June 7, 2022

Intel Demonstrates Commitment to Security at RSA Conference 2022

Intel's latest security innovations – cutting-edge product capabilities, demos and real-world use cases – were in the spotlight throughout RSA Conference.

SAN FRANCISCO--(BUSINESS WIRE)-- At RSA Conference this week in San Francisco, Intel reinforced its commitment to security. At the event, leaders from Intel and its ecosystem partners came together to discuss how the company is addressing some of the toughest security challenges, including hybrid workforces and an increase in connected devices. Intel's approach remains steadfast, investing in unparalleled people, processes and products to deliver security without sacrificing performance.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20220607005561/en/

Endpoint security starts with Intel. A long-standing co-engineering commitment drives Windows 11 performance, manageability and security capabilities, enabled by layers of Intel hardware protections, from chip to cloud. (Credit: Intel Corporation)

As the cyber and network security landscapes continue to grow and evolve, Intel's goal is to stay one step ahead by driving innovation across products and research to help build strong security communities both internally and externally. Intel's 2021 Product Security Report noted that 93% of vulnerabilities addressed in Intel products were a direct result of Intel's proactive investment in security assurance. Security begins with Intel, and every component in the system — from software to silicon and network to edge — plays its part to help secure data.

Security is a team sport and addressing security challenges requires the entire ecosystem to come together. Intel continues to engage with ecosystem and government partners to advance the conversation on policies, best practices, standards and public-private partnerships that advance security and trust.

New Design Blueprint Enables Fast Deployment of Network Security Workloads

Offering an augmented approach to edge and cloud network security integration, the newly announced Intel® NetSec Accelerator Reference Design will enable improved network and security processing performance, while reducing the overall infrastructure footprint for network and security solution providers.

The first-of-its-kind reference design is a highly efficient blueprint that allows original design manufacturers to quickly build – and bring to market – PCIe add-in cards featuring Intel® QuickAssist Technology (Intel® QAT) acceleration and full Intel-based server functionality, including orchestration and management. Ideal for IPsec, SSL/TLS, firewall, SASE and

analytics workloads, design-optimized cards can be integrated by network and security vendors within their solutions to expedite the integration of network and security functions and maximize the capabilities of server infrastructure at the edge.

Ecosystem partners are currently developing products based on the reference design. This allows systems vendors, solutions integrators and end customers broad choice and the ability to consolidate more network and security workloads onto server platforms without increasing the use of rack space. The reference design also allows development of solutions, like software assets developed on Intel-based platforms, that may be used without additional re-architecting, porting or compiling. Silicom and F5 will be among the first to utilize the Intel NetSec Accelerator Reference Design to offer integration and acceleration of networking and security functions for rapid scale and time to market.

More: The Intel® NetSec Accelerator Reference Design Enables Scale and Flexibility

Project Circuit Breaker Expands with New Events

Following this year's introduction of Project Circuit Breaker, Intel recently completed its first two pilot events, "Camping with Tigers," and "SGX-Guarden Party." This expansion of Intel's existing open Bug Bounty program brings together a community of elite hackers to hunt bugs in firmware, hypervisors, GPUs, chipsets and other hardware. Project Circuit Breaker is part of Intel's effort to meet security researchers where they are and create more meaningful engagement. Intel remains committed to offering training to security researchers, exciting new hacking challenges and opportunities to explore new and pre-release products, as well as new collaborations with Intel hardware and software engineers. More trainings and hacking challenges are on the horizon this summer, starting with, "Alders and Seekers," where participants will test the Intel® NUC Kit including a 12th Gen Intel® Core™ desktop processor with the Intel vPro® Platform, and "Trusted Crossings," which will target a new Intel technology. For researchers who are interested in participating in these upcoming events, applications are now being accepted on the Project Circuit Breaker page.

More: Product Security at Intel | Project Circuit Breaker | Intel's Bug Bounty Program

Hardware-based Security Starts with Intel

In March, Intel announced the latest Intel vPro® platform, powered by 12th Gen Intel® Core™ processors and built for business productivity. This momentum continued at RSAC, where Intel showcased its built-in security capabilities enabling hardware, software and service providers to protect against threats using innovative methods. Intel® Threat Detection Technology (Intel® TDT), part of Intel® Hardware Shield's suite of advanced capabilities on Intel vPro and also available on Intel® Core™ platforms, equips endpoint detection and response (EDR) solutions, such as ESET and CrowdStrike, with CPU heuristics for advanced memory scanning, cryptojacking and ransomware detection. With nearly a billion Intel TDT-capable PCs in the market, these are the only CPU-based malware behavior-monitoring capabilities in market that go beyond signature and file-based techniques.

Intel continues to collaborate with partners such as Microsoft on enhancing security for Windows 11 and beyond, including the integration of Intel TDT into Microsoft Defender for Endpoint. From power-on through boot-up, Windows 11 security protections from Intel are

part of a comprehensive strategy based on hardware layers of security, from chip to cloud. Today, 12th Gen Intel® Core™ processor-based business client platforms deliver highly effective, low-overhead security protections for Windows 11 and the applications and data that run on it.

Additionally, Intel and Dell have been partnering for decades in the commercial device space, employing a holistic approach to security through software-based protections, silicon-based protections from Intel and hardware-based capabilities that help defend against attacks targeting the deepest levels of a device. This co-enablement relationship is founded on the commitment to keeping commercial customer networks secure.

More: Intel Threat Detection Technology | Intel vPro Platform | A Business Built on Intel vPro is a Business Built on Security: Introducing 12th Gen vPro Security | Cyber Threat Detection at the Silicon Level | Intel vPro Security – Can your PC do that? | Windows 11 Security Starts with an Intel Hardware Security Foundation | Security Foundation: Intel vPro® & Dell

Evolution of the Digital Supply Chain

Security challenges in supply chains have become more sophisticated over time, especially when considering the built-in complexity of modern device supply chains where multiple parties can have vastly different security processes, tools and abilities. Intel's supply chain strategy covers several elements including B2B vulnerability disclosure managed in a coordinated fashion with Intel's ecosystem partners to ensure visibility into released mitigations and guidance. It also includes traceability and digital transparency supported by Intel® Transparent Supply Chain that encompasses the tools, policies and procedures that help provide visibility and traceability of hardware components, firmware and systems.

To keep pace with the changing security landscape, supply chain strategies must evolve to augment physical supply chain security with expanded digital supply chain security. These new capabilities would expand supply chain protections to recording and tracking key device information, including manufacturing data and subsequent modifications across its lifecycle.

More: Supply Chain Security is Evolving into a Platform with 'Digital DNA' | Transparent Supply Chain | Smarter End-to-End Security: How Lenovo is Securing the Supply Chain | Supply Chain Security Goes Digital, Learn Why | Introduction to Compute Lifecycle Assurance | Compute Lifecycle Assurance

Confidential Computing Investments Accelerate

Confidential computing is on the rise, as demonstrated last month at Intel Vision with the introduction of Project Amber, a service-based security implementation of an independent trust authority. Project Amber will help provide organizations with remote verification of the trustworthiness of a compute asset in cloud, edge and on-premise environments, and help drive forward adoption of confidential computing for the broader industry.

Customers like BeeKeeper AI are also using Intel® Software Guard Extensions (Intel® SGX) technology and Microsoft Azure's confidential computing infrastructure to provide a zero-trust platform. It enables an AI algorithm to help compute against multiple real-world clinical datasets without compromising the privacy of the data or the intellectual property of the algorithm model, while also accelerating healthcare AI development and deployment

innovation by more than 30% to 40% when compared with the current method.

As workloads expand from the cloud to the edge, it's more important than ever to secure sensitive data. Lockheed Martin Hardened Security for Intel processors is a technology solution that can obfuscate communications and images using Intel SGX and Edgeless Systems is unleashing the power of confidentiality through connected cars. Rooted in silicon, Intel hardware and software-based security creates a trusted foundation to help protect data and support multiparty collaboration while helping maintain data privacy and compliance.

More: Confidential Computing Consortium | Intel Software Guard Extensions (Intel SGX) | Confidential Computing | Intro to Confidential Computing and SGX | Confidential Computing and Trusted Execution Environments | Confidential Computing: Protecting Data at Every Point | Increasing Trust in Confidential Computing with Project Amber

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220607005561/en/

Jennifer Foss
1-425-765-3485
jennifer.foss@intel.com

Source: Intel