SOLUTION BRIEF

Intel® Authenticate Solution

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

Hardware-enhanced, multifactor authentication security[1] delivers breakthrough identity access protection.

Any time an employee's user name and password are compromised, your business is vulnerable. Eight-character passwords that change every 90 days worked well a decade ago, but increasingly commonplace attack methods, like password cracking, phishing, or screen scraping, accentuate the need for stronger identity protection. 63% of data breaches are caused by stolen or misused credentials.[2] Costs associated with these breaches are growing, with the average cost of a data breach estimated at a staggering $4M.[3]

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

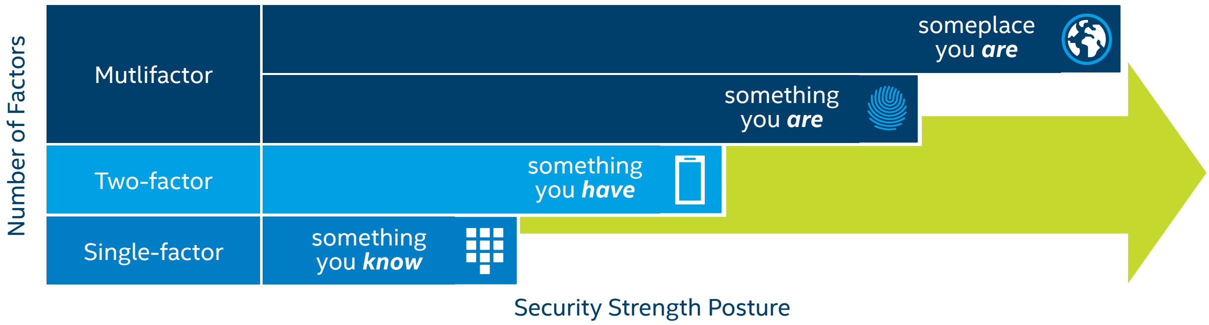
To thwart these identity-based security attacks, multifactor authentication is becoming a new industry standard. But not all solutions are created equal. Intel is reducing the vulnerabilities of software-only solutions with Intel Authenticate Solution,[1] hardware-enhanced, multifactor authentication. It protects the endpoint by hardening security outside of the operating system to reduce the risk of data breaches. Authentication factors, IT security policies, and authentication decisions are all encrypted in the hardware. User credentials managed by Intel Authenticate Solution are protected in hardware to prevent exposure to software attacks.

Mitigate risk with customized, multifactor protection.

Intel Authenticate Solution verifies a user's identity for domain and network access login by using any combination of multiple hardened factors at the same time, in an IT customizable manner, including:

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

What is multifactor authentication (MFA)?



Each additional authentication factor improves security assurance by an order of magnitude. IT can easily customize a combination of factors to meet their security criteria. On 6th and 7th Generation Intel® Core™ vPro™ processor-based PCs,[1] the hardware-enhanced factors supported include fingerprint sensors, *Bluetooth*® technology/BLE proximity with a smartphone, a protected PIN on the computer display, and Intel® Active Management Technology[1] to identity the user's network location. Furthermore, new 7th Generation Intel Core vPro processor-based devices[1] are poised to support more features, including smart virtual card, and offer additional customization options based on OEM, IHV, and ISV innovation.

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

IT can deploy Intel Authenticate Solution with the familiar tools and infrastructure already in place. It works with Windows* 7, Windows* 8.1, 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 these tools to configure and deploy Intel Authenticate Solution and enforced policies to the client PCs and then set up any combination of factors with Intel Authenticate Solution's flexible IT policy configuration and enforcement capabilities. Then end users are prompted by the Intel Authenticate Solution application to enroll all their required authentication factors, enabling them to start quickly without calls to IT.

Where to get more information.

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

Taking multifactor authentication further.

Intel Authenticate Solution's multifactor authentication is a new solution that supports hardened factors and how they are implemented, managed, and enforced. The technology is built into the platform in 6th Generation and 7th Generation Intel Core vPro processor-based systems.[1] It reduces the vulnerabilities of software-only solutions by hardening platform security outside of the operating system so that your organization has a stronger security posture. This includes not only protecting user credentials, but also securing the authentication data so it is less prone to theft, misuse, or impersonation by an outsider. All factors, policies, and decisions are captured, encrypted, stored, and matched in the hardware layer of the platform.

[1] 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 intel.com.

[2] The 2016 Data Breach Investigations Report (DBIR) by Verizon http://www.verizonenterprise.com/DBIR/2016/

[3] Ponemon Institute, June 2016.

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's terms and conditions of sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Unless otherwise agreed in writing by Intel, the Intel products are not designed nor intended for any application in which the failure of the Intel product could create a situation where personal injury or death may occur.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

1216/BC/DOR/PDF