Trellix

DATA SHEET

Trellix File Protect

Detect and eliminate malware on file shares and content stores

Key Benefits

- Finds latent malware undetected by traditional AV engines
- Deploys in active quarantine (protection) or analysis only (monitoring) modes
- Provides recursive, scheduled, and on-demand scans of CIFS and NFS compatible file shares
- Provides proactive protection for Microsoft OneDrive and SharePoint
- Includes analysis of a wide range of file types such as PDFs, Microsoft Office documents, and multimedia files
- Integrates with Trellix IVX Cloud for analyzing files and shares threat data through Trellix Central Management and Trellix Dynamic Threat Intelligence cloud

Overview

Trellix File Protect secures data assets across a wide range of file types against attacks that originate from email, online file transfer tools, the cloud, and portable file storage devices. Such attacks can spread to file shares and content repositories. File Protect analyzes network file shares and content management stores to detect and quarantine malware that bypasses next-generation firewalls, intrusion prevention systems (IPSs), antivirus (AV) systems, and gateways.

Challenges of malware on file shares

Today's advanced cyberattacks use sophisticated malware and advanced persistent threat (APT) tactics to penetrate defenses and spread laterally through file shares and content repositories. This enables malware to establish a long-term foothold in the network and infect multiple systems, even those that are offline.

Many enterprise data centers remain especially vulnerable to advanced, content-based malware. That's because traditional defenses are ineffective against these attacks, which often enter the network through legitimate means. Adversaries leverage these vulnerabilities to spread malware into network file shares and embed malicious code in vast data stores, resulting in a persistent threat even after remediation.

Importance of file content protection

Without a way to detect resting malware in content, APTs can exploit network assets to extract proprietary information and cause significant damage. File Protect analyzes file shares and enterprise content repositories using the Trellix Intelligent Virtual Execution (IVX) engine, which detects zero-day malicious code embedded in common file types (PDF, MS Office, vCards, ZIP/RAR/TNEF, etc.) and multimedia content (MP3, Real Player, JPG, PNG, etc.).

File Protect performs recursive, scheduled, and on-demand scanning of accessible network file shares and content stores to identify and quarantine resident malware. This halts a key stage of the advanced attack life cycle.

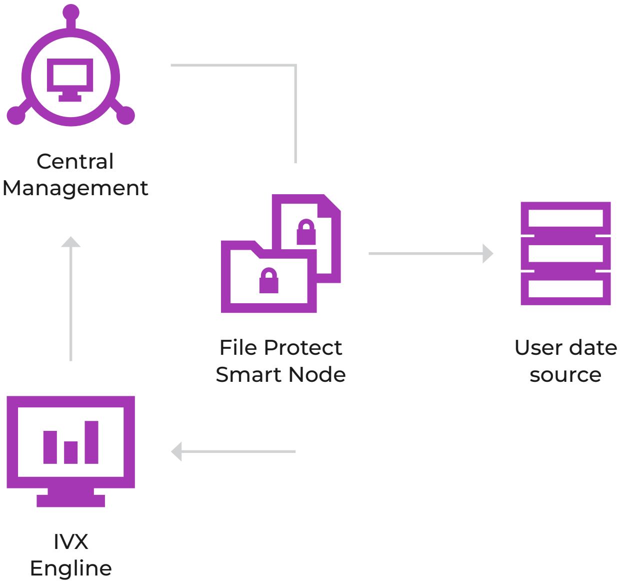

Figure 1. Sample Trellix File Protect deployment

Reveal unknown, zero-day threats

Trellix FX uses the IVX engine to inspect each file and confirm the existence of zero-day exploits or malicious code. The IVX engine detects zero-day, multi-flow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops the infection and compromise phases of the cyberattack kill chain by identifying never-before-seen exploits and malware.

The power of IVX Smart Grid

Trellix IVX Smart Grid improves organizations' security posture with a flexible and scalable deployment architecture via hybrid or private cloud. IVX Smart Grid uses an innovative approach to more effectively secure campuses, branch offices, and remote users by separating the IVX engine from hardware and virtual Smart Nodes. Smart Nodes analyze internet traffic to detect and block threats using a variety of techniques, such as static analysis, analytics, IPSs, applied intelligence, and more, while the IVX engine performs core dynamic analysis.

Protect Microsoft OneDrive and SharePoint

File Protect continuously scans content to alert and permanently quarantine malware discovered in OneDrive and SharePoint repositories. It leverages WebDAV protocol to securely integrate with SharePoint services to protect enterprise business workflows that use SharePoint repositories.

Enable customization with YARA-based rules

File Protect supports custom YARA rules to analyze large quantities of file threats specific to the organization.

Streamline incident prioritization

With Trellix Endpoint Security, each malicious object can be further analyzed to determine if antivirus vendors were able to detect the malware stopped by File Protect.

This enables your organization to efficiently prioritize incident response follow-ups and use common naming conventions for known malware.

Share malware intelligence

The resulting dynamically generated, real-time threat intelligence can help all Trellix products protect the local network through integration with Trellix Central Management.

This intelligence can be shared globally through the Trellix Dynamic Threat Intelligence (DTI) cloud to notify all subscribers of emerging threats.

Deploy with no tuning and near-zero false positives

Unlike other security solutions, Trellix File Protect requires absolutely no tuning. Flexible deployment modes include analysis-only monitoring and active quarantining. This allows your company to learn how much malware is resident on file shares and to actively stop the lateral spread of malware.

Protection where you need it with Content Smart Nodes

With Trellix Content Smart Nodes content and security managers gain a flexible, virtual solution to protect mission-critical content throughout the enterprise. Leveraging the IVX Smart Grid, content protection scales and deploys seamlessly where it's needed.

Deploy via flexible form factors

Choose between either virtual Content Smart Nodes or traditional on-premises hardware appliances to get the solution that's ideal for your environment.

Table 1. Trellix File Protect Smart Node Virtual Appliance Specifications

	FX 2500V
OS support	Microsoft Windows, MacOS X, CentOS
Performance	50,000 files per day
Network interface ports	Ether 1, Ether 2
CPU cores	2
Memory	8 GB
Drive capacity	512 GB
Hypervisor support	KVM 1.5.3, VMWare ESXi 6.0 or later

Table 2. Trellix File Protect Smart Node Cloud Appliance Specifications

	FX 2500V
OS support	Microsoft Windows, MacOS X, CentOS
Performance	50,000 files per day
Network interface ports	Ether 1, Ether 2
CPU cores	2
Memory	8 GB
Drive capacity	512 GB (AWS), 2TB (Azure)
Hypervisor support	AWS m5.xlarge, Azure

Table 3. Trellix File Protect Smart Node Hardware Appliance specifications

	FX 6600
Performance	Up to 87,000 files per day
Network interface ports	1x 1 GigE BaseT
IPMI port (rear panel)	included
USB port (rear panel)	2X USB2.0 , 2X USB3.2
Serial port (rear panel)	115,200 bps, no parity, 8 bits, 1 stop bit
Storage capacity	4x 4TB RAID 10, HDD 3.5 inch, FRU
Enclosure	2RU, fits 19-inch rack
Chassis dimensions (WxDxH)	17.2 x 25.5 x 3.5 inches (437 x 620 x 88.4 mm)
AC power supply	Redundant (1+1), FRU, 920W with Input 100-240V, 11-4.4A, 50-60 Hz IEC60320-C14 inlet
Power consumption maximum	618 watts
Thermal dissipation maximum	2108 BTU/hr
MTBF	26023
Appliance alone/as shipped weight lb (kg)	41 lbs/ 67 lbs
Safety certifications	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
EMC/EMI certifications	FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CISPR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35
Operating temperature	5°C - 35°C (41°F - 95°F)
Operating relative humidity	5% - 95% (non-condensing)
Operating altitude	0 to 5000ft