Hardware-enhanced protection for healthcare

The majority of data breaches start at the endpoint
Data breaches in healthcare are becoming routine, with 90% of all healthcare organizations reporting a breach in the past two years.¹ That’s not a surprise considering the rapid proliferation of connected devices being used by caregivers from mobile to bedside coupled with the fact that hospitals and healthcare facilities store and share large amounts of personally identifiable health and financial data, which are especially lucrative for hackers. These hackers are gaining access to this sensitive and valuable data through the endpoint. In fact, compromised user credentials are the leading cause of all data breaches.²

Traditional software-only security solutions aren’t enough
Passwords alone fall short in providing ample security. They can be difficult to remember, and even eight-character passwords changed every ninety days fail to protect against password cracking, phishing, screen scraping, and other attack methods.

Traditional two-factor authentication common in healthcare and software-only multifactor authentication (MFA) are a good start for hardening devices. But these methods remain vulnerable to certain types of threats, such as an exploit in the operating system (OS), because they store and process authentication data in the software layer.

Hardware-enhanced MFA with Intel® Authenticate
Increase your security posture with Intel® Authenticate, a full end-to-end secure, easy-to-deploy hardware-enhanced MFA system that complements existing software authentication. Intel® Authenticate uniquely captures and stores factors, credentials, policies, and authentication outside the OS in the hardware layer—defending your endpoints to protect the user’s identity while preventing access to confidential patient information. Newly added facial recognition offers an alternative to passwords, providing robust security without the hassle of forgotten passwords and password-related tech-support calls.

---

Simple, comprehensive data protection at the point of care

Working together, Dell and Intel® provide a hardware-based, IT policy-managed, multifactor authentication solution that mitigates security risks at the point of care.

Protected identity
Dell PCs provide a robust computing platform for use in the hospital or out in the field, while Intel® Authenticate provides the hardened MFA to secure user identities on select 6th, 7th, and 8th generation Intel® vPro™ systems.

Protected data
Dell Data Protection | Encryption protects patient data from multiple angles with management tools, hardware crypto accelerators, and self-encrypting drives (SED). Using different encryption keys for different users and different types of data from clinical to claims makes for simple granular, policy-based data protection without compromising user productivity.

Dell’s layered encryption operates transparently to the user while giving IT administrators the management tools they need for helping to comply with HIPAA and GDPR regulations and maintaining the proper controls across the healthcare system.

Protected access
With Intel® Authenticate, you can create customizable multifactor security policies based upon clinical workflow using existing tools, giving you additional flexibility while reducing your exposure to malicious attacks. Intel® Authenticate can be integrated with identity access management (IAM) software to combine the separate disciplines of access management and authentication with identity governance and user life-cycle management into one comprehensive suite to provide robust MFA without impeding caregiver workflow. Intel’s new facial-recognition feature, for example, offers caregivers the option to keep their gloves on as they work—enabling them to focus on the patient while Dell and Intel make it difficult for attackers to access or tamper with patient data. Touch-free access combined with hardware-enhanced security features create simple user experiences with a high level of security on which IT administrators can rely.

HARDWARE-ENHANCED MFA REDUCES SOFTWARE-LAYER VULNERABILITIES

Software-only MFA
Stores credentials in software and is more vulnerable to potential threats

Hardware-enhanced MFA
- Hardened authentication reduces risks of software-based attacks
- Encrypted credentials offer more resilience against theft
- Management policy protected within devices
- Self-service factor enrollment and verification

Intel® technologies’ features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://www.intel.com.

© 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. Reference Number: H17060