March 15, 2021

Intel Study: Transparency and Security Assurance Drive Preference

Organizations are More Likely to Purchase Technologies and Services from Companies that are Transparent about Ongoing Security Assurance

NEWS HIGHLIGHTS

- Global study indicates 73% of respondents say they are more likely to purchase technologies and services from companies that proactively find, mitigate and communicate security vulnerabilities.
- Intel has established systems to deliver security assurance and product innovation that help customers be more resilient to emerging threats.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Today, Intel released the results of a study examining how transparency, security innovation and ongoing security assurance impact purchase decisions. Key findings indicated a preference for technology providers that are transparent and proactive in helping organizations manage their cybersecurity risk.

Building security and privacy into products from concept to retirement is not only a strong development practice but also important to enable customers to understand their security posture and truly unleash the power of data.

“Security doesn’t just happen. If you are not finding vulnerabilities, then you are not looking hard enough,” said Suzy Greenberg, vice president, Intel Product Assurance and Security. “Intel takes a transparent approach to security assurance to empower customers and deliver product innovations that build defenses at the foundation, protect workloads and improve software resilience. This intersection between innovation and security is what builds trust with our customers and partners.”

Study Highlights

Ponemon Institute independently conducted a survey of 1,875 individuals in the United States; the United Kingdom; Europe, the Middle East and Africa; and Latin America who are involved in overseeing the security of their organizations’ information technology (IT) infrastructure. In addition, respondents are familiar with their organizations’ purchases of IT security technologies and services.

Key findings from the study, sponsored by Intel, include:

- Seventy-three percent of respondents say their organization is more likely to purchase technologies and services from technology providers that are proactive about finding, mitigating and communicating security vulnerabilities. Forty-eight percent say their technology providers don’t offer this capability.

- Seventy-six percent of respondents say it is highly important that their technology provider offer hardware-assisted capabilities to mitigate software exploits.
- Sixty-four percent of respondents say it is highly important for their technology provider to be transparent about available security updates and mitigations. Forty-seven percent say their technology provider doesn't provide this transparency.
- Seventy-four percent of respondents say it is highly important for their technology provider to apply ethical hacking practices to proactively identify and address vulnerabilities in its own products.
- Seventy-one percent of respondents say it is highly important for technology providers to offer ongoing security assurance and evidence that the components are operating in a known and trusted state.

Vendor Characteristics

The key findings indicate that specific vendor characteristics affect purchase decisions. In some cases, there is a significant gap between the importance of these characteristics and the ability of the provider to have the capability. Characteristics include:

- Transparency about security updates and available mitigations.
- Vendor's ability to identify vulnerabilities in its own products and mitigate them.
- Ongoing security assurance and evidence that the components are operating in a known and trusted state.
- Hardware-assisted capabilities to help protect distributed workloads and data in use, and to defend against software exploits.

Developing the strongest products requires power, performance and security. Security capabilities rooted in hardware not only provide security assurance against current threats, but also improve software reliability and provide additional layers of protection at the foundation and across workloads to protect against future threats.

Intel's approach is driven by extensive research and continuous integration of key learnings throughout the development processes and practices. As a result, Intel products are designed to deliver security assurance and advance security capabilities.

To read the full report, go to: The Role of Transparency and Security Assurance in Driving Technology Decision-Making

More: 2020 Product Security Report | People, Processes, Products Define Intel's Security Strategy, Intel Newsroom | Silicon as Code, the Cybersecurity Vulnerability Paradox, and the Transparency Requirements for a 21st Century Processor Vendor (IDC white paper, sponsored by Intel)

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.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20210315005033/en/

Megan Phelan
Highwire Public Relations
916-834-0802
megan@highwirepr.com

Source: Intel Corporation