Intel IT Business Review

Striking a balance between protection and enablement

Information security has traditionally revolved around keeping the "good guys" in and the "bad guys" out. Taking a page from the medieval playbook, security professionals have tirelessly built higher virtual walls, deeper digital moats, and more capable gatekeepers to suppress nefarious individuals and their cyber armaments.

But times have changed, and it is no longer possible to fully separate the good from the bad.

With the rise of enterprise mobility, real-time collaboration, cloud computing, and application-driven services, data is flowing in and out of corporate networks more freely than ever before.

These trends present a wealth of opportunity for employee productivity and operational efficiency, but they also provide new openings and vulnerabilities for malware and other threats which have become more pervasive and sophisticated. The barrier to entry for malicious actors has fallen, requiring far less in-depth technical knowledge to cause broad ranging harm.

At Intel IT, we accepted and embraced this reality a few years ago with our "Protect to Enable" strategy. It's a novel approach to enterprise security, built on the implicit assumption that compromise is inevitable. Instead of attempting to shutter all vulnerabilities and thwart all attacks, it focuses on flexibility and survivability.

Balance is the key.

"The barrier to entry for malicious actors has fallen, requiring far less in-depth technical knowledge to cause broad ranging harm."

Chris Sellers
General Manager, Intel IT Information Security

Striking a balance between protection and enablement

Our goal is to improve protection and minimize risk, but without hindering the flow of information or the adoption of new technologies. That means we must strike a balance between locking things down and opening them up.

For example, cloud, collaboration, and choice—what we call the "three C's"—were areas of emphasis for Intel IT in 2013. We want to support and enable these things, but they all present inherent security risks and concerns. So we have to find new ways of facilitating and advancing the adoption of the three C's while applying appropriate levels of protection for our users, our information, and our infrastructure.

Three key focus areas are driving our "Protect to Enable" strategy and helping achieve this balance.

Identity and Access Management (IdAM) is the first area of focus, representing the frontlines of our security strategy. Like many companies, we had been struggling with different IdAM capabilities for different systems and programs. There was no single approach to IdAM, which introduced risk and administration challenges, and it was difficult to adapt our IdAM capabilities to enable things like the three C's.

Today, we are completely overhauling our IdAM services and systems. We are currently building a new foundational infrastructure that will support a more holistic identity and access strategy. Instead of multiple tools and policies, we will have a single IdAM hub through which all of our applications flow. This is one of our biggest programs for 2014, and we will start to transition all of our applications to the new IdAM platform toward the end of the year.

The second focus area of our "Protect to Enable" strategy is our Cyber Security Center, the command post for threat prevention, detection, and response. The Cyber Security Center is responsible for analyzing events in our environment, identifying security issues, and initiating a response.

We currently centralize, aggregate, and correlate large amounts of data from disparate systems and capabilities across the corporate environment. Finding the malicious activity across this huge data set necessitates a tremendous amount of data crunching and analytics, and we are constantly working to refine and advance our capabilities.

One of our goals this year is to increase the capacity and efficiency of our Cyber Security Center. We want to track more events, enhance our analytics, and improve the speed with which we identify and respond to incidents. We also want to bolster a closed-loop system that drives continuous improvement and adaptation. As we gather intelligence about new threats and incidents, and as we refine our response measures, we feed those insights back into our detection and prevention systems and capabilities.

Security and Privacy by Design (PbD) comprise the third focus area of our "Protect to Enable" strategy. We are driving our risk mitigation philosophy and privacy principles upstream into our application and service development. By working with our design teams to build greater security and risk awareness into our applications, we can move the needle from reactive to proactive, develop stronger products, and deliver a better user experience.

To integrate privacy into our applications and services, we are focused on applying the principles of PbD. These principles help guide our development teams on privacy considerations at each phase of a product's or service's lifecycle. In essence, we want the latest security intelligence, criterion, and privacy principles built into our applications and services, not bolted on.

But truth be told, there is no finish line when it comes to enterprise security. Infrastructure environments and security risks are too dynamic, and change is the only constant. IT organizations must prevent what they can, detect everything else, and respond with speed. And they must continually adapt their capabilities to an evolving threat landscape.

INTEL IT BUSINESS REVIEW APP

Check out the Intel IT Business Review, a new mobile app (for smart phones) and digital magazine (for tablets). Download this app and you'll receive a regular cadence of articles from Intel IT thought leaders sharing their insights on IT strategy, best practices and examples of the ways IT is committed to deliver business value to Intel. The app delivers rich multimedia content from an extensive portfolio of IT@Intel white papers, videos, radio shows, podcasts, as well as the Intel IT Annual Report. Join in the conversations and connect with other IT professionals via social sharing and help Intel IT keep the conversation going throughout the year.

Download the app: