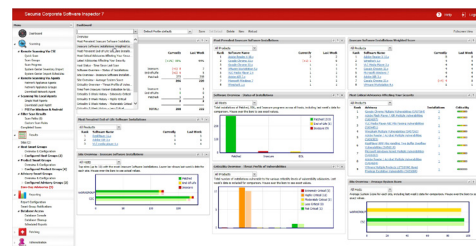


Secunia Corporate Software Inspector (CSI)



While security professionals tend to shy away from cloud-based solutions, those with less stringent security requirements can really benefit from the ease of deployment those types of solutions offer. Secunia's Corporate Software Inspector (CSI) is one such solution, enabling users to leverage its signature-based vulnerability scanner via installable software agents and/or a simple-to-use web-based console.

As the solution is cloud-based, the setup was minimal. After logging in to the website, we downloaded an Internet Explorer plugin and refreshed the page. From there, we were able to conduct our first scan. While setting up the System Center and WSUS integration was slightly more involved, it was nothing excessive and was easily accomplished by following the included documentation.

All in all, we had our first scan results within five minutes of our initial login – this is the power of cloud-based solutions. The Secunia CSI is a signature-based vulnerability scanner, meaning it captures metadata from various software executables and dynamic linked libraries installed on a user's system and compares them to its own centrally managed list. This allows the product to key in on an application's exact version number, which can be compared to its database of vulnerabilities, and reports can be generated based on any matches. Access to the web-based console can be controlled via IP address restrictions and role-based user accounts. While the software was apparently designed primarily for Microsoft systems, with Windows Software Update Services and System Center integrated tightly, there is support included

for Mac OS X and Red Hat Enterprise Linux systems. Notably, regarding the Linux support, while Red Hat is the only distribution officially supported by the product, it relies on the operating system's internal RPM database, so it may be possible to get the product to work with other RPM-based distributions. There are several ways of initiating vulnerability scans: single host agents may be installed on servers or endpoints, an agent may be installed in network appliance mode enabling that agent to scan an entire network, or scans may be initiated via the CSI console. Secunia also offers a Zero-day advisories module, which compares the compiled data from a user's network against a list of currently known zero-day vulnerabilities.

Documentation was provided to us as a PDF file. We found it easy to navigate with bookmarks, screen shots and network diagrams presented where appropriate. The product's features and configuration were clearly explained and we had no trouble during setup or testing.

Secunia offers two tiers of product support: Standard tier includes a setup assistance call and email-based aid with a two-day response SLA. Enterprise level offers full setup and implementation services, with phone and email support on a one-day response SLA. Secunia also hosts a web-based user forum.

The Secunia Corporate Software Inspector starts at \$3,375 per year, which provides one user account and up to 100 scan targets. The standard support package is included with the purchase of the tool, and the Enterprise upgrade is priced at \$1,227 per year.

DETAILS

Vendor Secunia

Price \$3,375 (one year, one user, 100 hosts).

Contact secunia.com

Features ★★★★★½

Ease of use ★★★★★

Performance ★★★★★

Documentation ★★★★★

Support ★★★★★

Value for money ★★★★★

OVERALL RATING ★★★★★

Strengths Simple deployment, integration with Microsoft WSUS and System Center.

Weaknesses Relatively limited support for Mac OS X and Linux devices, cloud-based product may give some security professionals pause.

Verdict Users comfortable with a cloud-based solution will be very satisfied with this product.

Secunia
Stay Secure

Mikado House
Rued Langgaards Vej 8, 4
DK-2300 Copenhagen S
Denmark
Phone: +45 7020 5144
Website: <http://secunia.com/>

Lake Calhoun Business Center
Suite 420
3033 Excelsior Boulevard
Minneapolis, MN 55416
USA
Phone: +1 888 924 8265

SC
MAGAZINE
Reprints