Secured Component Verification

With Secured Component Verification (SCV), organizations can confidently deploy new devices knowing that critical components are matched exactly with the configuration that left the factory.

Key Benefits

- Verify devices are secure through setup: SCV ensures that Dell commercial devices are delivered and ready for deployment exactly as they were built by Dell manufacturing.
- Enhance IT security: Align your security standards with Zero Trust principles and other emerging industry guidelines to meet the most demanding requirements for secure IT infrastructure.
- Improve IT security operations: Add SCV to your standard operating procedures for deployment for a low touch, low risk enhancement that ultimately secures your overall IT security operations.
- Accelerate IT innovation: With added peace of mind that devices are built and shipped as intended, IT teams can focus on other areas such as business-related innovations.
- Secured Component Verification provides digital proof and supply chain security by ensuring that the Dell system hardware components ordered match the components that were manufactured and assembled in the factory.

Supply chain security is a major concern with organizations demanding more vigilance and scrutiny over product security from the factory to their loading dock. Ensuring the safety of their devices and accompanying is 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 optimize them, some customers have elevated component security requirements. SCV provides these added security measures.

Key Features

- Platform certificate created during build and stored on the PC or in a secure cloud environment.
- 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.

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 either on the local drive or in a secure Dell cloud for delivery to the customers. Upon receipt, the customer can validate the components delivered to the certificate. This process ensures that what the customer ordered is what they received and is free of tampering. See Illustration on page 2.

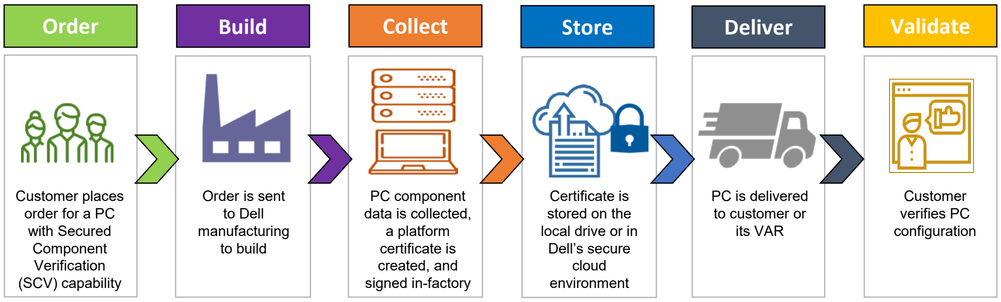
* Please note that the customer assumes chain of custody upon delivery, and that the device has undergone the intake process and completed certificate validation at Customer (or VAR’s) site within 30 days from the day of signature upon receipt of asset.

Learn more at www.Dell.com/endpoint-security

DELL Technologies

Options

SCV (on Device) On-Host Solution	SCV (on Cloud) Off-Host Solution
Certificate Storage: Generates and stores an inventory certificate on the Dell device that confirms authenticity.	**Certificate Storage:** Generates and stores an inventory certificate off-host in Dell's secure cloud environment that confirms authenticity.
Validation method: • Use tool from Dell drivers & downloads site to extract the certificate • Use a 3rd party tool (HERS tool) to do the validation using the certificate and endpoint.	**Validation method:** • Deploy Support Assist for Business & the Dell Trusted Device (DTD) Notification agent on the endpoint • View validation status via online portal (TechDirect) for retrieval verification status.
Product Availability: **Latitude:** 5320, 5420, 5421, 5430, 5520, 5521, 5530, 7320, 7330, 7420, 7430, 7520, 7530, 9420, 9430, 9520. 7320 (2-in-1); 5430 (Rugged); 7330 (Extreme Rugged). **OptiPlex (Micro Form Factor):** 5090, 7090. **Precision:** 3560, 3561, 3570	**Product Availability:** secured-component-verification-availability.pdf (delltechnologies.com)



Customer places order for a PC with Secured Component Verification (SCV) capability

Order is sent to Dell manufacturing to build

PC component data is collected, a platform certificate is created, and signed in-factory

Certificate is stored on the local drive or in Dell's secure cloud environment

PC is delivered to customer or its VAR

Customer verifies PC configuration

About Dell Endpoint Security

Secured Component Verification is part of the larger Dell Trusted Workspace endpoint security portfolio. Through Dell Trusted Workspaces, customers can access "built-in"/"built-with" security features, as well as "built-on" software-based protections, to help ensure a comprehensive defense framework for today's evolving threat landscape.

Built-in & Built-with Security

Hardware & firmware protections for Dell commercial PCs

- **Dell SafeBIOS:** Mitigate the risk of BIOS and firmware tampering though Dell's exclusive[1] off-host BIOS verification, BIOS Image Capture and BIOS Events and Indicators of Attack.
- **Dell SafeID[2]:** Only Dell[1] secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.
- **Dell SafeShutter:** Maintain onscreen digital privacy with integrated sensor-enabled webcam.
- **Dell SafeSupply Chain[3]:** Gain assurance that PCs are safe from the first boot with supply chain security solutions, such as Secured Component Verification, tamper-evident packaging and NIST-level hard drive wipes.

Built-on Security

Software protections for Dell and non-Dell devices alike

- **Dell 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.
- **Dell 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.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture.

[1] Based on Dell Internal Analysis, September 2022. *[2] Features vary by model.* *[3] Availability may vary by product, region and market.*

Learn more at www.Dell.com/endpoint-security