PRODUCTS   SUPPORT   SOLUTIONS   DEVELOPERS   PARTNERS   USA (ENGLISH)   Search Intel.com

Blogs@Intel   Jobs@Intel   CSR@Intel   IOT@Intel   Policy@Intel   Technology@Intel   Programmable Logic   IT Peer Network   Intel Developer Zone

TECHNOLOGY@INTEL

Search Technology@Intel

INTEL AFTER MCAFEE: HARDWARE-ENABLED SECURITY TO ADDRESS INCREASING CYBER THREATS

Written by Rick Echevarria | April 3, 2017

We've all read the recent headlines and seen the alarming statistics. According to Cybersecurity Ventures cybercrime damages will cost the world more than $6 trillion by 2021. Cyber identity theft is also on the rise: The biggest online data breach in history came to light last year, involving more than 1 billion user accounts.

Most of us have also experienced this global problem firsthand. It happened to me: A few months ago, I received a call from my credit card's fraud protection line asking if I was anywhere near Nebraska. (I was not.) Fortunately, my account hadn't been breached or compromised, but I was forced to change my credit card for the third time in a year. (Read more about my take on security in the payment industry.)

Clearly, consumers and businesses alike need a dependable foundation for security. Cyber threats are also moving down the stack, from application, software to hardware. That means the traditional model of "software protecting software" isn't enough.

But here's the good news: Intel is in a unique position to meet these increasing security challenges head-on.

Why? Because Intel designs hardware-enabled security solutions with the customer and user experience in mind. By collaborating with partners across hardware, software, and services industries to deliver new security capabilities to market, we help drive an open ecosystem. These solutions and services deliver integrity, reliability, recoverability, and consistency through hardware-enabled security.

And now that McAfee has become a separate company—in fact, one the largest standalone cybersecurity companies in the industry—Intel will continue to work with them, along with many other ecosystems partners, to bring security, privacy, and safety to new levels.

So what does the future of security at Intel look like after McAfee? And what will that mean for our customers and partners? Doug Fisher, senior vice president and general manager of the Software and Services Group, has an excellent perspective on the urgent need for hardware-enabled security—and how Intel is leading the way. Read his blog post to learn more: "Our unwavering commitment to security, post McAfee."

Be sure to follow me on LinkedIn and Twitter (@RJEche) for security insights, best practices, and discussions.

📅 April 3, 2017   👤 Rick Echevarria   📁 Security   🏷 data_protection; IT_security; cybersecurity, security

← Prev post | Next post →

RECENT POSTS

Intel's Quality Point of View: Quality matters!

IPAS: Security Advisories for November 2020

Intel and Cisco: Working Together to Enable Wireless Smart Manufacturing

ABOUT RICK ECHEVARRIA

Rick J. Echevarria is vice president and general manager of Intel Platforms Security Division. He leads Intel's initiative to transform security across the computing landscape, and fulfill the value and promise of hardware-enhanced security. He is responsible for innovating and implementing silicon-based security platform technologies and features, while also driving differentiated connections with Intel's security software that deliver world-class security solutions for people and businesses. Over the course of his more than 20-year career with Intel, Echevarria has provided leadership and innovation across hardware and software engineering, product line management, new business development, sales and marketing, and strategic business planning and management.

View all posts by Rick Echevarria ➡

1 THOUGHT ON "INTEL AFTER MCAFEE: HARDWARE-ENABLED SECURITY TO ADDRESS INCREASING CYBER THREATS"

Richard Curran says:

April 4, 2017 at 2:28 am

Good to get regular insights from Intel execs on how security delivers value to partners and customers .

Comments are closed.