Real Time Application Servers and Endpoint Protection

MITEL PRODUCT SECURITY AND COMPLIANCE GROUP

TECHNICAL PAPER

VERSION 1.0

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Real Time Application Servers and End Point Protection
Mitel Product Security and Compliance Group – Technical Paper
Version 1.0

Overview

This Mitel technical paper discusses the use of Endpoint Protection solutions to provide security for servers that are involved in processing real time data applications.

The paper discusses the following topics:

- Endpoint Protection Terminology.
- Antivirus Software and Endpoint Protection.
- Endpoint Protection Solutions.
- Endpoint Detection and Response Deployment Guidelines.
- Mitel Support and EDR Deployments.
- Ensuring that the Server has Sufficient Compute Resources.
- Key Compute Resources.
- Typical Compute Resources Required for EDR Agents.
- Tools for Measuring the Server's Compute Resources.
- Operational Recommendations.
- Additional Security Recommendations.

Introduction

Mitel's product portfolio offers many products and applications that process real time data for voice calls, voice call recording and messaging and video calls.

The range of real time data applications include Call Control Engines, Collaboration applications, Unified Communications applications and Application Session Border Gateways. Depending on the application, it may be deployed in a virtualized environment, on an industry standard server or on a purpose built hardware appliance.

Real time applications are sensitive to network and processing delays that add unacceptable latency to real time data streams. Such latency causes poor voice and video quality and/or results in failed connections.

Testing of several real time applications while antivirus/malware software was operating has shown that that the antivirus/malware software consumed unacceptable amounts of computing resources which impacted the processing of voice and video media and was therefore not suitable for deployment with real time applications. As a result, up until now servers running real time applications could not support the use of a security software solution.

With recent security industry developments, there are now Endpoint Protection solutions available that do not require large amounts of compute resources, and when there are adequate compute resources provisioned on the servers, Endpoint Protection solutions can be used to secure real time severs without impacting the quality of the real time data.

This paper provides Administrators and IT Security personnel with guidelines on how to ensure that real time data applications are not negatively affected by the operation of an Endpoint Protection solution on the server.

Who are the Parties that Should Use this Document

This document will be of interest to individuals that are involved with system administration, information technology and network security who are considering deploying Endpoint Protection technology on a server that is running real time applications.

Endpoint Protection – Terminology

Endpoint Protection or endpoint security is a general term that encompasses centrally managed security applications that are deployed on network endpoints and utilize advanced techniques to detect and respond to security threats.

Network endpoints are any network connected device such as servers, laptops, desktop computers, routers and switches.

Endpoint Protection Software Agent is the software component that is installed on an endpoint, it may also be referred to as an Endpoint Protection Agent or more simply an Agent.

Antivirus Software and Endpoint Protection

While antivirus software is typically installed on an endpoint, it is not considered to be part of the newer more sophisticated Endpoint Protection technology.

Antivirus/Malware Software

- Antivirus/Malware software (A/V) only protects against threats that the A/V software knows about.
- A/V uses signature-based threat detection.
    - The A/V signature database must be regularly updated, and between updates there is no protection against recently discovered threats.
- A/V only protects the endpoint that it is installed on, it does not monitor data from other endpoints or the network.

Endpoint Protection Software Agent

- Endpoint Protection Agents
    - Use behavioral analysis to detect suspicious activity and previously unknown threats
    - Agent threat signature updates are automatically maintained on an on-going basis.
- The Endpoint Agent passively monitors network traffic for suspicious activity and can have visibility to all network endpoints and associated network traffic.
- The Endpoint Agent has rules based automated response and analysis capabilities and can respond to threats and suspicious activity according to the assigned rules. Agents can respond to threats by:
    - Sending alerts to the Administrator and the security team.
    - Containing threats by automatically isolating all affected endpoints.

Endpoint Protection Solutions

New Endpoint Protection solutions are rapidly evolving; however, the functionality of Endpoint Protection solutions can be generally grouped into the following categories:

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR), also known as Endpoint Threat Detection and Response (ETDR), is a type of integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint agent data with rules-based automated response and analysis capabilities.

- EDR agents can provide visibility to all network endpoints and associated network traffic.
- EDR agents require the IT or security team to provide active monitoring and supervision of the EDR agent installations.

Endpoint Protection Platforms (EPP)

Endpoint Protection Platforms (EPP) automatically collect, consolidate, and analyze EDR agent data from a network wide perspective.

- An EPP platform can use analytics and machine learning to provide a higher level of security compared to sites that only use EDR agents.
- A solution utilizing EDR agents in conjunction with an EPP requires minimal supervision and unlike deployments that only utilize EDR agents, does not require constant monitoring by IT staff.

Managed Detection and Response Services (MDR)

Managed Detection and Response (MDR) services are a Security as a Service (SaaS) offering where the collection, consolidation and analysis of EDR agent data is outsourced to a security service provider.

- An MDR solution is considered an advanced 24/7 security control that often includes a range of fundamental security activities for organizations that cannot maintain their own security operations centre.
- MDR services may combine advanced analytics, threat intelligence, and human expertise in incident investigation and response.

EDR Deployment Guidelines

The Administrator and Security personnel should consider the recommendations in the following sections which are intended to assist with the successful installation and operation of EDR agent software on servers that are running real time applications.

Mitel Support and EDR Deployments

While the use of EDR agent software is widely accepted within the IT industry for use on general purpose servers and desktops, due to the wide range of vendor offerings and the variability of servers and their compute resources there is always the possibility of an EDR agent adversely affecting the performance of real time applications. (e.g. voice quality).

Mitel does not endorse the use of any specific EDR Agent software for Mitel applications and Mitel does not endeavor to test or evaluate EDR solutions available in the marketplace.

Should a customer require technical support from Mitel related to a system that has an EDR agent installed, Mitel may require that the EDR agent be removed as part of the Mitel troubleshooting process.

Mitel Appliances and Devices

Mitel purpose built hardware devices such as IP phones and Call Control hardware appliances (e.g. EX Controller) are fully closed systems and do not support the installation of EDR Agents or antivirus/malware software.

Ensuring that the Server has Sufficient Compute Resources

A key requirement to a successful EDR Agent deployment on a real time application server is to determine whether the server has been provisioned with enough compute resources to run the EDR Agent without impacting the performance of the real time applications.

Key Compute Resources

Once all of the installed real time application's resource requirements have been accounted for, the Administrator will then need to determine if the server has adequate compute resources available for also running the EDR Agent. The key compute resources that need to be determined are:

- CPU utilization.
- Memory utilization.
- Hard Disk Drive utilization.

Typical Compute Resources Required for EDR Agents

Based on specifications provided by EDR vendors and investigations conducted by Mitel, it can be expected that the additional compute resource requirements for the EDR agent will be in the following ranges:

- CPU utilization: Up to 5%.
- Memory utilization: Up to 10%.
- Hard Disk Drive utilization: Up to 10%.

A server may therefore require that additional compute resources be added by the customer to run both the real time application and the EDR Agent successfully.

Tools for Measuring the Server's Compute Resources

If it is necessary to measure the available compute resources, there are a number of tools available that can be used.

Microsoft Windows

Microsoft provides an application called Performance Monitor that can be used to determine compute resource utilization. There are also several performance monitoring tools available from third party vendors, and if the server supports an SNMP agent, then SNMP can be used to retrieve the performance data.

Linux

Most versions of the Linux operating system offer the system monitor tools called top (Table Of Processes) and htop (Hisham's Table Of Processes). These tools can be used to determine compute resource utilization.

If the Linux operating system supports an SNMP agent, then SNMP can be used to retrieve performance data from the server.

Mitel Standard Linux

Mitel Standard Linux (MSL) has the following tools available for determining compute resource utilization.

- MSL provides a Real Time System Information page and an Historic System Monitoring page.
- SNMP can be used to retrieve performance data from the server.
- MSL supports the system monitor tools top and htop.
- An SOS report can be downloaded and MSL provided plugins collect data related to the specific installation, for details refer to the MSL Installation and Administration Guide.
- Mitel has available an SOS Report Analysis Tool which is designed to process an original SOS report from an MSL server, creating an easy to read summary of the contents with that report, including commonly reviewed items, while also highlighting possible areas of concern. For details, contact Mitel Technical Support.

MiCollab – System Activity Report

MiCollab includes a system monitor tool called System Activity Report (SAR). SAR can be used to report on CPU utilization, memory and swap space utilization and network utilization.

The path to SAR is */var/log/sar*. Mitel's SOS Report Analysis Tool can be used to graph the data and can be used to help identify performance issues.

Operational Recommendations

To ensure that the real time applications are not impacted by the operation of the EDR Agent, the Agent's configuration settings will need to be tuned from their default settings. The following recommendations should be followed:

- Real Time Monitoring of network traffic for indicators of compromise or Malware scanning of related processes should be excluded or disabled.
- Full system malware scans should take place during a maintenance window or outside of core business hours.
- If a full system malware scan takes an excessive amount of time to complete, then it is recommended that the Administrator include large log files in the scan exclusion list.
- Malware scan exclusions should be considered for files frequently written to or read from, e.g. database files.

Additional Security Recommendations

In addition to the use of EDR Agents, other measures that can be employed to protect the server are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure.
- The proper configuration of internal and external public facing routers and firewalls.

There are also a number of general security aspects that need to be covered and addressed by the Administrator and/or the IT security personnel.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations because many data-exposure attacks can be mounted by unauthorized persons having physical access to a host. Further, the IT data infrastructure must be designed with security in mind, security mechanisms and protocols must be enabled, and all components of the whole system must be correctly configured and maintained and updated as necessary.

For further information refer to the documentation suite for the particular product or application. The documentation suite includes Security Guidelines, Personal Data Protection and Privacy Controls documentation, Engineering Guidelines and Administration Guides.

Product and application documentation is available on Mitel's Document Center Web site.

https://www.mitel.com/document-center

Mitel Powering connections | mitel.com