Innovation Brief

Security in the digital workplace

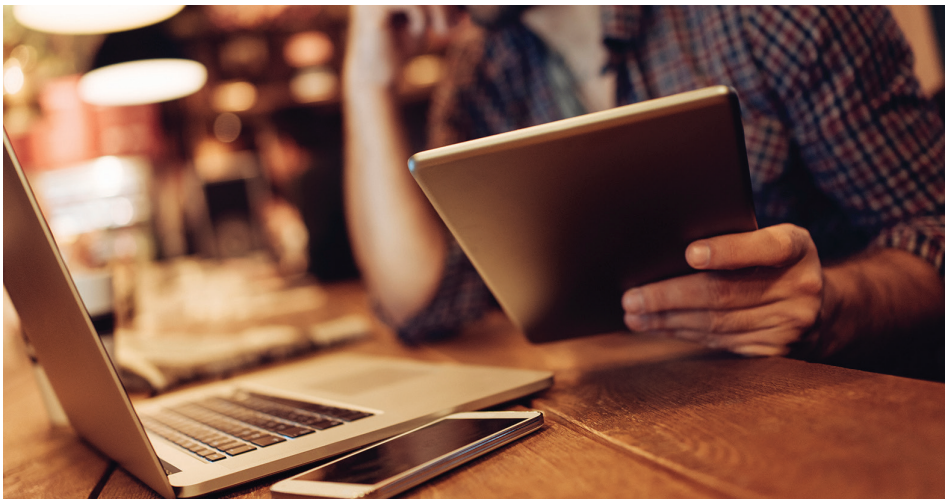
World-class Innovation and Consulting from Intel® Authenticate and Atos

The Intel® and Atos collaboration combines hardware-enhanced multifactor user authentication with expert security consulting for a powerful digital workplace security solution that increases efficiency and lowers cost.

With Intel® Authenticate, multifactor authentication is secured in the hardware layer (below the operating system) to strengthen identity protection for user authentication into enterprise domains and VPN infrastructures. This innovative solution for managed IT environments helps protect workforce credentials directly on the endpoint PC.

Intel® Authenticate:

- **Strengthens identity protection through hardware-enhanced multifactor authentication into Windows domains and VPNs**
- **Enables administrators to create tailored combinations of hardened factors:**
  - **— Something you know (such as a PIN)**
  - **— Something you have (such as a smartphone)**
  - **— Something you are (defined by a fingerprint)**



Business Challenge: Identity Protection in the Digital Workplace

A digital workplace is more innovative and productive. Enhanced collaboration and flexibility enable the workforce to identify and capture new opportunities and find better ways to solve current problems. For the enterprise to take full advantage of its resident talent, it must ensure that they have access to the right data. And it must also minimize the risk of extremely expensive and damaging breaches[1], which often begin at the credential level. In fact, weak passwords and stolen or misused credentials are responsible for 81% of data breaches[1]. Breaches caused $1.6B in damages to business and reputations in 2016 alone[2]. From 2015 to 2016, there was an 86% increase in records compromised by data breaches[3], and from 2015 to 2020, cybercrime damages are predicted to rise from $3T to $6T[4].

Providing a trusted environment begins at the human level: protecting the identities of the workforce. Simple username and password combinations have given way to multifactor authentication solutions, which provide an unmatched degree of protection. However, multifactor authentication that operates at the software level is not sufficient protection.

Further, while most enterprises are staffed with talented IT experts who can address security, not all are expert in the realm of security solution design, implementation and rollout. This can lead to decreased workforce efficiency, increased support costs, and a risky, permeable security environment.

About the authors:
John J Minnick, Sr. Director, Global Strategic Technology Partner Team, Atos Inc.
Rhett Livengood, Director, Digital Business Enabling, Intel

Intel® Authenticate: Identity Protection at the Hardware Layer

Multifactor authentication at the software layer leaves identities vulnerable to software exploits. Intel is reducing the vulnerabilities of software-only solutions with Intel® Authenticate, a hardware-enhanced multifactor authentication solution. Intel Authenticate further protects the PC 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.

Intel Authenticate 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. Each additional authentication factor can help improve security assurance.

On PCs with 6th and 7th generation Intel® Core™ vPro™ processors, supported hardware-enhanced factors include fingerprint sensors, Bluetooth/BLE proximity with a smartphone, a protected PIN on the PC display and Intel® Active Management Technology (Intel® AMT), which identifies the user's network location. New PCs that use 7th generation Intel Core vPro processors are poised to support more features, such as facial recognition, and offer additional customization options based on innovation from original equipment manufacturers (OEMs), independent hardware vendors (IHVs) and independent software vendors (ISVs).

Intel and Atos: Better Together

Hardware alone, however, cannot itself provide a digital workplace security solution. In collaboration with Intel, Atos applies its expertise to creating such solutions by providing clients with cybersecurity advice, and design, build and operate services.

Together, Intel and Atos provide a hardened digital workplace security solution that is much stronger than the sum of its parts. Through a collaborative and close relationship, Intel and Atos work together to provide technologies and services that make the secure digital enterprise a reality.

For more information about the Atos and Intel collaboration, visit: **atos.net/workplace**

"The Intel® Authenticate Solution leverages an enterprise's existing infrastructure and management tools combined with the unique ability to protect identities at the hardware layer versus software where the majority of breaches occur today. We expect enterprises to greatly benefit from this cost effective and smart approach to solve for the increasing security threats."

- John J. Minnick , Senior Director, Global Strategic Technology Partner Team, Atos, Inc.

Atos: Olympic-Level Security Experience

For more than 50 years, Atos has delivered proven and trusted security solutions to organizations such as defense and security agencies. It helped ensure the safe operations of the Olympic and Paralympic games in Rio de Janeiro in 2016.

The number of IT security events detected at the Rio 2016 Olympic Games were a staggering 510 million, which means 400 per second – double the equivalent figure from the London 2012 Olympic Games.[5]

Atos provided water-tight IT security in environments under immovable deadlines with zero tolerance for failure by expecting the unexpected and leaving nothing to chance. Prior to the event, Atos undertook 200,000 hours of testing and full 'dress rehearsals', running literally thousands of different scenarios. During the event, the Atos team worked 24/7, scrutinizing everything flowing through the network and cutting through "digital noise" to identify genuinely suspicious behavior. This involved a combination of using the very latest complex-data analytics to look for patterns, flagging the items that required a "human call," and then feeding all of it back into the mix, in real-time. The Atos team, in conjunction with partners, worked tirelessly to ensure that this information was delivered successfully, allowing the world to share in real time in the most connected way yet.

About Atos

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of circa €12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, and Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public Sector, Retail, Telecommunications and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market.[5] Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

About Intel

Intel (INTC) expands the boundaries of technology to make the most amazing experiences possible. Information about Intel and the work of its more than 100,000 employees can be found at newsroom.intel.com and intel.com.

Atos Innovation Radar: Mapping the Future

Regularly updated for our clients, the Innovation Radar diagram provides a pictorial view of our technology and market findings, allowing you to quickly understand how disruptive each trend is likely to be and the actions you might consider taking.[6] Each technology trend is analyzed from three perspectives: potential size of impact on your business, likely time to impact your business and the technology maturity.

[1] Verizon 2017 Data Breach Investigations Report.
[2] Cost of Breach Study: Global Analysis, Ponemon Institute, 2016.
[3] Gemalto 2016 Breach Index Report
[4] Cybersecurity Ventures, 2016
[5] To learn more about Atos's contributions to the Olympic Games, visit: atos.net/en-us/home/olympic-games.html
[6] "Look Out Trends 2016. More on ascent.atos.net

atos.net