Highlights from a recent Webcast on IT security

ENDPOINT TO PERIMETER: NETWORK PROTECTION THAT'S INSIDE-OUT AND OUTSIDE-IN

Endpoint protection and perimeter defense must work together seamlessly rather than functioning as separate entities.

Silos are great for farmers, but they're almost always bad news for IT professionals. For years, IT has worked to crack open information and applications silos so that data and systems work together seamlessly and are easy to manage and maintain from a single point of view.

Unfortunately, however, silos have started to show up again in IT departments, this time in the realm of security. Endpoint protection and perimeter defense have, in many organizations, traveled different paths and might even be working at cross purposes. Once again, IT must find a way to open these silos in order to maximize network security and enable users to maintain maximum productivity.

The solution to this challenge lies in deploying systems that communicate from the data center through company-issued computers and all the way out to user-provided devices. Network protection only works if it shields an organization from threats that exist both inside and outside company walls and can actively detect both types of breaches at the same time—all in a way that's easy to manage and doesn't burden the user. Sound impossible? It's not.

New Devices, New Threats, New Problems

An increase in the number of types of devices connecting to the Internet, and with each other, is the primary factor driving the move toward consolidated security solutions and away from silos.

"What happens is that people tend to think about internal security and external security as being two entirely separate things," says Christian Christiansen, program vice president for IDC's security and product services group. "There is a great deal of overlap already. And that overlap is going to increase."

Christiansen cites the convergence of networked devices—from endpoint laptops to tablets to smartphones, to consumer items such as automobiles that are connected via the "Internet of things"—as the primary reason why organizations need to take a holistic approach to security. It's unsafe, and even less manageable, to try to monitor each of those elements individually.

Organizations of all sizes have been experiencing this phenomenon for several years, as users have embraced, authorized or not, the concept of Bring Your Own Device (BYOD) in the workplace. BYOD is causing not only security headaches but also regulatory problems in heavily monitored industries such as finance and healthcare.

wwwAdd to that the concept of accidental breaches, and things get really complicated. Accidental breaches happen when a well-intended employee, for instance, unintentionally sends a sensitive email to the wrong recipients or puts data at risk by transferring it to a cloud service with the aim of working with it at home or during non-work hours. Certainly, employees falling into the trap of phishing attacks would fall into this category as well. These accidental breaches have no malicious intent behind them, but they can cripple an organization nonetheless.

Then there's the issue of knowing whether or not the attack was accidental or whether an outsider has taken over an employee's identity within the company. Sometimes attacks that look accidental are actually malicious and vice versa. The key is being able to see breaches coming before they happen and being able to respond properly once they do occur.

But as important as security concerns are, they're not the biggest driving factors behind the rethinking of security strategies and the elimination of silos. Christiansen says two things are even more important: cost and the user experience.

Maintaining multiple security applications gets expensive, as each needs separate management and maintenance. And the more times users have to type in a password or learn a new interface, the more frustrated they become, and they more they either try to bypass security measures altogether or flood the help desk with calls.

Consolidating Security Infrastructure

Some steps to merging security capabilities are relatively simple. One is implementing single sign-on, which accomplishes the goals of both increasing security around user access and making the computing experience easier for users themselves. Building stronger user authentication for both endpoints and peripheral devices is a necessary element of implementing single sign-on.

Another step is boosting patch management capabilities and incorporating them into the management of both desktop and mobile devices. Patching can prevent a lot of problems, but many IT departments fail to keep up with it properly. Patching desktops internally isn't enough anymore, either. IT security professionals need to know which BYOD devices users are bringing into their environments so that they can keep those devices patched as well.

Beyond that, things get a little more complicated but not out of the realm of possibility. One area with which many IT security departments struggle is threat detection. There are multiple vendors that sell threat detection, and their solutions all have varying degrees of effectiveness. But no vendor or combination of vendors can detect every threat all the time. More importantly, IT professionals need to know how threats might affect their particular systems from the data center, to desktops, to the periphery and back.

What IT needs to do is take an inventory of its entire infrastructure, inside and out and including BYOD, and determine which elements of it are most likely to be threatened and how it can protect them. There are solutions that can help with that task, as Christiansen explains.

"You can buy all the threat-intelligence data pieces in the world," he says, "but if you didn't have the context, if you didn't know what your assets were, you didn't know what you wanted to monitor, it would be a useless waste of money.

"So we have external service routers—managed security service routers—that can provide this context and do the analysis, can very carefully look for and discriminate between the false positives and to determine what's really serious and what needs to be followed up on."

And all of this needs monitoring and management needs to be available to IT from a single vantage point. With hiring of IT security experts becoming a nearly impossible and very expensive task, it's more critical than ever that IT security professionals lean on the technology available to make their jobs easier. Vendors that provide a holistic approach to security can actually help IT departments cut costs by eliminating the need to increase headcount.

With the right strategic approach and the right technology, IT security departments can actually accomplish the goals of greatly increasing network protection from the data center all the way out to the periphery while also cutting costs and improving the user experience.

The Dell Approach

Dell takes the type of holistic approach to security today's IT departments need. Dell is a strategic partner that can enable organizations to hone in on their security needs and then help organizations meet those needs. From threat analysis and user authentication through to periphery defense and single-source management and monitoring, Dell has the solutions and the expertise to provide IT departments with a modern security strategy.

A pioneer in the field, Dell develops its solutions and expertise with the goal of eliminating security silos and converging security infrastructure. Dell is uniquely positioned in the industry to build for its customers network protection that truly is both inside-out and outside-in.