental fees. These services may be additional Managed Services or Professional Services

** InterVision is committed to providing your organization with the latest and greatest technology releases to protect your environment. InterVision supports Trend Micro recommended versions and may not be running on the latest version.

*** If an upgrade requires an uninstall of a previous version, to maintain SLA and incident response, client must assist InterVision with the uninstall and reinstall process within 6-months of the request.

9 SUPPORTED ENVIRONMENT

The Managed Cloud Protection service is designed to work in AWS with support for Azure roadmapped for 2023. The Workload module is compatible with modern Windows and Linux operating systems. See the Trend Micro Cloud One Agent Compatibility Guide at this permalink[2] for current system requirements.

10 COMMERCIAL TERMS

Managed Cloud Protection is sold based on covered workload, storage, network, application, or container utilization, sizing, and term. A minimum of a 1-year commitment is required for new and add on purchases. This service is billed monthly, in advance of the coming month.

No other services are required to utilize the Trend Micro Cloud One software.

2 https://cloudone.trendmicro.com/docs/workload-security/agent-compatibility/