EXECUTIVE VIEWPOINT

Yasser Rasheed
GLOBAL DIRECTOR OF BUSINESS CLIENT SECURITY

Yasser leads worldwide sales for Intel's hardware-based endpoint security solutions and products, such as Intel® Authenticate solution. Previously, Yasser was the CTO for Intel's Business Client Platform Division, responsible for product definition, architecture and execution of key innovations for Intel's business client platforms. Since joining Intel in 2000, he has led various R&D projects and established Intel's early vision for Digital and Connected Home. Yasser holds a Ph.D. in Electrical and Computer Engineering from the University of Toronto, and an Executive MBA from the University of Oregon.

FOR MORE INFORMATION
visit intel.com/EndpointSecurity

Defense-in-Depth: Critical in the Mobile-Cloud Era

The massive transformation of IT we've seen in the past two years—driven by mobility, cloud computing, and the number and variety of devices—has upended cybersecurity at every level.

The traditional "moat and castle" firewall configuration is no longer sufficient. Security is moving to the device and data level and increasingly relying on hardware enforcement. Yasser Rasheed, Director of Business Client Security at Intel, discusses his views on these new security paradigms.

Q: With the veritable explosion in the amount and variety of network endpoints, how have security strategies and technologies evolved to provide adequate protection?

A: We're facing several changes in the industry today. First is the proliferation of the number of devices. Second is the trend toward mobility. A lot of devices are mobile: notebooks, tablets, phones, and so on. And third is the transition to cloud. A lot of services are offered from cloud providers and no longer within the firewall. So the defense in-depth concept is becoming more critical. In other words, it's not enough to protect the perimeter. You have to bring in this level of protection at the device itself. I see this to some degree as a challenge, but I also see it as an opportunity for companies such as Intel to offer device-level protection in an unprecedented way. And we can do it at the hardware level, below the OS, beyond the typical attack surface the OS and applications are facing today.

"We want to eliminate reliance on the user as much as possible"

Q: what are the strategic imperatives for safeguarding identity and data? And why is that important?

A: Let me use an analogy to explain this. When you protect your house, you control who has keys to it. But there are certain things, such as jewelry or documents, you want to protect at a different level. Identity is about who gets access to those important items, the data classes assigned to them, and where you want to apply different data protection policies.

You need the granularity of protection at the file and folder level. It's like locking the master bedroom and putting a safe in the closet. You can now apply those levels of protection.

This is why we believe that the notion of full disk encryption is a good first step but not enough. Full disk encryption is really kind of a master lock on the device. And as soon as you enter the password, you're in. Today that's done mostly in software. Only a few that use full disk encryption on the hard drive do it with hardware. The point being, it's easier to hack software encryption today, because fundamentally, the keys need to be in memory for the software to work. What we're doing [at Intel] is encryption in the hardware. The keys are never exposed in memory. Are we mitigating software attacks? No. I believe we're designing them out completely. And that's the main difference between Intel's doing things in the hardware versus a stronger software product.

Q: Are passwords passé? What are some of the current best practices for establishing and managing passwords?

A: I believe we need to get rid of password-only access completely and transform access to devices and services. The reality is that you need multiple authentication factors. We classify them as something you know, something you have, and something you are. Something you know—your password, a PIN, a phrase, and so on. Something you have could be your phone, a Bluetooth headset, a wearable, or your ID badge. And the third category is something you are—which means biometrics. We could add where you are—your location—and then who you are: personal biometrics, such as a fingerprint, face, voice, iris, palm vein, and so on.

Q: Is identity protection better served by policy enforcement or applying security technologies such as two-factor authentication?

A: It's not just two-factor; it's multifactor. One is protecting the authentication factors themselves—those three classes we just discussed (something you know, have, and are).

Second, it's protecting the policy you apply. If the policy is not protected, the attacker will move from attacking the passwords or authentication factor such as the fingerprint to attacking the policy itself.

> "It's not enough to protect the perimeter. You have to bring in this level of protection at the device itself."

And the third aspect is protecting the token or set of credentials. You've got to protect those credentials, because attackers will move to that third part if they can't attack the first or the second. You need all three together.

Q: How should security solutions and technologies work with organizational policy to best support security?

A: This is what trips up a lot of companies. Even if you have the best technology, it has to be manageable in a simple and dynamic way. In other words, you must be able to quickly change policy. We develop mechanisms that allow for the right management infrastructure for something like the Intel® Authenticate solution. We also offer plug-ins for existing management consoles.

Q: What are some of the best strategies and technologies for safeguarding data when it moves beyond the firewall?

A: You've got to protect the data at the time of creation and throughout its lifecycle. First, the protection at the time of creation has to be simple and transparent, so the user doesn't have to do anything, since the user is usually the weakest link. And the second part is the protection travels with the document or file itself. If users want to share their files on Dropbox, for example, they can just put it there and it's protected. Only the right user has access. We make it simple on the infrastructure side, by providing the best hardware for encryption and decryption and the best tools for IT to manage the process.

Q: What are the different strategies for protecting data in transit and data at rest?

A: Data is, by definition, now in transit everywhere. Even when you believe that it's at rest, you share drives, share with Dropbox, and share content with yourself on another device. So it's not enough anymore to say I'm protecting it on this device by locking the device's hard drive. We call it protected by default and throughout the lifecycle. So you protect the document at the time of creation, and that protection travels with the document. And that enforcement is done in the hardware, so it's not user dependent. We want to eliminate reliance on the user as much as possible. ■

intel®

To learn more visit **intel.com/EndpointSecurity**

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer, or learn more at intel.com/EndpointSecurity.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps, or visit intel.com/EndpointSecurity.
Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.