



J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294

Dramatic Changes Coming in Endpoint Security

Current models of endpoint security are becoming outmoded as a more diverse set of mobile and Internet-connected devices become a larger share of the market. The endpoint protection market will change dramatically in the next 3-4 years, with major implications for end users, businesses and the security vendors. Will the vendors be able to change and the end users adapt to the new requirements?

There is a significant change coming to endpoint security, with dramatic implications for how end users will be protected and what security companies must do to remain relevant and competitive. In fact, within 3-4 years, I expect endpoint security to change so much that it will hardly resemble the architecture we currently have in place. The changes will be mostly transparent to users, but will increase their level of protection, extend the umbrella across a much wider array of devices, and protect against a changing threat environment. So what will change?

First, “thick” clients (like current AV and Firewall SW suites) will be slimmed down dramatically, as a result of new platforms that are exposed but not as rich a target as current PCs (e.g., smart phones, tablets, Internet devices). Further, the “thick client” model is mostly broken, as security companies (e.g., McAfee, Symantec, Trend Micro) are finding it increasingly difficult to keep up with an expanding array of malware threats without seriously impacting device performance.

Second, much of the defensive posture will move to the networks and the cloud, where most data delivered to end user devices will originate and where it will be scanned and secured. This means a good deal of the security footprint will be behind the scenes and often invisible to the end user, and with little device impact. Some security SW will remain loaded on the device, but its imprint will be substantially diminished and will provide only basic services.

Third, the network will become much more malware aware than it currently is, and include advanced threat detection based on packet sniffing, smart analysis of traffic, etc. Current network topology is basically designed as a server of bits, with no attempt to detect and correct threats. This posture will change to be much more proactive, particularly as more cloud based services are employed (this will be driven home the first time a major cloud-based service provider is sued over a malware incident causing damage to a customer). Network-based security will become a key component from infrastructure vendors (e.g., Cisco).

Fourth, apps will be downloaded, stored and executed much less frequently on the local device. More use of HTML5 apps means less access to underlying OS, less interaction with other on-

board resident apps, and more protection against device compromise and infection. That does not mean there will be no threat from cloud-based apps. But the threat profile will change, and cloud-based destinations (e.g., Google, Yahoo, Microsoft) will need to assure users that their services are safe and protected.

Fifth, we will see increasing use of Virtualized clients, both through increasing use of thin clients (i.e., Citrix Receiver) and through sandboxed virtual machines on the devices (e.g., VMWare). This will result in application silos that will build a defensive barrier between executing apps, the underlying device, and adjacent apps running in other virtualized silos. Such services will become common place on smart phones and mobile devices within 2-3 years.

Sixth, more security will move into the HW/chip level, in conjunction with cloud based services and virtualization, which will create instantly recoverable systems from threats and infections. This means that the processors/chip sets will be a key component of future security (hence why Intel bought McAfee), and security will become a key differentiator for chip providers supplying device designers.

Seventh, cost of protection will shift from primarily endpoint device SW purchases to embedded costs within services and infrastructure, often on a per user/per service basis. This will disrupt the revenue stream of traditional SW Suite-oriented vendors and some level of security will be offered for free as a service component/differentiator of cloud-based services.

Finally, much more protective services from key security vendors will be available through the cloud, with real time updates and analytical observations of threats.

The companies who currently offer such services (e.g., McAfee, Symantec) are already transforming and applying their significant resources to the task. Smaller players with limited resources (e.g., Trend Micro, AVG, Kaspersky, etc.) will either need to partner with stronger players, be acquired, or fade away.

One threat that will not change dramatically is the user behavior targeted malware attack (e.g., “phishing”). While systems will be put in place to limit such attacks and the damage they can do, ultimately it will remain a “human factor” problem that will need to be dealt with through education, policies and threat information delivery. Technology alone will not be able to eliminate this risk.

Bottom line: The endpoint security transformation will play out over a 2-3 year period. End users should find increasing levels of “security as a service” being offered, with less focus on on-board device SW. Businesses should start planning now for the changes that new device types (e.g., smartphones, tablets) and new services will bring, and work with vendors to create a path to the new security architecture, including at the network and infrastructure level. Failure to do so will lead to unnecessary risk and exposure, and ultimately higher cost of operations.

Jack Gold is the founder and principal analyst at J.Gold Associates, an information technology analyst firm based in Northborough, Mass., covering the many aspects of business and consumer computing and emerging technologies.

For more in-depth comments or analysis on this or other subjects, feel free to contact us.

Jack E. Gold

jack_gold@jgoldassociates.com
www.jgoldassociates.com
508-393-5294

Copyright 2011 J.Gold Associates, LLC. All right reserved.