CSA Migration FAQ

Cisco has announced the End Of Life for the Cisco Security Agent. Current CSA customers will have questions as they plan a migration to a replacement. Bit9 offers the industry leading White Listing agent which can replace CSA functionality, and is much easier to manage. This document provides answers to many frequently asked questions about Bit9 in comparison with CSA.

What is Bit9 Parity?

Bit9 is considered the leader in application whitelisting by research analysts covering endpoint security and application control. At the Gartner IT Security Summit 2008, Gartner said Bit9 was the leading provider of application whitelisting solutions, which are the "foundation for the future" of endpoint security.

> "Bit9 differentiates itself from its competitors by focusing on making the management of whitelists and black lists less burdensome for IT departments. Most notably, Bit9 has built a vast repository, the Global Software Registry that catalogs "known good" and "known bad" applications and files, and serves as the policy enforcement center for Bit9 Parity."
>
> "Cool Vendors in Infrastructure Protection", Gartner Group April 2008
> Ray Wagner, Peter Firstbrook, Arabella Hallawell, Lawrence Orans, Greg Young, Neil MacDonald, John Pescatore

Gartner

Why is it a credible replacement?

Most Cisco CSA customers use CSA for one or more of three functions: stopping known and unknown attacks, controlling desktop and server applications to meet policy requirements, and compliance (especially for PCI). The Bit9 Parity agent performs these same functions.

Known and Unknown attacks are stopped by whitelisting and blacklisting. A White List specifies authorized applications that are permitted to run; a Black List is the opposite – it specifies known malicious or undesired applications that are blocked. What is unique about Bit9 is the almost 8 billion records in the Global Software Registry™ database, which removes the burden of identifying good and bad from the administrator. Known attacks will be on the black list, and will be stopped because they are recognized. New and unknown attacks will not be on the white list, and so will be blocked from running because they are not recognized.

Servers and desktops can be controlled per corporate policy by using the same white list. For example, if Instant Messenger applications are prohibited, they are added to a "Black List" by the administrator.

Creation of both White and Black lists is simplified by a software inventory capability which collects a list of all applications installed in the environment and classifies them by category (Instant Messenger clients, Media Players, Hacking Tools, etc).

PCI Compliance is an area of focus for Bit9, and the Parity agent provides compliance for PCI DSS requirements 5, 10.5.5 and 11.5. Bit9 also offers compliance modules for NERC CIP, HIPAA, FDA, and SOX.

Is it like CSA?

Bit9 Parity™ is an Agent-Manager architecture, similar to CSA. Rather than hooking Operating System calls like CSA does, the Parity agent relies on Bit9's enormous database of "known good" and "known bad" file hashes (over 15 million applications comprising almost 500 million unique files, with 8 billion application-file matches). As applications are patched by vendors, Bit9 crawls their download sites to capture the latest files and generate a hash. This means that most of CSA's management complexity ("Is it good or bad that this process is attempting this task?") becomes irrelevant – if this is one of the applications that you use, Parity can tell you that this is in fact the application, and not malware trying to masquerade as it. The "Live Inventory" simplifies deployment: the agent scans all executables currently installed and compares them to the database of known good/bad.

Architecturally, agents report to the centralized console, just as with CSA. Like CSA's "Audit Mode", it can audit but not block applications. Up to 50,000 agents can be controlled by a single console.

How did Bit9 Parity stop the latest attack?

CSA offers a Defense-in-Depth to block unknown malware, observing various stages of the attack lifecycle as it unfolds. By correlating events triggering different CSA rules, previously unknown malware can be blocked.

The most important CSA rules in this process are the ones that classify "downloaded content" that executes. Since much of the new malware exploits flaws in web browsers to silently download, this is often the first time that CSA sees the new malware.

Bit9 Parity works at exactly these same stages: when executable content is written to disk, when it attempts to execute, and when it tries to modify system startup configuration (RUN, RUNONCE keys, .INI files, etc). By ensuring that only authorized applications can do these, new unknown malware is stopped just as with CSA.

How does Bit9 Parity Improve Manageability and Understandability?

CSA customers will notice manageability and understandability as the biggest differences. Rather than the sometimes opaque CSA policies, the white list/black list concept is much simpler. The amount of tuning required to deploy an operational system is much less than that required by CSA, and administrators do not have to weaken default security policies to get the system operational.

Day-to-day administration is further simplified because of the richer integration with existing IT infrastructure: Active Directory, trouble ticketing systems, Management infrastructure (SMS, BigFix, etc), and SEIM for compliance reporting.

Who has looked at Bit9? Has anyone moved from CSA to Bit9 Parity? What do they say?

Bit9 has case studies of customers who have migrated from CSA to Bit9 Parity. This is a sample; others are available at the Bit9 Contact at the end of this document.

> **Customer: Fortune 1000 Global Information Company**
>
> Bit9 proves secure cost saver for large international market research firm that transitions from Cisco Security Agent to Bit9 Parity Suite.
>
> **Industry:** Information services
>
> **Customer:** Large International Market Research Firm
>
> **Environment:** The global company has more than 400 offices in more than 100 countries and supports more than 2,000 custom applications.
>
> **Business Challenge:** Transition from the complex host intrusion prevention system, Cisco Security Agent, without affecting the firm's security posture.
>
> **Solution:** Bit9 Parity
>
> **Benefits:**
>
> - Able to smoothly and cost-efficiently migrate from legacy CSA to Bit9's Parity without ripping and replacing infrastructure.
> - Automatically generates an application inventory across the more than 36,000 endpoints to see potential problems.
> - Transitions handling of most security alerts to help desk thanks to automated mitigation tools and Bit9 Parity knowledgebase.
> - No longer have to poke holes in security to deal with each application's exceptions.
> - Ease of use means higher adoption rate, which increases the firm's ability to stop zero-day attacks and unauthorized software from spreading to the entire network.

Is the Bit9 Agent localized into languages other than English? If so, which ones?

The CSA agent GUI is localized into Chinese, French, German, Italian, Japanese, Korean, Polish, Portuguese, Russian, and Spanish.

The Bit9 Parity client does not appear in the task bar, and so no end user interaction is available that way. There are two popup messages that can be delivered by the Parity agent based on the policy in use: one informs the user that the application cannot be run as it has been prohibited by corporate security policy; the other informs the user that the application is trying to run and asks whether this should be allowed.

The text of both of these messages can be modified to suit the customer's needs, including localization (8 bit ASCII).

What should I expect the migration to look like?

Priveon has put together a migration plan to move operational CSA deployments to operational Bit9 Parity deployments without having to sacrifice CSA protection during the migration period. It consists of:

Deploying Bit9 Parity while still keeping CSA protection

- While Parity is in audit mode, you still need protection
- Once Parity is configured, you can shift CSA to audit mode (verify protection)
- After Parity is fully deployed and validated, CSA can be removed

Rollout Overview:

1. **Planning**
   - Porting CSA custom policies to Parity

2. **Initial Infrastructure**
   - Active Directory integration
   - Initial inventory and white/black list tuning

3. **Mass deployment**
   - Fine-tune inventory and white/black lists

4. **Training and hand-off**

Who is Priveon?

Priveon is the premier CSA training and deployment services partner, responsible for most of the large CSA customer installation efforts. Their extensive knowledge of CSA policies and rules gave them the ability to more rapidly tune CSA policies for customer environments. In fact, they literally wrote the book on CSA – Cisco Press' book on CSA was authored by Priveon.

Priveon now brings that expertise to Cisco customers looking for a CSA replacement, and who are focusing not just on product excellence, but on operational success as well.

Who should I contact for more information?

Priveon:

Phone: +1 877 783-1337
Fax: +1 866 735-5504
http://priveon.com/csamigration

Bit9:

Phone: +1 617.393.7400
Fax: +1 617.393.7499
http://bit9.com/csamigration