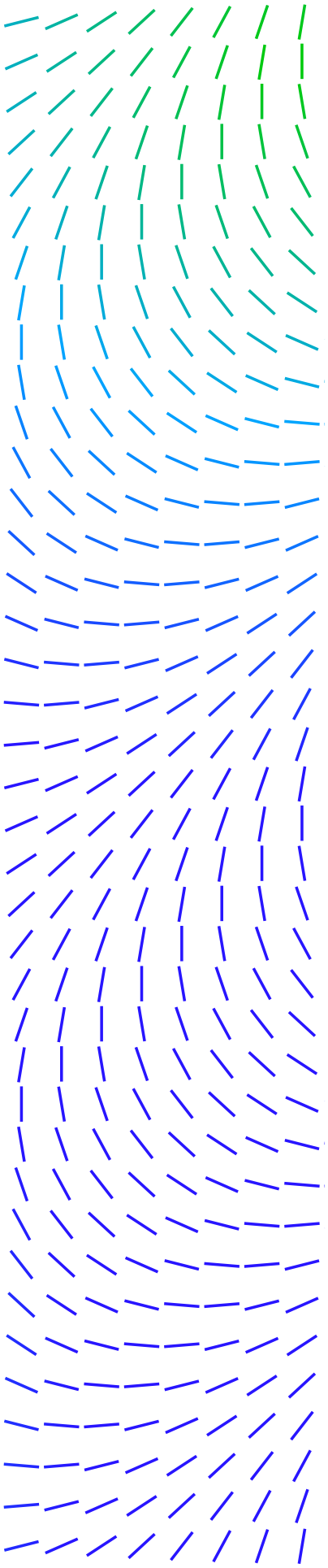

WHITEPAPER

# Protecting the Private Cloud with Integrated and Automated Security

Trellix

# Table of Contents

# Protecting the Private Cloud with Integrated and Automated Security

## Executive Summary

Enterprises have evolved their data centers to include private clouds, and they have started virtualizing the network as well. However, with the evolving data center technologies, they are challenged to secure these environments. Breaches in the data center are difficult to detect and can go unnoticed far too long. Advanced analysis capabilities are needed to effectively improve detection capabilities of sophisticated advanced attacks within the data center. Organizations are dealing with increased complexity with too many siloed technologies to help deliver contextual insights for threat protection. Security administrators often lack the technical expertise to accurately manage the threat landscape, or there is a shortage of people to handle critical activities. Customers need to find threats sooner and stop them faster.

To realize such security, Trellix offers a solution for protecting the private cloud that comprises several bestof- breed, enterprise-class security products:

- Trellix Intrusion Prevention System
- Trellix Management of Optimized Virtual Environments (Trellix MOVE Antivirus)
- Trellix Intelligent Sandbox
- Trellix ePolicy Orchestrator (Trellix ePO)
- Trellix Threat Intelligence Exchange
- Data Exchange Layer

The role of each product in this solution is described further in this white paper.

### Business challenge

Enterprises are moving data centers to hybrid environments that contain physical, virtual, and cloudbased infrastructure from multiple vendors. Data centers contain data and applications that reside on premises and off premises, depending on where your data centers are located. With the network architecture evolving as such, security administrators have less visibility into data and applications across the infrastructure, preventing you from learning how an application works and the threat it poses to assets. For software-defined data centers (SDDC) where the network is virtualized, much of the traffic stays within the data center, requiring not only north-south but also east-west traffic inspection. Security systems focused on north-south traffic, with east-west traffic going undetected at times.

The three key challenges for IT are:

- Lack of visibility into all traffic to ensure they are not victim a targeted attack: Targeted attack will traverse a private cloud environment differently than in a traditional data center. Security architects need to understand the differences, know where to look, achieve visibility, and combat targeted attack in this new environment, as they cannot secure what they cannot see.
- Challenge to match up the agility of cloud while providing security: The last thing the security team wants is to be blamed for slowing down applications, compute time, or services they deliver. As the IT team moves to more dynamic and agile computing, the security needs to adapt and move just as fast.
- Lack of ability to manage security policies while ensuring strong service level agreements (SLAs): Insufficient security staffing can impact effective and efficient management of security across private clouds. Moreover, it is crucial to have a security solution that is easy to deploy on virtualized networks that extend from traditional

on-premises networks to the software-defined data center (SDDC).

Enterprise IT is seeking solutions to help them with these challenges, and these solutions should not only be just security point products but also integrated and automated. Specifically, IT would like to see the following outcomes:

- Security visibility of all private cloud workloads: With the elastic compute of private cloud, maintaining visibility and control even with a dynamic architecture is key. Moreover, integrating their private cloud security system in, with the rest of their IT security systems will speed up defense against a targeted attack.
- Ability to secure an ever adapting private cloud environment: When security is weaved in right from deployment of a private cloud environment, this objective can be achieved. Security should not be an afterthought.
- Simplified security management to efficiently deliver on SLAs: Having strong management tools and the ability to monitor security policies and provide insight is key to success. IT must have the management tools in place to be able to provide these reports and share insights.

## Solution Overview

The Trellix solution for the private cloud provides the answer to protecting physical and virtual environments within data centers. The solution provides visibility into data and applications running in these environments. This solution offers both virtual network security and virtual machine-based security through Trellix Intrusion Prevention System (Trellix IPS) and Trellix MOVE AntiVirus.

The private cloud security solution provides a centralized management system where you can define security policies, monitor security status, and respond to threats. Security policies are automatically applied as the compute resources scale up and as they scale down. This solution also provides a management console for endpoint security solutions through Trellix ePO software and for deploying security within the SDDC through the Open Security Controller from Intel.

## Components of the Solution

Several individual security products come together to offer an integrated and automated security solution, as illustrated below. Each product is defined in this section, along with its role in protecting a private cloud data center.

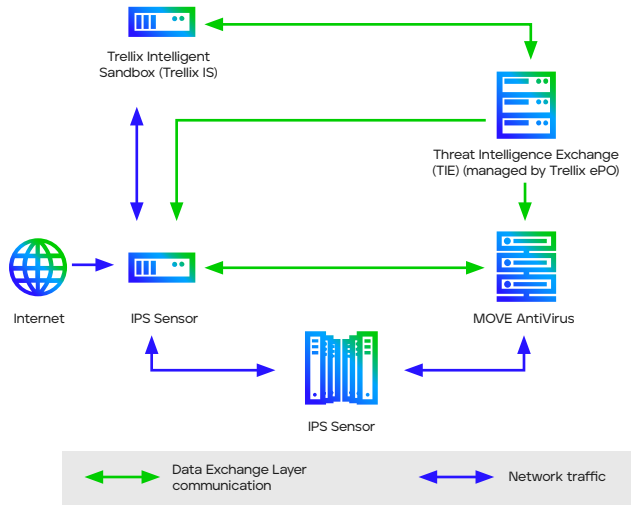


**Figure 1.** Trellix solution architecture.

### Trellix Intrusion Prevention System

The IPS Sensor from Trellix Intrusion Prevention System (IPS) is the component that detects any threat present in network traffic. It can either be a physical IPS sensor, virtual IPS sensor, or a virtual security system that has multiple instances of a virtual IPS sensor. It all depends entirely on the expected throughput, your data center architecture, and intended functionality.

Similar to a physical sensor, you use a manager to configure and manage virtual sensors. This manager can be installed on a physical server or on a virtual machine. Also, you can use the same manager to manage both virtual and physical sensors, including heterogeneous sensor environments.

Whenever the IPS sensor detects a suspicious file that cannot be determined malicious by other malware scanning engines, the sensor sends the file to Trellix Intelligent Sandbox for static and dynamic analysis. Trellix Intelligent Sandbox returns a score for the file. Based on this score, the IPS sensor initiates the configured response actions such as blocking the file.

### Trellix MOVE AntiVirus

Trellix Management for Optimized Virtual Environments AntiVirus (Trellix MOVE AntiVirus) is optimized for protecting virtual environments. It eliminates the need to install an antivirus applications on every VM, while providing the protection and performance needed for your organization's requirements.

Multiplatform and agentless deployment options offload all scanning to a dedicated security VM—an offload scan server. Guest VMs are no longer required to run antivirus software locally, which improves performance for antivirus scanning and increases VM density per hypervisor.

When Trellix MOVE AntiVirus detects a threat either during an on-demand scan or an on-access scan, it queries Trellix Threat Intelligence Exchange for the reputation score through the Data Exchange Layer. If Trellix Threat Intelligence Exchange does not have a score for the file, the file is sent to Trellix Intelligent Sandbox for sandbox analytics.

### Trellix Threat Intelligence Exchange

Trellix Threat Intelligence Exchange is a repository of file reputation details accessed by security solutions across the network. By providing file reputation, it enables a security administrator to take corrective action or a connected security product to take an automated action based on policy. As Trellix Threat Intelligence Exchange is installed within Trellix ePO, you can use the Trellix ePO platform dashboard to deploy policies to the server.

Data Exchange Layer is the main communications infrastructure that Trellix Threat Intelligence Exchange uses to communicate with the IPS sensor, Trellix MOVE Antivirus, and Trellix Intelligent Sandbox. In general, communications to and from the Trellix Threat Intelligence Exchange servers are always through the Data Exchange Layer.

### Data Exchange Layer

Data Exchange Layer is a real-time, bidirectional, communications infrastructure. It provides the framework that enables context (situational awareness, commands, events, and more) to be shared among different Trellix products. Network, endpoint, database, application, and other security solutions are meant to use the Data Exchange Layer to operate as one synchronized, real-time, context-aware, and adaptive security system. Trellix Threat Intelligence Exchange uses the Data Exchange Layer to query for information about file reputation requested by either Trellix Intelligent Sandbox or Trellix MOVE AntiVirus.

### Trellix Intelligent Sandbox

Trellix Intelligent Sandbox is a multilayer security product that includes pattern matching, global reputation, program emulation, static analysis, and dynamic analysis. All these layers are seamlessly integrated to provide you with a single point of control for easy configuration and management. It uses sandboxing technology to provide scores for the malware files sent for analysis.

Trellix Intelligent Sandbox integrates with the IPS sensor to provide malware scores to files. When the IPS sensor detects malware, it sends the file to Trellix Intelligent Sandbox for sandboxing and static analysis. Trellix Intelligent Sandbox then analyzes the file and returns a malware score to the sensor. The IPS sensor then takes the configured corrective action, depending on the score. The Trellix Threat Intelligence Exchange server communicates with Trellix Intelligent Sandbox through the Data Exchange Layer to provide file reputation for malware files.

### Trellix ePolicy Orchestrator (Trellix ePO)

Trellix ePO is an extensible platform for centralized policy management and enforcement of your system security products: antivirus, desktop firewall, and antispyware applications. Trellix ePO can be integrated with multiple products - either from Trellix or third party vendors to deploy polices to the endpoints. In this solution, Trellix Threat Intelligence Exchange server is managed by Trellix ePO. Any policy update that has to be made to the endpoints is deployed through Trellix ePO.

## How Trellix Private Cloud Security Solution Works

In the current threat landscape, it is a priority to protect the virtualized environment. With more and more new threats being detected, all traffic flowing in the network needs to be monitored. All environments are exposed to threats from outside and inside. The private cloud security solution from Trellix helps detect the malware files in the network.

The IPS sensor acts as the first line of defense for inspecting any traffic entering the network. It inspects traffic packets before allowing it to reach endpoints. When the IPS sensor is not able to detect malware due to unsupported file formats, that file is sent to the endpoint without inspection. In this case, Trellix MOVE AntiVirus helps detect malware during an on-demand scan or an on-access scan. Together, the solution acts as layered protection where malware is either detected before it enters the network or is detected and blocked after it enters the network. This provides complete protection for the virtualized environment regardless of the mode in which it enters the network. The general working of this solution is explained depending on where the threat originates.

### Threats that originate outside the network

- When any known malware attempts to enter the network, the IPS sensor immediately blocks the file, as it already contains information about the malware through attack signatures and on-board heuristics.
- When up against an unknown file that might end being a zero-day attack, the IPS sensor sends the file to Trellix Intelligent Sandbox for static and dynamic analyses.
- Trellix Intelligent Sandbox returns a malware reputation for the file—then the file is either blocked or allowed to the endpoint.
- If Trellix Intelligent Sandbox is not able to send back a reputation within stipulated time, the IPS sensor holds the file for six seconds and then passes it through to the endpoint.
- When the file reaches the endpoint, and an ondemand or on-access scan is triggered, Trellix MOVE AntiVirus queries Trellix Threat Intelligence Exchange for the reputation.
- The file is then blocked by Trellix MOVE AntiVirus if its reputation determined malicious.
- When such a file attempts to enter the network the next time, the IPS sensor queries Trellix Threat Intelligence Exchange and blocks the file.

### Threats that originate within the network

- When a suspicious file is already in the network, Trellix MOVE AntiVirus helps detect such files during an on-demand scan or an on-access scan.
- When Trellix MOVE AntiVirus detects a suspicious file, it queries Trellix Threat Intelligence Exchange for a reputation score through the Data Exchange Layer.

- If Trellix Threat Intelligence Exchange contains a reputation score for the suspicious file, it responds to Trellix MOVE AntiVirus with the score.
- If Trellix Threat Intelligence Exchange does not contain the score, it sends the file for scanning to Trellix Intelligent Sandbox through the Data Exchange Layer.
- When a reputation score is available from Trellix Intelligent Sandbox, Trellix Threat Intelligence Exchange passes it on to Trellix MOVE AntiVirus.
- Depending on the score, Trellix MOVE AntiVirus blocks or allows the file.
- Customized policies for your environments can be configured from Trellix ePO and updated in the Trellix MOVE AntiVirus server.

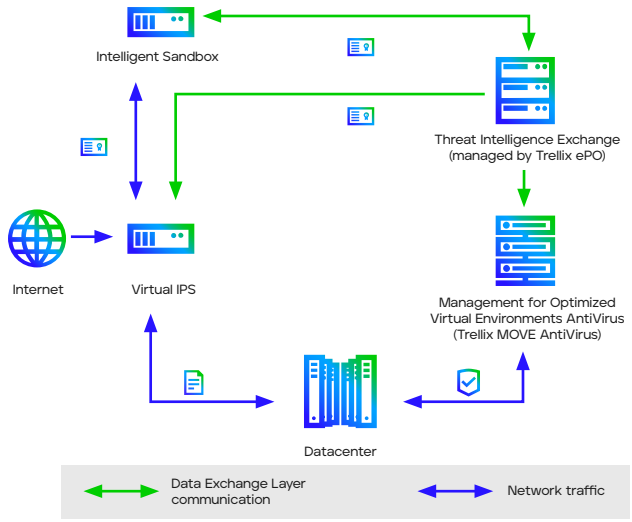


**Figure 2.** Trellix solution architecture for protecting the private cloud.

## Real-World Scenarios to Illustrate Deployment

The processes mentioned in the section above are explained through two real-world scenarios.

### Scenario 1

An endpoint user accesses a web portal and attempts to download a file. The file arrives at the IPS sensor and is scanned using policies configured in the IPS sensor. The sensor establishes that the file is unknown and suspicious, and, after completing the scan using the various malware scanning engines on board, routes the file to Trellix Advanced Threat Defense.

The IPS sensor sends the file to Trellix Intelligent Sandbox for scanning. The sensor has a six-second hold time when the file goes to Trellix Intelligent Sandbox. This hold time means that the last packet of the file is withheld by the sensor. If after six seconds Trellix Intelligent Sandbox does not return a result, the file is permitted into the network. Trellix Intelligent Sandbox shares the results of the scan with Trellix Threat Intelligence Exchange and the IPS sensor. But since the file has entered the network, the IPS sensor cannot block the file and can only raise an alert, after which a security administrator must take corrective action. If such an event occurs during a weekend or after-work hours, there is the likely risk of the malicious file proliferating across the network and infecting other endpoints.

However, when Trellix MOVE AntiVirus discovers a suspicious file on the endpoint during a scan, Trellix MOVE AntiVirus queries Trellix Threat Intelligence Exchange, which had earlier received malware reputation for the file from Trellix Intelligent Sandbox. Trellix MOVE AntiVirus receives intelligence about the file and is able to block it based on the file reputation shared by Trellix Intelligent Sandbox. As for the network perimeter, the IPS sensor is aware of the malicious file and is able to keep it out of the network by blocking it if it makes another attempt at entering the network.

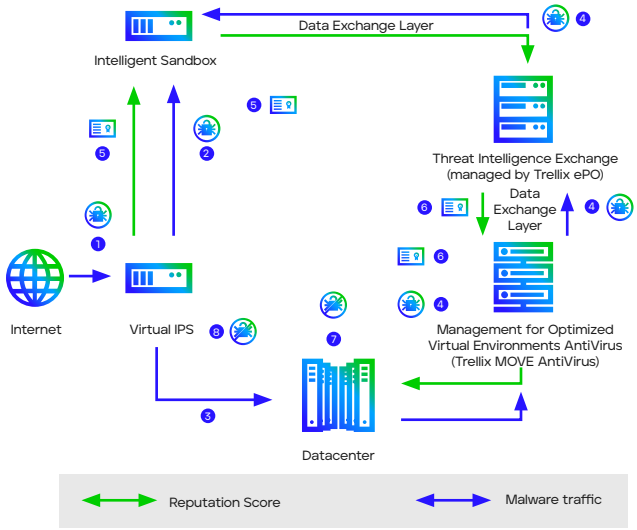


**Figure 3.** Scenario where a malicious file is allowed to enter network due to non-availability of reputation.

Here's how it works:

1. The malware file enters the network from the internet when an endpoint user requests it.
2. The IPS sensor does not have the reputation score for the file. Hence, it sends the file to Trellix Intelligent Sandbox for sandboxing.
3. When Trellix Intelligent Sandbox does not send the reputation score within the stipulated time, the IPS sensor sends the file to the endpoint after the six-second hold timeframe.
4. During an on-demand scan, Trellix MOVE AntiVirus discovers the suspicious file in an endpoint and queries Trellix Threat Intelligence Exchange for the reputation score through Data Exchange Layer.
5. Trellix Intelligent Sandbox has by now shared the malware reputation of the file as "Known Malicious" with the IPS sensor and Trellix Threat Intelligence Exchange.
6. Trellix Threat Intelligence Exchange returns this reputation to Trellix MOVE AntiVirus.
7. Trellix MOVE AntiVirus blocks and removes the file from the endpoint.
8. Since the IPS sensor is aware of the malicious file, it is automatically blocked if it tries to enter the network again.

### Scenario 2

When a file enters the network through a source within the network—such as a USB device, from a demilitarized (DMZ) network, or another vector—an inline IPS sensor does not even see the file. The file that slipped into the network, for instance, on a Linux-based system begins proliferating laterally to Microsoft Windows-based endpoints. At this point, Trellix MOVE AntiVirus detects the suspicious file during a scan and queries Trellix Intelligent Sandbox through Trellix Threat Intelligence Exchange. If Trellix Threat Intelligence Exchange does not have a malware reputation for the file, Trellix MOVE AntiVirus sends the file to Trellix Intelligent Sandbox for analysis.

Trellix Intelligent Sandbox then returns a reputation to Trellix MOVE AntiVirus through Trellix Threat Intelligence Exchange. Trellix MOVE AntiVirus now blocks and removes the file. The next time the file tries to enter the network, the IPS sensor queries Trellix Threat Exchange Intelligence, which responds with a "Known Malicious" file reputation and enables the IPS sensor to block the file.

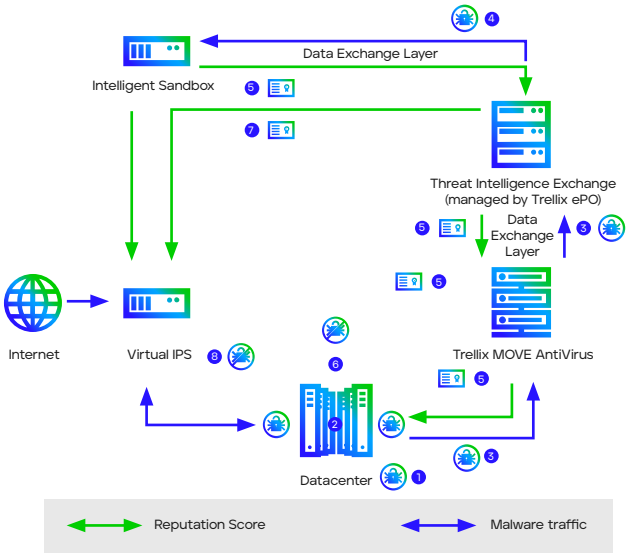


**Figure 4.** Scenario where a malicious file enters the network through an external device.

Here's how it works:

1. The malicious file enters the network through an external device, like a USB device.
2. The file proliferates in the network laterally.
3. Trellix MOVE AntiVirus detects the file during an on-demand scan and queries Trellix Threat Intelligence Exchange for the malware reputation of the file through Data Exchange Layer.
4. Since Trellix Threat Intelligence Exchange does not have the score for the file, Trellix Threat Intelligence Exchange queries Trellix Intelligent Sandbox through Data Exchange Layer.
5. Trellix Intelligent Sandbox returns the reputation to Trellix MOVE AntiVirus as "known malicious" through the Trellix Threat Intelligence Exchange server.

6. Trellix MOVE AntiVirus deletes the file from the endpoint.
7. The next time the file tries to enter the network, the IPS sensor queries Trellix Threat Intelligence Exchange for the score.

The file is blocked.

## Conclusion

Collaboration between all products that encompass the private cloud security suite protects valuable assets within a data center environment from threats, regardless of whether the threat emerges from the endpoint or from within the network. These products include:

- Trellix Intrusion Prevention System
- Trellix MOVE Antivirus
- Trellix Intelligent Sandbox
- Trellix ePO
- Trellix Threat Intelligence Exchange
- Data Exchange Layer