Dell SafeID

Built-in Security on Trusted Devices

Dell SafeID with ControlVault protects PCs against sophisticated threats

Keeping organization's 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 users credentials is critical to securing an organizations 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

While other solutions are available such as the Trusted Platform Module, Dell SafeID with Dell ControlVault is a solution unique to Dell and provides an extra layer of security.

Dell SafeID helps protect secure operations by isolating them from the operating system environment and memory and instead, all processing and storage of critical data takes place on a processing and memory chip.

This provides a unique hardware-based security solution that provides a hardened and secure bank for storing user credentials such as passwords, biometric templates and security codes within firmware and locked away from malicious attacks.

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

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.

Learn more at Dellemc.com/endpointsecurity

Dell SafeID is part of the larger Dell Trusted Security portfolio including:

- **Trusted Devices:** The foundation to a modern workforce environment with invisible and seamless protection to ensure smarter, faster experiences. End users stay productive and IT stays confident with modern security solutions.
- SafeBIOS: Gain visibility to hidden and lurking attacks with BIOS tamper alert through Dell exclusive off-host BIOS verification.[1]
- SafeID: Only Dell secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.[1]
- 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
- **Trusted Data:** Dell constantly monitors and protects the endpoint ecosystem with Dell SafeGuard and Response, while giving IT confidence that data is secure even while end users collaborate freely with Dell SafeData.

ESTABLISH A MATURE SECURITY FRAMEWORK:

Proactively managing your organization's cybersecurity maturity is essential for defending against targeted cyber-attacks. Establishing a set of mature, robust security controls and understanding that prevention alone is not enough, can help you prepare proactively and enable your organization to successfully deal with the next security event.

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

1 - Claims based on internal analysis

Learn more at Dellemc.com/endpointsecurity