MANAGED ENDPOINT PROTECTION - SERVICE GUIDE

Last Modification Date: 02/14/2024
Exported and Shared on: 03/18/2024

For additional information, visit www.intervision.com

CONTENTS

1 Service Description 1
2 Service Details 1
3 Implementation 1
4 Support 2
5 InterVision Support Portal(s) 2
6 Alerting 2
7 Reporting 2
8 Roles & Responsibility Matrix 3
9 Supported Endpoint Protection Platforms and Environments 6
10 Managed Endpoint Protection and InterVision's Managed Detection and Response Services 6
11 Commercial Terms 6

1 SERVICE DESCRIPTION

The Managed Endpoint Protection Service covers malware detection, prevention, and containment for protected endpoints (servers, workstations, laptops, or mobile devices) in an environment. This includes management of an associated Endpoint Protection Platform (EPP), managed services via trained and focus cybersecurity experts, alerting of malware issues, and reporting of malware protection activity. This managed service is designed to cover all qualified endpoints within an environment; a partially covered environment for reasons other than software incompatibility is not acceptable.

2 SERVICE DETAILS

This service is designed to provide endpoint malware protection, managed support of an associated Endpoint Protection Platform, and incident management for associated alerts. The following features are included in the service:

- Provides managed endpoint protection software to defend endpoints against malware and computer viruses (or supports InterVision resold EPP licensing, depending on service scope)
- EPP software troubleshooting and support
- Alerting and ticketing of malware incidents
- Remediation guidance for malware infections
- Activity and summary reporting
- Ongoing operations by knowledgeable Security Operations Center staff
- EPP software updates
- EPP administrative support with 24/7/365 coverage
- Proactive isolation of compromised Endpoints*
- Automated analysis of unknown rarely seen executables*

*on EPP's with associated capabilities

3 IMPLEMENTATION

The rollout of the EPP software has multiple steps to help ensure a successful deployment. However, this may vary depending on the EPP chosen and the unique client environment and requirements. Below is the typical implementation process:

- Customer provides details on environment (operating systems, types of endpoints).
- The InterVision SOC creates audit mode groups/policies and sends endpoint agent installation instructions to the customer.
- Customer deploys endpoint agent software (in audit mode) to a set of test machines in tandem with their current anti-virus solution for a short period of time
- The InterVision SOC reviews the audit mode findings that include initial detections from the EPP, and customer reports any issues (machine performance, execution issues, etc.).
- The InterVision SOC provides recommendations for allow-lists/exclusions to the customer.
- Customer approves change list, and The InterVision SOC makes the necessary changes.
- The InterVision SOC moves existing installed endpoints to active/quarantine mode.
- The InterVision SOC provides customer with new endpoint agent installer to deploy active/quarantine mode agent on remaining systems.
- Customer deploys software to the rest of their environment and then removes any other anti-virus software.
- The InterVision SOC provides reports of machines with endpoint agent software installed.
- Customer deploys endpoint agent to any missing machines not in the inventory report.
- Upon successful implementation, The InterVision SOC will move into normal Managed Endpoint Protection runtime state with 24/7 production support.

4 SUPPORT

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

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

- EPP Software Troubleshooting and Support
- Policy management
- Allow-listing assistance
- Initiate 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 support and ticketing 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 Network Services, Help Desk, and Professional Services are available for these additional remediation capabilities.

5 INTERVISION SUPPORT PORTAL(S)

Customers with the Managed Endpoint Protection service can request access to the following portals:

- The InterVision Service Portal - All service ticket information is available via this portal and enables tracking of implementations, changes, releases, and general support issues. Accessible via https://support.intervision.com.
- The associated EPP console portal - Access varies depending on the EPP product utilized. Co-management of all supported EPPs is allowed and client support staff can be provided with role-based or administrator access to the EPP at client request.

6 ALERTING

The endpoint protection software will attempt to block malware (when configured in active/quarantine mode), however, new threats such as unseen zero-day attacks may evade software detection. The service will alert upon critical or high risk events including an event such as “malware executed and not quarantined” via the ticketing system. These critical alerts are sent to both the 24/7 Security 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 Endpoint Protection provides many operational, event, and activity reports that vary based on the EPP utilized. The following reports are examples of what may be available on upon request or schedule:

- Computers with Failed Scans

- Detected Files Not Quarantined
- Failed Policy Update Attempts
- Last Scan Completed by Host
- List of Uninstalled Clients
- List of Vulnerable Applications by Computer
- Threats Detected by Count
- Total Endpoints

Reports including malware file trajectory, sandbox activity, and research results are available on an as needed basis.

8 ROLES & RESPONSIBILITY MATRIX

	InterVision SOC	Customer	Extended (Professional Services)*1
General			
Provide client escalation contacts and procedures		X	
Provide operating systems information		X	
Provide estimated number of endpoints to be installed		X	
Provide general network information (locations, bandwidth, bandwidth utilization) for EPP software policy optimization		X	
Installation and Configuration			
Provide licensed software	X	*2	
Install software on machines		X	X
Set up and administer Malware Protection software policies	X		
Identify which application, folder and files to exclude/allow		X	

	InterVision SOC	Customer	Extended (Professional Services)*1
Configure exclusion: application, folder and files	X		
Monitoring and reporting			
Provide access to InterVision service portals	X		
Configure malware activity dashboard in monitoring portal	X		
Manage incident notification profiles	X		
Provide ticket based notification for all high severity security incidents	X		
Provide reporting for overall malware activity	X		
Provide reporting for machines not checking in and not running scans	X		
Provide lists of endpoints with vulnerable applications *3	X		
Monitoring of custom alert or script functionality		X	X
Operations			
Provide agent software updates based upon InterVision supported versions *4	X		
Deploy/apply software update to endpoints *5	X		
Software vendor management	X		

	InterVision SOC	Customer	Extended (Professional Services)*1
Initiate unknown file investigations with vendor *3	X		
Update exclusion list 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 *3	X		
Custom script creation		X	X
Infection and Remediation			
Malware quarantine (software)	X		
Root cause analysis of malware that is 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, running scans, or running scripts		X	
Reimage endpoints machines infected by malware		X	

	InterVision SOC	Customer	Extended (Professional Services)*1
Deep investigation of Malware Outbreak			X

1: Extended services are optional services that can be provided with incremental fees. These services may be additional managed services or professional services

2: Support for customer provided EPP licensing may be available; check with your account manager for more information.

3: On EPPs that support this functionality

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

5: If an upgrade requires an uninstall of 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 ENDPOINT PROTECTION PLATFORMS AND ENVIRONMENTS

The Managed Endpoint Protection service currently provides support for the following EPPs:

- Cisco Secure Endpoint (CSE) EPP with with either InterVision owned licensing or InterVision resold EA licensing at Essentials license level. See the CSE user guide at this permalink[1] for current system requirements.
- SentinelOne Singularity EPP with InterVision resold term licensing. See the SentinelOne FAQ at this permalink[2] for current system requirements. The currently supported licensed modules are Singularity Complete and Singularity RemoteOps.

10 MANAGED ENDPOINT PROTECTION AND INTERVISION'S MANAGED DETECTION AND RESPONSE SERVICES

For customers consuming both the InterVision Managed Endpoint Protection and InterVision Managed Detection and Response (MDR) partner services, event tracking and incident notification for EPP related alerts will flow through the MDR provider for broader visibility with discounts available for the combined level of effort. There is no associated change regarding platform administration, ownership, support, or licensing.

11 COMMERCIAL TERMS

The Managed Endpoint Protection Service is sold per endpoint defined as a workstation, laptop, server, virtual machine, mobile device, or any other operating system instance. 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.

1 https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf
2 https://www.sentinelone.com/faq/

No other services are required to utilize the associated Endpoint Protection software.