



ALL TECH - ALL THE TIME

EXPERT ADVICE

## Redefining Endpoint Security



By Ron Penna  
TechNewsWorld  
07/27/10

**The point at which a device becomes "valuable" to criminals is typically when it combines both the device and the user credentials. As a result, an endpoint should not just be looked at as a device, system, computer, server or laptop. The definition of an endpoint should also include the notion of employees, contractors, third parties, telecommuters, travelers, and other insiders who use these systems.**

---

Most security professionals believe that endpoint security is a strategy in which security software is distributed to end-user devices but centrally managed. Endpoint security systems work on a client/server model. A client program is installed on or downloaded to every endpoint, which in this case, is every user device that connects to the corporate network. Endpoints can include PCs, laptops, handheld devices, servers, printers and even specialized equipment.

Endpoint security software has been around longer than any other information security solution (namely desktop antivirus). Most of the time and effort IT administrators have spent in securing their environments has been focused on endpoint devices. However, most publicly disclosed data breaches include the compromise, exploit, loss, or theft of an endpoint device.

For years, security professionals looked beyond their networks for the source of data breaches. The fear of hackers, cybercriminals, and other external threats drove the market -- and subsequently the majority of information security solutions that are available today. So the vast majority of "endpoint" security solutions attempt to solve the "outsider" problem when in reality it is insiders who pose the greatest threat to organizations.

## **Endpoint = Device + User**

Users often excuse themselves from "patching" and other computer maintenance tasks because they believe nothing of value is on the computer itself. What they forget is the value of that system may not be in what it is storing, but what it can be used for, or what other systems and data it can access.

Often, a device by itself doesn't have access to other systems and data. Usually a system only has this access in conjunction with the credentials of an authorized employee. So in most cases, the point at which a device becomes "valuable" to criminals is when it combines both the device and the user credentials.

As a result, an endpoint should not just be looked at as a device, system, computer, server or laptop. The definition of an endpoint should also include the notion of employees, contractors, third parties, telecommuters, travelers, and other insiders who use these systems.

Perhaps the term "endpoint" should include the notion of insiders due to the symbiotic relationship between the device and the user, which ultimately creates a valuable asset. Once an organization has a valuable asset, it needs to protect it; however, traditional security solutions only solve half the issue, because they are only looking for outside threats.

Endpoint security solutions that focus on digital fingerprinting, code analysis, software behavior, and other technical aspects miss the larger part of the problem -- the insider.

## **The Greatest Threat**

In addition to traditional endpoint security agent software, organizations need a solution designed to protect them from their greatest threat -- the insider. Whether this is a careless, untrained or malicious individual, companies can protect themselves by using technologies designed to mitigate this threat.

Solutions should offer an all-in-one endpoint security suite designed to protect an organization from insider threats through features like data loss prevention, Web filtering, asset management, tracking and recovery and insider monitoring.

A key element in endpoint security is centralized management. Deployment, configuration, updates, reporting, auditing and monitoring must be done centrally, or major security gaps can result. Remote users such as travelers and telecommuters are often excluded due to the limitations of traditional endpoint security solutions.

The most effective endpoint agent can be loaded on any computer anywhere in the world and can still be managed centrally from the same cloud-based management platform.

## Cloud-Based Solutions

To take it a step further, a cloud-based solution (also known as Software as a Service, or SaaS) can offer deployment ease and no hardware requirements, as well as maximum visibility, complete coverage, centralized management and global reporting.

The solution should include multiple risk-mitigation technologies within one agent from one vendor to avoid software conflicts and support nightmares. A combination endpoint/cloud solution can also take care of those remote users, travelers and telecommuters who need the same level of security but often don't get it, because they are not inside the brick and mortar of an office.

Endpoints should include both devices and users, because the combination of the two makes up the greatest threat to organizations today. The next generation in endpoint security software allows IT administrators, compliance officers and executives the ability to control what traditional endpoint security solutions ignore -- the insider. **ECT**