Cisco Security Agent Antivirus

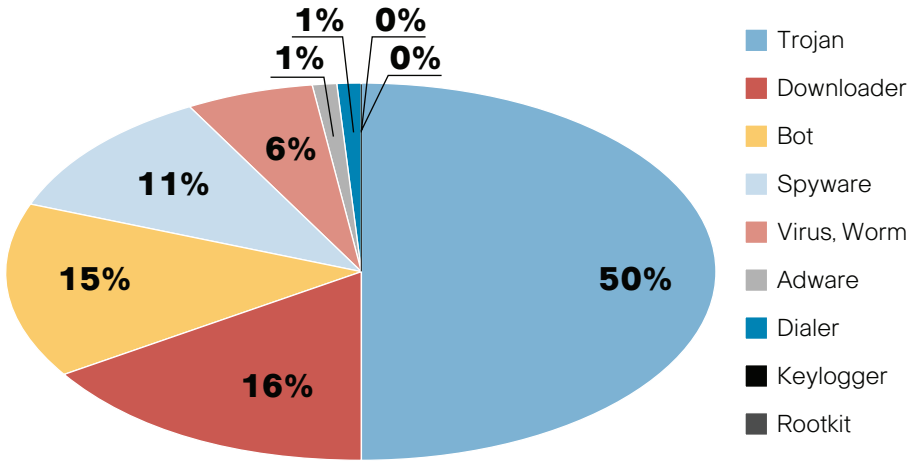
Signature-based antivirus products have long been the mainstay of endpoint security. Although new forms of malware require behavior-based protection for effective day-zero protection, antivirus continues to be a valuable component of endpoint protection strategies. The primary value of signature-based antivirus is providing confidence that malware can be removed from the endpoint, since the malware was identified by name. Although behavior-based controls are the primary means of stopping malware attacks on endpoints, signature-based antivirus plays an important role in identifying the malware, allowing a high level of confidence in malware removal.

Cisco Security Agent is the leading behavior-based endpoint security product. ClamAV™ is widely used on UNIX or Linux e-mail servers, scrubbing the e-mail data flows for malware and protecting millions of Windows desktop systems. Cisco Security Agent Version 6.0 now includes the open source ClamAV antivirus engine to protect Microsoft Windows desktops at no additional cost. This combination offers a complete endpoint protection solution that accurately identifies malware, prevents malware execution, and quarantines or deletes malware from the system.

ClamAV is an open source product, providing strong virus scanning and detection capabilities. The ClamAV database includes more than 200,000 unique signatures, covering many different types of malware: trojans, downloaders (file droppers), bots, spyware, worms, and others.

ClamAV has a reputation for very fast response time when new viruses are released. As a result, it scores well in public antivirus comparisons.

Figure 1. The ClamAV Virus Signature Database



The Shadowserver Foundation is a volunteer organization that gathers, tracks, and reports on malware activity observed on the Internet. The information the foundation gathers is publicly shared with security researchers and vendors.

The Shadowserver Foundation publishes daily, weekly, and monthly statistics about virus detection effectiveness for many antivirus products. As this monthly chart shows, ClamAV has a very high degree of malware detection accuracy.

The integration of ClamAV into Cisco Security Agent provides an ideal complement of security capabilities to provide a complete endpoint security solution:

- Identification and protection from known and day-zero threats
- On-demand scanning
- Identification of rootkits
- Malware quarantining and deletion
- Centralized management, reporting, and policy controls

Table 1.

Vendor	Detected	Total	Percent
AntiVirus	1204953	1229800	97.98%
Vexira	1203678	1229800	97.88%
VirusBuster	1203471	1229800	97.86%
F-Secure	1203244	1229800	97.84%
Norman	1203274	1229800	97.84%
F-Port6	1202403	1229800	97.77%
Clam	1201805	1229800	97.72%
DrWeb	1201442	1229800	97.69%
AVG7	1200639	1229800	97.63%
Avast	1199011	1229800	97.50%
McAfee	1185278	1229800	96.38%
F-Prot	1176390	1229800	95.66%
Panda	1138986	1229800	92.62%
Kaspersky	1036869	1229800	84.31%
BitDefender	1036210	1229800	84.26%
VBA32	994177	1229800	80.84%
NOD32	798148	1229800	64.90%

Source: http://shadowserver.org

Cisco Security Agent is an enterprise-class, centrally managed endpoint protection agent. Agents report to a central management server, the Management Center for Cisco Security Agents. The Management Center provides the administrative interface, allowing security configuration changes, event analysis, granular policy creation, and report generation.

Agents poll the Management Center for Cisco Security Agents periodically for security updates. As part of this polling process, the Management Center distributes daily signature updates to each of the agents. Because of Cisco Security Agent's demonstrated best-in-class protection against new and day-zero malware, agents are protected even if they are out of the office and cannot receive updates immediately. Organizations will find that relying on Cisco Security Agent day-zero protection will allow them to more sensibly manage their antivirus and patching updates.

Table 2.

Delete MalwareFeature	Clam Only	CSA + Clam Combo
Signature Database (>200,000 sigs)	✓	✓
Bulk File System Scan	✓	✓
Rapid Signature Update	✓	✓
On-Demand Scan	✗	✓
Quarantine File	✗	✓

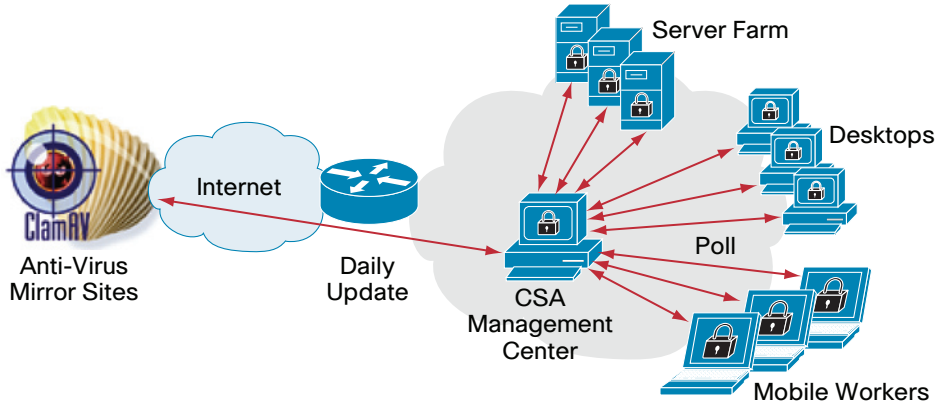
* PC Magazine review 1/22/08
http://blogs.pcmag.com/securitywatch/Results-2008q1.htm

The ClamAV virus scanning engine is packaged with Cisco Security Agent as a single installable agent. It is controlled from the Management Center for Cisco Security Agents console, providing a true single-agent/single-console endpoint security solution.

As a core component of the Cisco Self-Defending Network, Cisco Security Agent also links endpoint security to network security:

- Intrusion prevention system (IPS) and firewall collaboration enhances detection and containment of threats.
- Endpoint enforcement for Network Admission Control enhances security assurance.
- Per-application quality-of-service bandwidth prioritization increases availability of point-of-sale applications.

Figure 2.



For more information about Cisco Security Agent, including video demonstrations about preventing data theft, visit www.cisco.com/go/csa.

C11-458621-00 03/08