PROTECTING CREDENTIALS WITH THE STRENGTH OF SILICON

Staying ahead of industrialized hacking operations means you need an approach to identity and access management that goes deeper than software.

$17.36 MILLION: AVERAGE COST PER BREACH IN 2016[3]

It's never been easier to become a malicious hacker. If you've got the Bitcoin,* you can buy stolen passwords in bulk. DIY ransomware kits are also for sale on the dark web—little or no tech experience required. No wonder security experts predict ransomware will earn hackers more than $1 billion in 2017, compared to only $24 million in 2015.[1]

Combine the commoditization of hacking techniques with the proliferation of vulnerable devices in the enterprise and you can see why authentication should no longer rely solely on software. Security must also be grounded in silicon.

The need for hardware-enhanced security becomes even more clear when you consider the primary cause of data breaches. According to new research from Verizon,* stolen or weak passwords were used in 81 percent of hacking-related breaches in 2016.[2] The costs are considerable. A study of 237 U.S. companies in 2016 by the Ponemon Institute found the average cost of cybercrime was $17.36 million per breach.[3] It's harder to measure the costs in tarnished brand reputation and diminished customer confidence, but the losses are no less real.

To reduce risk, organizations need to embrace multifactor authentication.

Multifactor authentication, defined.

Multifactor authentication is a combination of something you know, something you are, and something you have. Something you know can be a password or PIN; something you are can be a biometric factor, such as a fingerprint or facial characteristic; and something you have can be the location of your PC or Bluetooth* phone proximity.

New 7th Gen Intel® Core™ vPro™ processor-based devices provide a portfolio of hardware-enhanced security solutions that help protect against modern cyber threats. The key solution is Intel® Authenticate Technology, which is designed to verify no less than two authentication factors, grounding the processing of credential keys and IT policies in the latest chipsets, where they are harder for thieves to access.

It doesn't make things harder for employees. As a hardware-based multifactor solution, Intel® Authenticate Technology helps increase productivity. Intel® Authenticate Technology also adjusts to individual company policies and preferences, providing smooth integration with SCCM (System Center Configuration Manager), GPO (Active Directory Group Policy Objects), and McAfee* Policy Orchestrator.

Malware continues to evolve, but so does the technology crafted to counter it. As software security partners such as Microsoft*, Citrix*, Cisco*, Intercede*, and RSA* build new capabilities on top of the Intel® Core™ vPro™ platform, Intel® Authenticate is expanding its range of identification factors to continue supporting new security innovation.

The fight against malware will be ongoing. Halting the adversary at the endpoint is essential.

[1] http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[3] http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

0710/CC/DOR/PDF