



Trend Micro Deep Security

Endpoint Security 

Similarities and Differences with Cisco CSA

A Trend Micro White Paper | May 2010



TREND MICRO DEEP SECURITY

I. INTRODUCTION

Your enterprise invested in Cisco Security Agent (CSA) because it understands the importance of a defense-in-depth strategy for protecting servers, desktop and laptop computers from threats that can bypass perimeter security. However, with the recent announcement of Cisco's End-of-Life plans for CSA, you need to explore alternatives that will continue to defend your systems from sophisticated, stealthy attacks.

While your need for zero-day protection probably hasn't changed since you first licensed CSA, today's other important realities must factor in to your current decision. Virtualization and cloud computing are fundamentally reshaping the enterprise IT landscape by providing organizations with the ability to consolidate systems, reduce energy consumption, and deliver significant cost savings. And driven by tight economic conditions, the pressure to reduce costs while ensuring compliance with a myriad of regulations, standards, and internal policies has become intense since you first selected CSA.

As such, the ideal migration strategy from CSA must address all these issues and provide comparable or better protection. With a mature, robust and widely deployed alternative to CSA, Trend Micro is pleased to be chosen as a Cisco preferred partner to help CSA customers continue to achieve their information security and business goals. Trend Micro, a global leader in content security and threat management, offers you a compelling solution.

II. TREND MICRO DEEP SECURITY – OVERVIEW

Trend Micro™ Deep Security provides comprehensive, modular protection for servers, desktops and laptops with security features that include anti-malware, deep packet inspection-based intrusion detection and prevention (IDS/IPS), web application protection and application control, stateful firewall, file and system integrity monitoring, as well as log inspection. Deep Security empowers systems to be self-defending, while helping to protect confidential data and ensure application availability. With Trend Micro's migration tools and services, transitioning from CSA to Deep Security is easy.

Key Benefits

Deep Security prevents data breaches and business disruptions:

- Provides a line of defense at the endpoint itself—whether physical, virtual or in the cloud
- Shields known and unknown vulnerabilities in web and enterprise applications, as well as in operating systems, and blocks attacks to these systems
- Allows you to identify suspicious activity or behavior and take proactive, preventive measures
- Detects and blocks a broad range of threats to endpoints, including viruses, web threats, spyware, rootkits, network worms, and blended threats, and prevents exposure to web threats





TREND MICRO DEEP SECURITY

Deep Security enables compliance:

- Addresses six major PCI compliance requirements—including file integrity monitoring, web application security, and server log collection—along with a wide range of other compliance requirements
- Provides detailed, auditable reports documenting prevented attacks and policy compliance status, reducing the preparation time required to support audits

Supports operational cost reductions:

- Offers vulnerability protection so that secure coding efforts can be prioritized and unscheduled patching can be cost effectively implemented
- Provides the security necessary to fully leverage virtualization or cloud computing, which significantly lowers costs
- Delivers comprehensive protection in a single, centrally managed software agent, eliminating the need for (and costs associated with) deploying multiple software clients

Before examining the modules and architecture, it is important to understand the key similarities and differences between CSA and Deep Security.

III. UNDERSTANDING THE SIMILARITIES AND DIFFERENCES

SIMILARITIES

Like Cisco CSA, Trend Micro Deep Security was designed to protect endpoints (servers, desktops and laptops) from a broad range of targeted, known and unknown attacks. Both products feature an enterprise architecture supported by software agents that enforce security policies, and both are centrally managed using a web management console. These two solutions protect a wide range of operating systems, including Windows, Linux, Solaris, and Unix. And while early releases of each product were principally considered host intrusion prevention systems (or “HIPS”), each has evolved to include additional protection capabilities. Both products have the scalability and performance necessary for large enterprise deployments. And, like earlier releases of CSA, Deep Security was designed to work as a complement to an anti-malware solution, allowing customers the flexibility to choose the right solution for their needs.

Both Deep Security and CSA have enjoyed broad commercial success, with their core protection modules having been deployed to millions of endpoints in a broad range of industries, including Fortune 1000 and Global 100 organizations in financial services, retail, energy and defense, as well as to small to mid-sized companies in a broad range of sectors, and to universities, school boards, healthcare providers and governments alike.



TREND MICRO DEEP SECURITY

Table 1 provides a summary comparison of the two products in terms of the protection they provide, the platforms protected, and other key features, such as integration.

Table 1: Comparison of Cisco CSA and Trend Micro Deep Security

	Cisco CSA	Trend Micro Deep Security
Protection Provided		
IDS / IPS	✓	✓ Detect and prevent, or detect-only modes
Firewall	✓ Application firewall	✓ Stateful, bi-directional network firewall
Web Application Protection	✓	✓
Application Control	✓	✓
Location Awareness	✓	✓
Integrity Monitoring	✓	✓ Monitors and reports changes to files, directories, services, ports, installed software, registry keys and values
Log Inspection		✓
Data Loss Prevention	✓ Available in r 6.0	✓ Available through other Trend Micro solutions
Antivirus	✓ Available in r 6.0	✓ Virtualized environments only (also available for physical endpoints through other Trend Micro solutions)
Protection From		
Buffer overflow	✓	✓
SQL injection	✓	✓
Cross-site scripting	✓	✓
Denial-of-Service	✓	✓
Malicious file execution	✓	✓
Information Leakage and Improper Error Handling	✓	✓
Rootkits	✓	✓ Available through other Trend Micro solutions
Viruses, phishing, spyware	✓ Available in r 6.0	✓ Virtualized environments (also available for physical endpoints through other Trend Micro solutions)
Protection For		
Windows	✓ 2000 Server 2003 XP Vista (32 bit) WEPOS 1.1	✓ 2000 Server 2003 (32 & 64 bit) XP (32, 64 bit, embedded) Vista (32 & 64 bit) 7 (32 & 64 bit) 2008 (32 & 64 bit)
Solaris	✓ 8, 9, 10	✓ 8, 9 10 (SPARC & x86)
Linux	✓ Red Hat 3, 4, 5 (32 bit) SUSE 10	✓ Red Hat 4, 5 (32 & 64 bit) SUSE 10, 11



TREND MICRO DEEP SECURITY

	Cisco CSA	Trend Micro Deep Security
Other		✓ HP-UX 11i v2, v3 AIX 5.3, 6.1 (Log Inspection and Integrity Monitoring)
Virtual machines		✓ Virtualization-aware and guest-based
Integration		
With Cisco NAC, NIPS, MARS	✓	✓ Via Syslog
With VMware vCenter		✓ ✓
With Microsoft Active Directory		✓ ✓
With SIEM		✓ Via Syslog
Open APIs		✓ Web Services API
Other		
Management Console	✓	✓ Customizable, intuitive dashboard Detailed security event summaries Recommendation scan
Reporting	✓	✓ Customizable, multiple formats (pdf, doc, xls)
Localization	✓ English, Chinese, French, German, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish	✓ Deep Security 7 is internationalized. Deep Security 7.5 localization kit available Q3, 2010
Certification		✓ Common Criteria EAL 3+ (EAL 4+ in progress)

KEY DIFFERENCE: BEHAVIORAL VERSUS NETWORK APPROACH

As with any two security solutions, Deep Security and CSA have many differences. The principal difference between the two products is the way in which they detect and block attacks or malicious code. CSA uses a behavioral approach, while Deep Security uses a network-based approach. Both operate at the host level.

The Behavioral Approach

Products like CSA examine the characteristics of executing code with the objective of detecting and blocking malicious code before it can damage the system. Hence, it learns what “normal” behavior is for a host, and applies protection whenever something strange or anomalous occurs. The behavioral approach represents the last line of defense because the malicious code has already entered the system and has started executing. This approach uses techniques such as system call interception, which monitors the interaction between application software and the operating system. The goal of this particular technique is to establish a baseline of “known good” application behavior and to “lock down” access solely to network resources needed by the application to successfully perform its requisite functionality. For example, this could mean limiting an application’s access to allowed network ports or disk areas only, or preventing a



TREND MICRO DEEP SECURITY

browser from executing JavaScript that invokes a command prompt and opens port 25 (SMTP), for this could be used to launch malicious code that could propagate throughout the network via email.

CSA provides a broad umbrella of protection that covers any operational anomaly. As a result, it can protect more than just the network interface and can cover attacks launched from portable storage devices and the keyboard. It also does not need signature updates, as the agents provide zero-day protection once they are trained on “normal” behavior.

However, there are also a number of important operational security issues associated with the behavioral approach used by CSA.

- **Slower time to protection:** Because this technique is behavioral-based, it must learn which behaviors are acceptable and which are not. As such, with this learning period, it can take time to configure and fine tune the system in order to minimize the number of false positives.
- **Operational overhead:** Products that use a behavioral approach also have relatively high maintenance requirements. In order to be updated with patches being applied to the host, each host must be trained to establish the rule set and then continuously retrained as software (operating systems and enterprise and web applications for example). Tuning the rules and policies with this approach can be quite extensive. It also requires administrators to be trained, or familiar with, embedded aspects of an operating system, such as all underlying operating system calls that a web server can make.
- **Clean-up time:** Systems like CSA allow malicious code onto the host, but then stop it from executing. However, since the malicious code is still on the host, in most cases, it would require time-consuming clean-up.
- **Cryptic alerts:** Since the behavioral approach generates alerts for anomalies that were learned during the “adapt period,” the result can often be very cryptic. For example, a known worm propagation might generate the following alert: “cmd.exe executed 4 heap memory calls outside of the baseline.” However, an administrator might generate the exact same alert simply by opening a command prompt and executing a data archive script. The file and network correlation data would then have to be analyzed in order to determine what happened. But even then, it’s not always easy to do. A host IDS/IPS relying solely on a behavioral approach not only generates many false positives, the analysis required to determine why an alert was generated is rarely easy and sometimes inconclusive.
- **Lack of visibility into protection:** With a behavioral approach, you can’t tell, or prove, what type of attacks you’re being protected against, or whether a specific vulnerability is protected. This can be problematic for auditing purposes. The only way to be sure is to test the malicious code on a host and confirm its outcome.



TREND MICRO DEEP SECURITY

The Network Approach

Products like Trend Micro Deep Security examine the incoming and outgoing network traffic stream to protect against malicious code with the goal of detecting, blocking and removing it before it ever gets onto the machine. The enforcement point is kernel mode-based, meaning it operates independent of the operating system and applications. This allows it to provide continuous protection without rebooting the system, even when new rules are applied or when there have been other application patches or software updates applied to the systems. Although this approach has a smaller coverage umbrella compared to the system execution control style of CSA, it does cover the network interface, which is the attack vector of greatest concern. In many cases, such as servers in the DMZ, this is the highest security priority.

- **Proactive protection:** In contrast to the behavioral approach, the network style is more proactive in that it stops malicious code before it ever gets on the host. Instead of training, Deep Security uses security rules to detect and prevent attacks. These rules are different from the reactive, exploit signatures used by antivirus engines. They are proactive, as they cover the vulnerability rather than individual exploits. As an example, consider the recent Google/Aurora attack. There was only one vulnerability, in this case CVE-2010-0249, but over 50 different exploits were created and approximately 50,000 payloads were observed. Deep Security, through its Labs team, protects against attacks like these by developing new rules whenever a new vulnerability is detected in an operating system or enterprise application. These rules are then automatically delivered to endpoints for further detection and prevention of an attack.
- **Faster time to protection:** One of the advantages of Deep Security is that a learning period is not required before full security protection is deployed. The administrator simply runs the recommendation scan to determine which rules to apply, then applies one or more existing rules from an extensive set of pre-configured rules. Administrators can also create new rules with appropriate application types selected. This security profile is then assigned to a set of hosts, making protection immediate. Normal application behavior changes and patches do not cause any false positives with a network approach.
- **Detection and/or prevention:** Deep Security can operate in either detect-only mode or detect and prevent mode. This is an important consideration for organizations that want to deploy HIPS in a phased approach. By initially operating in detect-only mode, the security rules can be further tuned at the application and sub-module level to maximize their effectiveness. This also allows the security team to demonstrate to key stakeholders that the addition of this important layer of security has no noticeable impact on system performance or availability.
- **Fewer false positives:** Upgrades or patches to any of the infrastructure components, such as the operating system or web and applications servers, have little or no impact on the agent itself, resulting in relatively few false positives.
- **Visibility into attacks:** Deep Security's reporting capabilities inspect both inbound and outbound network traffic, so that administrators gain full visibility into attacks. They can see the type of attack, attack variant, source IP, date, hosts targeted, and which rule stopped it.



TREND MICRO DEEP SECURITY

Other key differences: Another key difference between the two products is the management system. Deep Security's centralized, web-based management system is used to create and manage security policies, and track threats and the preventive actions taken in response to them. Role-based access allows multiple administrators, each with different levels of permission, to operate different aspects of the system and receive information appropriate to them. With a highly intuitive and familiar explorer-style UI, its' other key features include:

- **Customizable dashboard:** Allows administrators to navigate and drill down to specific information, providing visibility into threats and the preventive actions taken against them. Multiple personalized views can be created and saved. The figures below depict contrasts between the two management consoles.

Figure 1: Trend Micro Deep Security Management Console



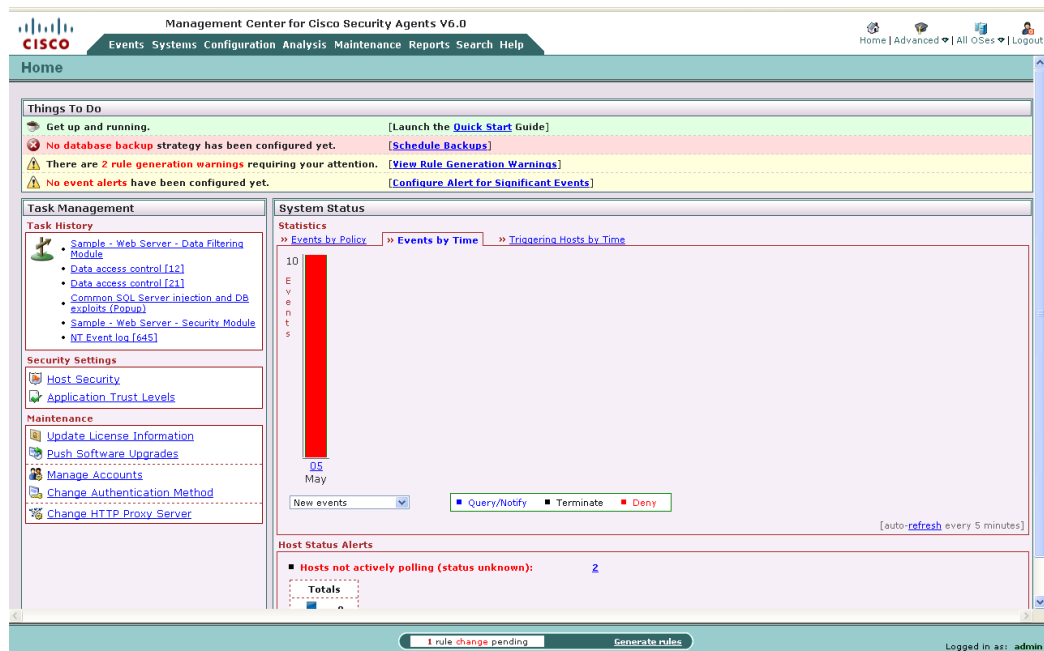
C





TREND MICRO DEEP SECURITY

Figure 2: Cisco CSA Management Console



- **Detailed reporting:** Deep Security attempted attacks to provide an auditable history of security configurations and changes. Reports can be customized and provided in PDF, DOC, and XLS formats.
- **Recommendation scan:** It also profiles the host being protected—identifying OS version, service pack and patch level, and all installed applications—and uses this information to determine potential vulnerabilities of the endpoint. Based upon this information, the Deep Security Manager recommends additional security rules that will shield the endpoint's vulnerabilities from exploit. In addition, as the endpoint environment changes, Deep Security automatically adds and removes security rules. This “auto-tuning” ensures the appropriate protection is applied to each host and improves operational efficiency.
- **Event tagging:** Streamlines the management of high-volume events by allowing administrators to apply predefined or custom labels to events generated by Deep Security. Event tagging can be manual or automatic. It improves the efficiency and quality of analysis, decision making and auditing by narrowing the number of events to be analyzed, with specialized views of events on the dashboard and in reports.
- **Risk ranking:** Allows security events to be viewed and sorted based on asset value, as well as vulnerability information.
- **Scheduled tasks:** Simplifies maintenance with the ability to schedule routine tasks, such as reports, updates, backups and directory synchronization for automatic completion.





TREND MICRO DEEP SECURITY

Beyond the management system, other differences between Deep Security and CSA include:

- **Platforms protected:** Deep Security supports a broad range of operating systems and versions, including Solaris 10 (SPARC and x86), Linux (32- and 64-bit), and SUSE 11. It also supports HP-UX and AIX for the Integrity Monitoring and Log Inspection modules.
- **Protection for virtualized and cloud computing environments:** Deep Security protects endpoints in physical, virtual, and cloud computing environments (both public and private). In addition to providing guest-based protection, it leverages VMware APIs to provide virtualization-aware protection, giving customers deployment flexibility.

IV. THE DEEP SECURITY DIFFERENCE

Trend Micro server and application protection addresses the challenging operational security and compliance needs of today's dynamic datacenter. It provides comprehensive protection, greater operational efficiency, superior platform support, and tighter integration with existing investments. With Deep Security, you'll obtain:

- **Deeper protection:** Provides stateful firewall, intrusion detection and prevention, application-layer firewalling, file and system integrity monitoring, anti-malware and log inspection—all in a single solution. Modules can be licensed independently.
- **Greater operational efficiency:** Deploying quickly and widely, and automating many key tasks—including the recommendation of appropriate protection to be applied to each endpoint—Deep Security can be managed more efficiently, with minimal impact on existing IT resources.
- **Superior platform support:** With full functionality across more platforms, and faster support for current versions of these platforms, you can continue to adopt the newest virtualization platforms and operating system releases without sacrificing protection.
- **Tighter integration:** Offers tighter integration with IT infrastructure, including directory and virtualization platforms and other best-of-breed security investments such as SIEM, to help ensure effective enterprise deployment and continued vendor flexibility.

With similar protection capabilities delivered through a network-based approach, a powerful and intuitive management console, and tight integration with VMware and other enterprise infrastructure, Trend Micro Deep Security makes the decision to switch from Cisco CSA a natural and wise one.

For more white papers on Trend Micro Deep Security, go [here](#).

For more information on other Trend Micro products, please visit us at www.trendmicro.com/go/enterprise/

To schedule a demo, please call +1-877-21-TREND