intel vPro® Platform

NAVIGATING A PRODUCT SECURITY JOURNEY

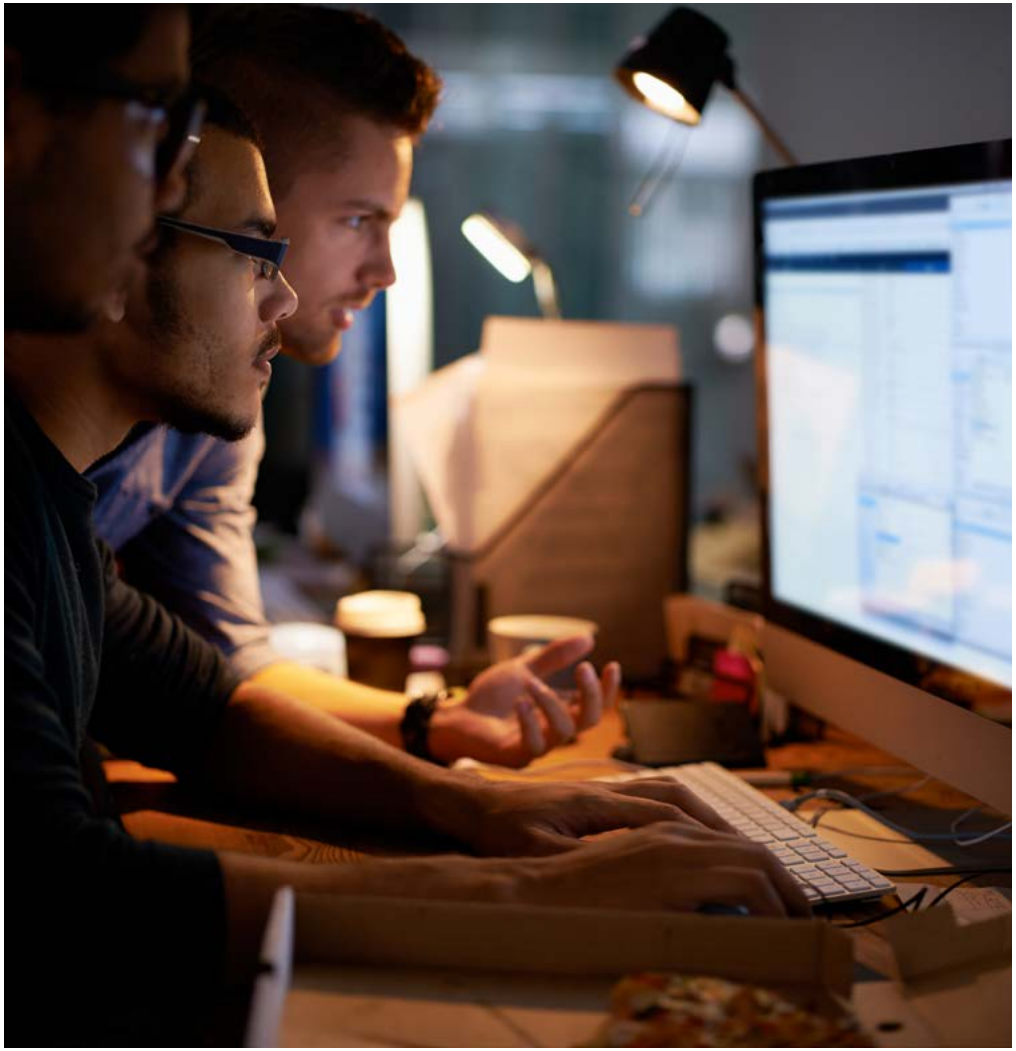
From inception to incident response, security needs to stay top-of-mind every step of the way through a product's lifecycle, say experts at Lenovo.

In today's world, data is everything. Organizations in both the public and private sector are more reliant than ever on the data they collect to drive decision-making, improve efficiency and supercharge operations.

"Data today is the new oil of yesterday," said Thorsten Stremlau, CTO and Principle Engineer, CISSP Commercial Portfolio, Intelligent Devices Group at Lenovo. "A company that loses its data loses its value."

The challenge, however, is that while protecting that data is more important than ever, it's also more demanding.

"This hybrid landscape is changing dramatically as hackers look to make more and more money and seek new opportunities for making money," said Stremlau. "So, rather than just going through the software channel as they've done in the past, they're looking through the hardware channel, through networking channels and through many, many other applications and even the social engineering channels to try to get at the data and at the value that's at the product. And that's why we really need to integrate security at every single level to, to block off any access that hackers might try to get at all levels."



THE WHAT AND THE HOW OF PRODUCT SECURITY

So, what does it take to truly integrate security at all levels of a product's lifecycle? It starts with a firm understanding of exactly what product security is, as well as what it means for customers.

"Product security means two things; I like to call them the "What" and the "How" — It's a two-pronged approach," explained Joe Pennisi, GM of PC and Smart Devices Global Security Lab, Lenovo. "The "What" is the solutions, the devices, the products, the things that we develop, the things we deliver with partners to solve customer problems around security. The "How" relates to how we build our products, ensuring that we utilize a secure development lifecycle for designing security in and validating that we're providing products without vulnerabilities."

This requires that security strategies and best practices like Zero Trust and Defense in Depth be incorporated through in every step of a product's process, particularly during its foundational stages. Pennisi points to the analogy of a house: Builders will start with the design element, drawing up blueprints that are reviewed and approved before work even begins on the structure.

"But even with every great design, not everybody knows how to build it correctly. So, you have inspectors that come along to ensure that what they've built meets the requirements. That's what we do as well with our security review boards: We inspect products before they're delivered to ensure that they've been built correctly and don't have these vulnerabilities," said Pennisi.

STRONG GOVERNANCE BREEDS GREAT SECURITY

In order to truly ensure that strong security practices remain in place throughout a product's lifecycle, however, requires strong security governance from inside the company itself. This is where Lenovo's Secure Development Lifecycle comes in to play, said Scott Kelso, principal researcher for Lenovo's Product Security Office.

"[The LSDL] is the set of requirements and process that we've put together to allow each business unit to understand where to begin in creating a product security process that's appropriate to their products and their customers. A key element of that is the SRB or security review board. This is a review board that sits really at all stages of the development cycle, but most prominently can review every product before it goes to market."

But governance extends even beyond the bounds of company walls. Lenovo also reviews each partner in its supply chain to ensure they're keeping up with security standards, as well as works with competitors to quickly and appropriately address emerging threats.

"Even if we did everything perfectly, we know that there still will be security incidents. That's the nature of this. One hallmark of a mature product security organization is its ability to respond to incidents," explained Kelso. "We participate in coordinated disclosure, and have relationships throughout the industry to make it work well."

According to Kelso, if Lenovo becomes aware of a vulnerability, it works to identify the source of the problem and works with everyone involved — be they suppliers, partners or even competitors — to get the issue fixed across the industry.

WHAT IT TAKES TO ACHIEVE COMPREHENSIVE SECURITY

Where do threats come from? When securing an organization's assets, this is often the question that informs policy, strategy and investments into cybersecurity software.

A better question, however, might be: Where don't threats come from? In fact, they come from almost everywhere. Malicious actors can penetrate networks through email, networks, connected devices and much more. Moreover, as technology expands, so do vulnerabilities. So, with data protection top-of-mind for organizations and security professionals, the question becomes: Where does security come from? At Lenovo, experts know that to fight comprehensive threats requires comprehensive security.

This is why the company has launched its ThinkShield brand — a promise that seeks to offer comprehensive, constantly evolving security solutions and tools to customers. Specifically, it addresses four areas of major security concern: Data, identity, online and device.

"ThinkShield's approach to security is to cover our customers on every level of their concerns. So whether it's the plastic shutter that we put in place the over the camera to help privacy to having a software solution that will detect whether somebody is looking over your shoulder and looking at your documents while you're in an open plan office," said Stremlau.

But he says the suite of solutions goes one step further in keeping customers secure, addressing more than just the threats we know about today.

"ThinkShield is also a promise to our customers to provide security over a period of time," he said. "We've dedicated our approach with every aspect of security to interlock with researchers, to interlock with our customers, to anticipate future needs and to anticipate future solutions to really make sure that we have our customers covered even in the future."

"We've dedicated our approach with every aspect of security to interlock with researchers, to interlock with our customers, to anticipate future needs and to anticipate future solutions, to really make sure that we have our customers covered even in the future."

— Thorsten Stremlau, CTO and Principle Engineer, CISSP Commercial Portfolio, Intelligent Devices Group, Lenovo