DELL Technologies

Device Security Practices at Dell

Three Considerations for Establishing Device Trust

Dell cyber experts explain the critical role device security practices play in the long-term resilience of your IT ecosystem.

Authors
Rick Martinez
Dell Fellow and Vice President

Eric Baize
VP, Product and Application Security

Introduction

In today's crowded cyber marketplace, you're likely inundated with options for security products and solutions. But what if I told you the most important part of your security strategy wasn't your security products?

As a major PC manufacturer, Dell thinks about security a lot. And what's become clear in recent years as we watch the devastating fallout of ransomware attacks and the expansion of firmware-based malware is that endpoint devices are a growing target. Unfortunately, single point solutions – no matter how innovative – can't keep users and data completely safe.

As you re-evaluate your existing ecosystem security and explore products for a refresh, **consider how your PC maker approaches security along with what to buy**. Why? You may think it's about product evaluation, but it's just as much about supplier evaluation. A trusted and experienced secure PC supplier who understands the threat landscape will be able to put that knowledge to use to help you protect your organization as that landscape evolves. With that partner, you'll construct a security ecosystem that intelligently mitigates the inevitable attack and drives long-term cyber resilience.

Security Begins Earlier Than You May Think

IT decision makers and end-users typically interact with some blend of sales personnel, the device(s) and product support. But that's just the tip of the iceberg when it comes to security. Why? It's similar to food safety. You can't judge food safety based only on your interactions with a waiter in a restaurant, because food safety starts in the kitchen. Similarly, what makes devices secure must be in place even before a product is produced – and is rarely visible as a result. Dell has devoted countless engineering hours and intellectual effort

to securing the customer IT work environment from the ground up – the intricate processes and protocols that govern the design, development and delivery of every device. The work that no one sees which forms the stable foundation under the surface to make the most secure device possible. The work that helps secure the customer IT work environment, whether you're a federal customer, enterprise or a small and medium business. Dell believes in enabling modern security for all businesses, big and small, and we are committed to delivering solutions that keep your organization – and by extension your customers – safe.

Our Device Security Practices

When we consider the protections for our commercial devices, we think about security outcomes – i.e., how the device contributes to the overall security health of an organization. How does the device help prevent attacks? What keeps it safe while under attack? And how does it remain safe throughout its lifetime?

As you might expect, we have dozens of practices in place for developing secure commercial PCs that align with industry standards and support a Zero Trust security approach. Today, I'll spotlight a few under three core themes: secure supply chain, secure code and security in-use.

1. We secure our device supply chain. That means strict controls around our supply chains for both hardware and software – a.k.a. the physical and the digital supply chains. These controls help maintain the integrity of our products as they flow through the manufacturing, assembly, delivery processes and on through deployment. This ensures that our customers get exactly what they purchased, nothing more and nothing less. Additionally, we convey these strict requirements to all of our suppliers. That said, in true Zero Trust "assume breach" fashion, we include verification checks during every step of this process.

These checks include advanced technologies like Secured Component Verification* to identify component swaps and SafeBIOS off-host verification to identify and alert on any tampering of the most privileged firmware in the system. These, and many other features, are built into Dell Trusted Devices – part of our Dell Trusted Workspace portfolio. But we also leverage them throughout our supply chain to keep all links in the chain intact. This allows us to spot deviations before they make it to the next step of the supply chain. *(*Optional add-on feature available for purchase. Availability varies by region.)*

That's what I mean by being outcome-focused. These features were developed, not for the sake of innovation, but because they actively solve real-life concerns that our customers have around supply chain security and fleet management. Never trust, always verify indeed.

Tying this back to supplier evaluation, remember, your OEM's supply chain is your supply chain – so be sure to vet the practices they have in place. (For more insight into what it takes to secure the supply chain, see our perspective in our supply chain white paper.)

2. We design and develop secure devices. Here's where you see the intersection of practices and features. This is how we develop effective – and innovative – hardware and firmware.

Now, security features are part of our market-facing offering – but that's just part of the puzzle. Our products would not be secure if their design, development and testing were not governed by our prescriptive Secure Development Lifecycle (SDL). A core responsibility of all technology providers is to ensure what they sell doesn't unintentionally present risk to users through vulnerabilities. To help prevent attacks and provide resiliency to our security software stack, we perform rigorous threat modeling during the software development process, identifying risks against very sophisticated adversary assumptions and even applying this methodology to critical hardware.

We test and verify these threat model assumptions throughout the development process, working with some of the best penetration testing consultants and third-party researchers, giving them Dell systems to try to break. Similarly, we offer a public bug bounty program to stress test the security of our commercial PCs. We take the output of those reports and feed that back into engineering to develop mitigations. Rinse and repeat. Why do we do this? Our customers' environments require hardened and trusted devices to operate effectively.

3. We work to ensure devices are secure in-use. Security takes a village. And today, true security includes protection at the hardware and firmware level, as well as software. That's why Dell makes an enormous effort to curate an ecosystem of fully vetted, best-of-breed partners that offer protection against advanced threats. Many are directly integrated into our commercial PCs. That said, hackers are constantly innovating new ways to break into software. For this reason, our SDL practices are designed to extend protection post-release, including the ability to quickly and easily identify and remediate vulnerabilities. Dell also proactively reports upcoming security updates and clear security support policies to make it easier for customers to understand how their products remain protected throughout their lifetime. To help customers quickly find information on vulnerabilities and applicability to product releases, we've consolidated all security advisories and notices in one place. Combining this with a well-documented vulnerability response policy allows us to work closely with researchers as new vulnerabilities are reported. This shortens the loop and ensures that accurate information is always available to allow customers to assess and remediate risk within their environments.

A Security Partner Putting it all Together

Dell strives to build trust and a secure, connected world. We work tirelessly to keep your and your customers' data, network, organization and safety top-of-mind – with security carefully engineered into all our solutions. To learn more about our security practices, please visit the Dell Security and Trust Center. And, as always, reach out your Dell representative with questions or connect with our security specialists at endpointsecurity@dell.com.

Learn more about
Dell Endpoint Security

Contact a Dell
Technologies Expert

View more resources

Join the conversation

DELL Technologies