DELL Technologies

Data Sheet

Dell SafeID

Built-in, hardware-based, end-user credential security provides protection from malware that looks to steal them

Dell SafeID protects PCs against sophisticated threats

Keeping organizations' data safe, whether it be their intellectual property or customer's Personally Identifiable Information (PII), is foundational to data security. Hackers have become increasingly sophisticated, and as commonplace threats are being thwarted more frequently, cyber criminals are looking for more advanced ways to gain this critical information. With increasingly sophisticated endpoint security solutions like next-gen antivirus and managed endpoint detection and response, the attack vectors are narrowing and adversaries are forced to look for alternate invasion points.

Protecting user credentials is critical to securing an organization's PCs

Many of today's endpoint security solutions focus primarily on the operating system level. This can leave things such as user credentials vulnerable to malicious attacks. Once credentials are accessed, security is compromised on the end point as well as throughout the organization.

Dell SafeID is a response to this risk

Dell SafeID offers two options:

- Dell SafeID with ControlVault
- Dell SafeID with Discrete TPM

Dell SafeID with Dell ControlVault (CV3+) is a solution unique to Dell and provides an extra layer of security. It is also FIPS 140-3 level 3 certified. No other embedded PC biometric solution has achieved this level of external validation from NIST.[1] Dell SafeID with CV3+ helps secure end-user credentials by isolating them from the operating system environment and memory. Instead, all processing and storage of critical data takes place on a processing and memory chip. This unique, hardware-based security solution provides a hardened and secure bank for storing user credentials such as passwords, biometric templates and security codes within firmware and keeps them locked away from malicious attacks. ControlVault is available on select Dell commercial PCs.

Dell SafeID with Discrete TPM (dTPM) is standard on all Dell commercial PCs. In this solution, the dTPM uses cryptographic techniques to protect critical information on PCs, enabling platform authentication and enhancing overall security. Dell TPMs are now FIPS 140-3 Level 1 validated, ensuring they meet stringent security standards. The TPM helps in verifying the integrity of the platform, making sure that the system has not been tampered with. Together, Dell SafeID and dTPM provide robust protection for user credentials, making them less vulnerable to cyberattacks.

Dell SafeID hardens end-user credentials

- Stores and executes code using a secure processor
- Stores end-user credentials to allow a single point of migration
- Supports a broad set of crypto algorithms such as Suite B and active ECC

Built-in Security for Dell Trusted Devices, the world's most secure commercial AI PCs[1]

Secure & Isolate Encryption Keys and Templates

SafeID executes operations and stores credentials within its secure boundary which allows credentials to be kept secure and protected against any inspection or modification of the execution process. SafeID stores the execution code for secure processes within this secure boundary keeping malicious applications from accessing it.

Sealing Off Code Execution & Storage

Dell SafeID lets applications store keys and templates within a protected boundary that is strictly controlled. All usage of keys and templates are isolated from the host so they are never exposed to attacks.

About Dell Endpoint Security

SafeID is part of the larger Dell Trusted Workspace endpoint security portfolio. Through Dell Trusted Workspace, 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, CVE Detection and Remediation for BIOS and firmware, and BIOS Events and Indicators of Attack.
- **Dell SafeID:** Only Dell[1] secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.
- **Dell SafeSupply Chain:** 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:** Prevent, detect, and respond to advanced malware and cyberattacks 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.

[1] Based on Dell internal analysis, October 2024 (Intel) and March 2025 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by Principled Technologies. A comparison of security features, April 2024.

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation