(intel®)

Identity threats have met their match with the Intel® Authenticate Solution.

Tighten identity protection with the Intel® Authenticate Solution on new Intel® Core™ vPro™ processor-based computers.

The need for identity protection has never been stronger. Identity theft accounted for 74 percent of all data breaches in the first half of 2017[1], and costs associated with cybercrime are expected to reach $6 trillion annually by 2021[2].

Any time an employee's username and password are compromised, your business is vulnerable. Eight-character passwords that changed every 90 days worked well a decade ago, but increasingly commonplace attack methods—like password cracking, phishing, or screen scraping—call for a new kind of protection.

Strengthen software security with an Intel® hardware-enhanced solution.

Accessibility to data is becoming even more important than where it's stored. When you look closely at breaches, a pattern emerges: Credentials are the main route hackers take to sneak into a network, steal data, and extort brands. The countless threat categories facing business today only continue to morph; no matter how many ways you try to apply scattered point solutions, identities are the crux of everything.

Log in with a look.

Facial recognition will change the game for identity management in 2018. For users, logging in will be easier than ever—just look at the device, give a smile if you want, and you're in. No more remembering and changing passwords, no more calls to IT for forgotten credentials. And IT will appreciate a higher level of security coupled with fewer service tickets from angry locked out users. But like all forms of authentication, facial recognition can be vulnerable when relying on software alone. That's why devices powered by the latest Intel Core vPro processors ground identity management in hardware with the Intel Authenticate Solution. Empowered by the strength of silicon, the Intel Authenticate Solution delivers more robust protections for facial recognition, ensuring easy logins for users and hardened security for IT.

Intel Authenticate Solution Benefits

"Hardened"
Factor Enrollment and Verification

"Hardened"
Authentication Decision

"Hardened"
Credential Storage and Token Release

Unified Management

"Hardened"
Policy Management

Considering that even multifactor authentication solutions have been duped at the software level, the need for hardened multifactor authentication becomes abundantly clear. In addition to premium performance, the latest-generation Intel Core vPro processor-based devices provide a growing portfolio of built-in security solutions to protect against the top threat vectors. And our comprehensive approach to hardware-enhanced security starts with the Intel Authenticate Solution.

The latest version of the Intel Authenticate Solution supports an even wider range of login factors so people can become their own password, including fingerprint and the latest addition of facial recognition. It also gives IT the confidence of hardening factors and IT policies at the silicon level. When credential keys, tokens, and policies are processed in the chip, they're much harder to see or reach.

Multifactor identity protection was yesterday; hardened multifactor identity protection with the Intel Authenticate Solution can mitigate modern risks that already know their way around software.

To be truly effective, MFA must be grounded in hardware.

Multifactor identity protection is becoming the new industry standard, but not all solutions are created equal. Unlike other MFA approaches, the Intel Authenticate Solution hardens factors, credentials, and IT policies in silicon, protecting all aspects of identity below the operating system. IT can customize factors in several ways, including:

- **Something you know** (such as a PIN)
- **Something you have** (such as a phone)
- **Something you are** (such as a fingerprint or facial recognition)
- **Someplace you are** (location-based identification)

Easily deploy an end-to-end identity protection solution.

IT can deploy the Intel Authenticate Solution with the familiar tools and infrastructure already in place. It works with Windows* 7 and Windows 10, and integrates with several common IT management consoles, including:

- **Microsoft System Center Configuration Manager* (SCCM)**
- **Active Directory Group Policy Objects (GPO)**
- **McAfee ePolicy Orchestrator* (McAfee ePO*)**

IT can use the above tools to configure and deploy the Intel Authenticate Solution and enforced policies to client PCs and then set up any combination of factors with flexible policy configuration and enforcement capabilities. End users are then prompted by the Intel Authenticate Solution application to enroll all their required authentication factors, enabling them to start quickly without calls to IT.

IT gets security. Users get productivity. Win-win.

Stronger security once came at the price of user productivity. The more layers of protection IT added, the more burdensome work became for users, forcing them to remember complex, ever-changing passwords and utilize cumbersome identity management software that practically required IT certification to operate.

With the Intel Authenticate Solution, that concern is history. It's designed to maximize identity protection and employee ease of use by taking advantage of new authentication factors that turn a person into a password.

And the Intel Authenticate Solution takes security and simplicity even further by grounding multifactor authentication into the hardware of the device. This locks credentials into a vault of protected silicon while also providing consistent, built-in, and intuitive authentication procedures for users. So employees can securely log in and get working faster, more reliably, and from just about anywhere.

Protect users and credentials from end to end.

A lot can happen between the time users input their login info and the system grants access. Hackers love to pounce on critical matching and enrollment processes, intercepting login data in transit. Software can help, but it often hampers ease of use. Bugs, glitches, and interoperability issues in software not only expose vulnerable data, but can also lock users out of the network, preventing them from working remotely, seizing key opportunities, or even just checking their email.

The Intel Authenticate Solution solves this issue by protecting login data from end to end and inside the hardware of the device. Throughout capturing, modifying, updating, or revoking, every step in the Intel Authenticate Solution process is hardened from server to client. So credentials stay hidden while users stay productive, wherever and however they like to work.

Give the right teams the right tools.

Security needs vary wildly from team to team within the enterprise. Sales and accounting departments may have access to sensitive financial data for the business and its customers. Marketing may need to protect information on unreleased products and services not ready for the public eye. And human resources holds the key to company secrets that could create PR firestorms if exposed.

With software-only security, it can be difficult or even impossible to effectively customize security protocols at the team or employee level. This can create data vulnerabilities that lead to financial and customer losses while also preventing users from easily accessing the tools and information they need to do their jobs effectively.

The Intel Authenticate Solution provides flexible security grounded in hardware, so you can give users the unique capabilities they need without compromising protection.

Depending on the different levels of security you want to apply to certain teams and employees, the Intel Authenticate Solution lets you easily customize which factors and how many are used. You can mix and match any number of factors, not just two, unlike other MFA solutions. And you can even update an entire policy without reissuing individual certificates.

Comply with new standards without curbing productivity.

Security regulations like GDPR are forcing enterprises to adopt stricter protection protocols to ensure compliance. With software-only security, this can result in a host of updates and patches that grind both user and IT productivity to a halt.

New hardware-based security tools like the Intel Authenticate Solution can better protect files at the point of identity and access to help you get in front of the latest regulations. So users and IT can keep work moving even as standards intensify.

Where to get more information.

Get the breakthrough identity protection of the Intel Authenticate Solution and safeguard your workforce credentials. Learn more at: **www.intel.com/authenticate**

[1] https://www.statista.com/statistics/215794/identity-theft-data-breaches-worldwide/
[2] https://www.csoonline.com/article/3210912/security/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html