DELL Technologies

Secured Component Verification

BUILT-WITH SECURITY FEATURE FOR DELL TRUSTED DEVICES,
THE INDUSTRY'S MOST SECURE COMMERCIAL PCs[1]

Secured Component Verification (SCV) is a supply chain assurance offering that enables customers to verify that the hardware components of the Dell system (PC) you have purchased and received match the components that were manufactured and/or assembled in the factory.

Verify Devices are Secure Through Setup

As more networks and devices become interdependent and connected, cyber complexities are causing more opportunity for disruption and opportunities for malicious actions. And these actions can occur at any step of the life of a product – even as it's being manufactured and shipped.

Supply chain security is crucial for any organization, as organizations are more dependent than ever before on others to provide components that are critical for their operations. Supply chain IT globalization is a reality for most products, and that means that the security of the technology supply chain is under constant scrutiny. While Dell has established comprehensive security procedures from the very beginning, and continues to make significant improvements, there are some customers with elevated component security requirements. Those customers need the ability to confidently deploy new devices knowing that critical components are matched exactly with the configuration that left the factory.

With Secured Component Verification, organizations gain an added level of security that they require. Verify that the hardware components of the system (PC) you receive match the components that were manufactured and/or assembled in the factory.

Platforms Supported

Latitude: 5320, 5420, 5421, 5430, 5520, 5521, 5530, 7320, 7330, 7420, 7430, 7520, 7530, 9420, 9430, 9520. 7320 (2-in1); 5430 (Rugged); 7330 (Extreme Rugged).
OptiPlex (Micro Form Factor): 5090, 7090.
Precision: 3560, 3561, 3570.

How it Works

Once a customer places an order for a PC with SCV, the product is built, PC component data is collected and encrypted, and this information generates a platform certificate that is created and signed at the factory. The digital certificate is stored on the local drive for delivery to the customers. One the customer receives; they can validate the components delivered to the certificate using a third-party verification tool. This process ensures that what the customer ordered is what they received and is free of tampering. *See Illustration on page 2.*

Key Features

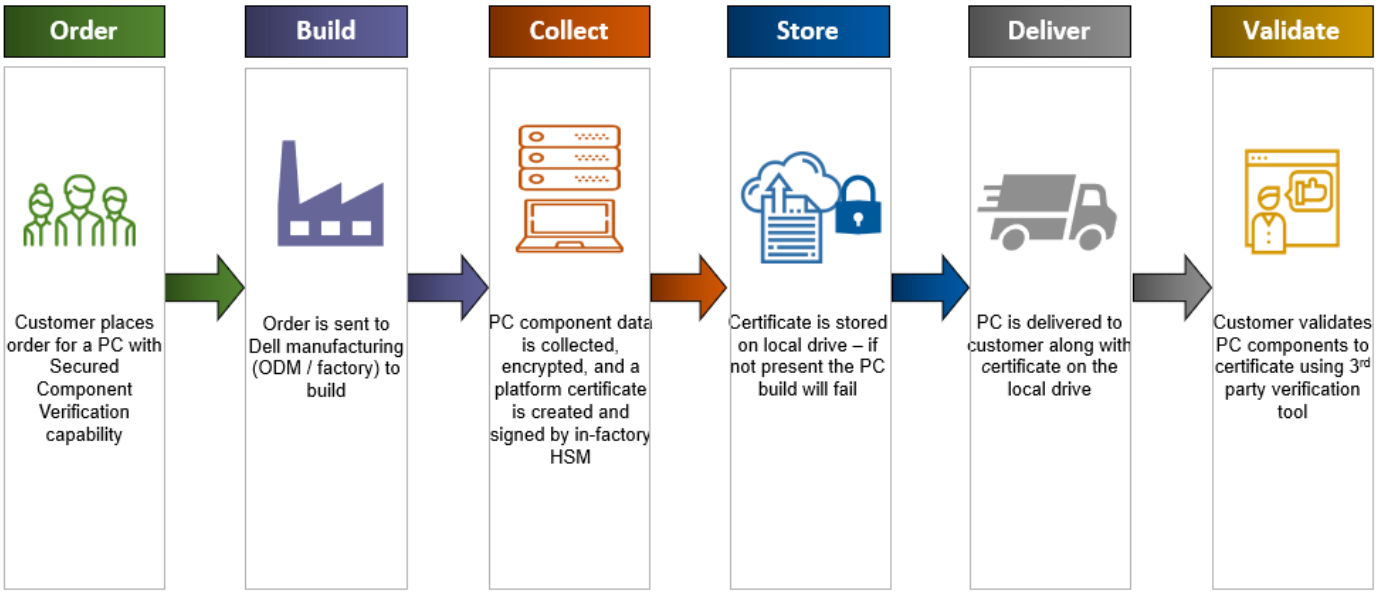
- Platform certificate created during build in Dell 2nd touch factory and stored on the PC.
- Deploy your Dell commercial devices with a component set that is delivered with an encrypted "as-built" certificate that you can validate.
- Platform certificate ensures that components such as the baseboard, processor, OEM, memory, hard drive, network card and TPM are delivered as ordered and per spec.
- Verify your as-built Dell hardware configurations for more secure deployments.

Benefits

- **Gain Assurance that your Hardware is Secure from the Start:** Dell Technologies Secured Component Verification ensures that Dell commercial devices are delivered and ready for deployment exactly as they were built by Dell manufacturing.
- **Enhance IT Security:** Align your comprehensive security standards with emerging industry guidelines to meet the most demanding requirements for secure IT infrastructure.
- **Improve IT Security Operations:** Adding SCV to your standard operating procedures for deployment is a low touch, low risk enhancement that ultimately secures your overall IT security operations.
- **Accelerate IT Innovation:** With added peace of mind that components and equipment are built and shipped as intended, IT teams can spend time focusing on other areas, such as business-related innovations.

[1] *Based on Dell Internal Analysis, September 2022.*

Illustration: SCV End-to-End Flow



Secured Component Verification is part of the larger Dell Trusted Workspace endpoint security portfolio. A supply chain security feature available exclusively via Dell commercial PCs, SCV is an example of the hardware/firmware-based protections Dell offers. Built-in/built-with security features, combined with built-on, software-based protections, provides customers a comprehensive defense framework for today's evolving threat landscape. Key offerings include:

- **SafeBIOS:** Gain visibility to hidden and lurking attacks with BIOS and Firmware tamper alert through Dell exclusive off-host BIOS and Firmware verification[1], BIOS Image Capture and BIOS Events and IoA.
- **SafeID:** Only Dell secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.
- **SafeScreen:** End users can work anywhere while keeping private information private with an integrated digital privacy screen.
- **SafeData:** Protect sensitive data on device to help meet compliance regulations, and secure information in the cloud giving end users the freedom to safely collaborate.
- **SafeGuard and Response** (powered by VMware Carbon Black and Secureworks): Prevent, detect, and respond to advanced malware and cyber-attacks to stay productive and free from the disruption and churn an attack can cause.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com to discuss how we can help improve your security posture.

[1]Based on Dell Internal Analysis, September 2022.

DELL Technologies