Quantum security for the connected age

As global marketplaces grow more complex, evolving possibilities may be harmful or beneficial at any moment. John McClurg, chief security officer and vice president of Dell Global Security, tells how his team puts full-spectrum security into practice.

Present-day enterprises are taking the phrase "well-connected" to a whole new level. Thanks to the cloud, social media and mobile devices, organizations possess virtually limitless ways to interact with customers, partners and employees faster and more frequently than ever before. The bad news? Now threats come from all directions, too — from malevolent outside forces to unaware users to disgruntled trusted insiders.

Some might call this state of affairs pure chaos. But to John McClurg, chief security officer and vice president of Dell Global Security, it represents opportunity. Here, he outlines the converged, connected core model for security that Dell has put into practice — and tells how other organizations can follow his company's lead to combat 21st-century risks.

What does your vision for a secure enterprise look like?

Modern CIOs are constantly challenged to reduce cost-to-revenue ratios. I try to contribute to that effort by holding to an indigenous, minimized security core — an operationally efficient set of technology solutions and professionals — that can be strategically augmented as needed.

My quest started over 20 years ago, when I began developing a converged security model, framed around the simple idea of physical and logical worlds coming together under one umbrella. I've seen countless perpetrators undermine physical vulnerabilities to launch cyberattacks, and vice versa. To effectively secure an enterprise, both sides of that coin must be addressed.

But it's important to note, even the best security products leave organizations exposed to gaping vulnerabilities when they are not connected. Dell's acquisition of critical security players creates an exceptional constellation of technologies and expertise for us to leverage. As a result, we can link to data stores, close security gaps and gain a high level of contextual richness in understanding and responding to attacks.

This converged, connected core model represents a paradigm shift. As we put Dell Connected Security into practice at our company, we see many organizations becoming comfortable with straddling the physical and logical worlds, and discovering the value in that.

How does the Connected Security model come to life at Dell?

Last year, Security magazine ranked Dell No. 1 in the Information Technology/Communications/Media sector[1] for the way we protect our own assets. We may not be the largest organization, nor do we spend the most, but we have established a minimally essential security core that can

[1] "2013 Security 500 Sector Reports," Security magazine, November 5, 2013, qrs.ly/w83u2x5.

"We may not be the largest organization, nor do we spend the most, but we have established a minimally essential security core that can be expanded at a moment's notice. At Dell, we truly believe in being our own best customer."

—John McClurg
Chief security officer and vice president, Dell Global Security
January 2014

be expanded at a moment's notice. At Dell, we truly believe in being our own best customer. We utilize Dell SecureWorks services to monitor our firewalls, helping us cut through the chatter and distill it down to a set of actionable items that our team can focus on. If needed, we can tap into the prowess of hundreds of security warriors on the SecureWorks team and the experience they have garnered from their broad customer base.

We also use Dell SonicWALL secure remote access appliances to provide a stable, secure platform for remote connection, as well as Dell Data Protection | Encryption solutions to protect end-user data and manage endpoint security and compliance. By interlocking our security products and their data, we deepen intelligence and gain a predictive defense. Security professionals are tired of being reactive. This opportunity to be proactive is extremely vital and exciting.

Are business units getting involved?

All around us, the traditional boundaries that delineated our world are changing. The line between work and home life is becoming porous, altering our roles as employees and family members. As those edges blur, we must look at security differently. The traditional notion of a security organization — guns, gates, guards and geeks — must now extend to every corner of the business.

There is a growing appreciation among our customers that business assurance is no longer the sole responsibility of the security team, but something we all must participate in. It is also a core value of the Dell Global Security organization. We lock shields with the business units and critical players throughout the organization to pursue security interests to the far reaches of our enterprise.

What upcoming security challenges should be on the radar?

One of the most interesting security issues right now is the trusted insider conundrum. It is an elusive animal, but one that organizations must address in order to comply with upcoming federal information security mandates. Trusted insider programs utilize early warning indicators to identify and preemptively thwart employees who are likely to compromise critical intellectual property.

The success of these initiatives will rely upon big data by connecting information stores and leveraging deep analytics to predict violations. This approach represents an exciting synergy with Dell Connected Security.

I also believe that social media will continue to drive change within security organizations. We are tasked with understanding not whether but when and how our adversaries will exploit social media, and we must be agile enough to neutralize those threats before they arise. It is up to us as security leaders to step up to that challenge — embracing new technologies and affirming our role as business enablers. PS