MULTIFACTOR AUTHENTICATION AND BIOMETRICS IN THE MODERN WORKPLACE

Empowering endpoint security in the enterprise

Dimitrios Pavlakis: Analyst
Michela Menting: Research Director

FEBRUARY 24, 2016

1. EXECUTIVE SUMMARY

This whitepaper looks at the limitations of current endpoint security mechanisms within the context of employee authentication to corporate computers. Continued endpoint infections, large-scale data breaches, and widespread system vulnerabilities require new efforts in terms of modernizing authentication within the enterprise. Budgetary constraints, the focus on network security, and the reliance on single-factor authentication methods are barriers that need to be addressed by enterprises in order to stay secure and competitive in an increasingly threatening cyber landscape.

The whitepaper seeks to provide clear and comprehensive guidance for decision makers and C-level executives aiming to implement modern multifactor biometrics-based authentication solutions. Intel's new Authenticate offering provides an answer to the rising cybersecurity challenges in the modern enterprise landscape with a powerful processor-based multifactor authentication and biometrics solution.

2. EVOLVING AUTHENTICATION IN THE MODERN ENTERPRISE

One of the most serious security threats to any computing device is impersonation of an authorized user allowing access to restricted systems.

The rapid propagation of personal computing devices along with implications of heightened security risks and cloud-based service adoption has caused a paradigm shift in how organizations are authenticating users. One of the most serious security threats to any computing device is impersonation of an authorized user allowing access to restricted systems. IT departments are faced with increasing challenges to provide the end user with the freedom to use any device and transparent access to corporate resources while enforcing stringent security policies to protect confidential information and corporate intellectual property. As a result, user identification and authentication forms a central component of any security infrastructure and should play a vital role in ensuring user identity and assurance before user access to resources is granted to an individual.

2.1. Passwords: The Traditional Core of Authentication

Oftentimes, the same password is used in several different situations—for logging on to Windows, running the payroll system, accessing an authenticated website, *etc*. This makes the threat actor's task considerably easier; once a password for a specific user is obtained, access to multiple other accounts under the same user can be more easily gained. Additionally, individuals tend to use easy-to-guess passwords, including technical experts and senior individuals. The use of trivial passwords to secure highly privileged accounts for backup programs, network control software, and anti-virus tools is common enough, and consequently, taking control of an entire network frequently takes no more than a few minutes during a penetration test.

Most of the debate over the continued value of passwords is hyper-focused on individual usage, which is just one part of a larger problem. Issues about passwords suggest that the problem organizations need to solve is one of authentication. Recent password breaches depict a failure of organizations to properly implement and operate modern authentication systems. There are three critical questions that organizations need to consider when implementing an effective authentication solution:

1) **What are the long-term pitfalls of the chosen solution?**
2) **Are there any interoperability / accuracy issues that will increase TCO over time?**
3) **Is security being addressed in a precise and streamlined manner**?

2.2. Security Shift: From Network to Endpoint

One of the issues with endpoint authentication is that, traditionally, enterprise security has placed a larger focus on the network than on the endpoint. The network security market is larger than the endpoint security market, but in the coming years, this will change. Both network and endpoint security mechanisms are essential components for building a layered cybersecurity framework. However, as more devices move outside of the enterprise walls, endpoint security is poised to eclipse network security as a sales driver for solution providers, creating new revenue opportunities.

Laptops, smartphones, and tablets are being used outside of the enterprise and off the corporate network, where they can't be protected by traditional firewalls and other network security solutions. This is a growing issue as endpoints continue to represent a significant threat vector for cyberattacks, either through unprotected connections to the network or through social engineering. Phishing attacks in particular are increasingly targeting smartphone users who are prompted to input their credentials (including biometric information) to websites that appear legitimate but actually siphon out user IDs and personal details.

As a result, encryption, authentication, anti-malware, and a host of other security options are moving to the endpoint, including smartphones, and a new era is emerging where network security is expanding beyond traditionally defined concepts. By recognizing endpoints as the new network perimeter, organizations can mitigate the vulnerabilities of new endpoint vectors, especially in personally liable devices, and limit outside infections and breaches into the corporate network. Endpoint security is also becoming critically important in the broadening areas of machine-to-machine (M2M) communications and the Internet of Things (IoT).

2.3. Making MFA the new standard

One of the toughest challenges in information security is ensuring that a user accessing sensitive, confidential, or classified information is authorized to do so. Such access is usually accomplished by a person proving their identity by the use of some method of authentication. It is most critical that the user be able to validate who they say they are before accessing information, and if the user is unable to do so, access will be denied. Most authentication systems are based on one or more of the following: a) proof by knowledge, b) proof by ownership, c) proof by property.

By applying two or more authentication procedures in combination, stronger authentication can be achieved. The use of multiple authentication factors considerably increases the security of a system. If such a risk exists that a single-factor authentication system will be compromised, then when a second factor of authentication is taken into consideration, this risk is significantly mitigated. Multifactor authentication (MFA) is the solution to the security issues brought about by the extension of the corporate perimeter and new technologies and work ethics including cloud and BYOD, expanding beyond the pitfalls of passwords to ensure that corporate access and information remains restricted to those authorized employees.

3. APPLYING MFA IN THE WORKPLACE

3.1. Endpoint Authentication Issues

Increasing complications, breaches, and ID theft involving endpoint authentication result from three major issues. First, the frequent use of ever-changing and restrictive passwords coupled with the growing number of personal and company accounts is a significant stumbling block for the creation of complex and un-guessable passwords. In the majority of the cases, employee passwords have a large number of similarities with the previous ones. Often, employees will change a few letters, replace them with numbers, or capitalize a different sequence. This also conflicts with the password creating process that employees have for their personal accounts. Within only one year of password changes and account creation or replacement, it is estimated that around 70% to 75% of the passwords will bear a resemblance with previous “password iterations.” If an attacker manages to obtain a couple of passwords from a user, they can quite easily launch a dictionary attack against their accounts by merely replacing a few characters. It is worthwhile mentioning that some of the most used passwords over the last 5 years are worryingly basic: “password”, “admin”, “qwerty”, “12345”, and “12345678”.

Second, another major problem with endpoint authentication is the focus on software-based protection. While this seems to be the standard as the most cost-effective solution in the workplace, it simply authenticates the password rather than identifying the user. Therefore, any user (legitimate or intruder) with the correct password is recognized as an authenticated user. Software-based password protection has no means of knowing whether the user is who they claim they are.

Thirdly, in today’s multifaceted cybersecurity landscape, having only one single authentication factor and one that can be easily shared, broken, or guessed, is a significant vulnerability. MFA is

not something that should be considered a technological indulgence or a "security extra," but rather a fundamental aspect of modern employee identification schemes.

3.2. The Weakest Link

Hackers will choose the weakest target and start with the weakest link in that target

Given enough time and resources, every system can be hacked. However, there is one crucial underlying concept that remains largely true: *hackers will chose the weakest target and start with the weakest link in that target*. Staying ahead of attackers is an arduous exercise and there is a fundamental split in enterprises that are actively dealing with the issue and those that are not: the "innovative implementers" as opposed to the more "traditional implementers."

The majority of enterprises (traditional implementers) host the minimum requirements for endpoint protection:

- Software-based encryption, firewall, URL filtering
- Laptop and desktop antivirus protection
- Email protection
- Logical access control: password-protected employee assets
- Potentially coupled with a second-factor authentication: an additional OTP, external USB device, token, *etc*.

Traditional implementers give much more emphasis on network security but are lacking in endpoint protection in itself. Threat actors are generally always one step ahead of enterprises in terms of exploiting vulnerabilities, especially at the software level. Implementing security solutions rooted in hardware, and secured again at the software level, significantly diminishes potential attack surfaces. Companies that employ such measures at both the network and the endpoint level are innovative implementers and make use of techniques including:

- MFA that is designed specifically to accommodate data in a secure location in the processor unit from three different and quite distinct sources: logical tokens (*e.g.*, user IDs, PINs, passwords); device-generated credentials like, *e.g.*, hardware tokens; Bluetooth pairing with smartphone devices; smartcard-based credentials; non-GPS location-based services (LBS) credentials (also available since Intel's fourth-generation VPro processor); biometric credentials using RSA or DES biocryptography variants and non-USB device-embedded fingerprint sensors (*e.g.*, Synaptics); and cameras (*e.g.*, Intel RealSense).
- Powerful processors and chipsets with embedded security such as trusted platform modules with UEFI, trusted execution environments, and other related security protocols in place designed to provide root-of-trust (RoT) in smaller endpoints and not only in servers and PCs.
- A sophisticated and multi-layered policy strategy specifically designed to address identity policy issues.

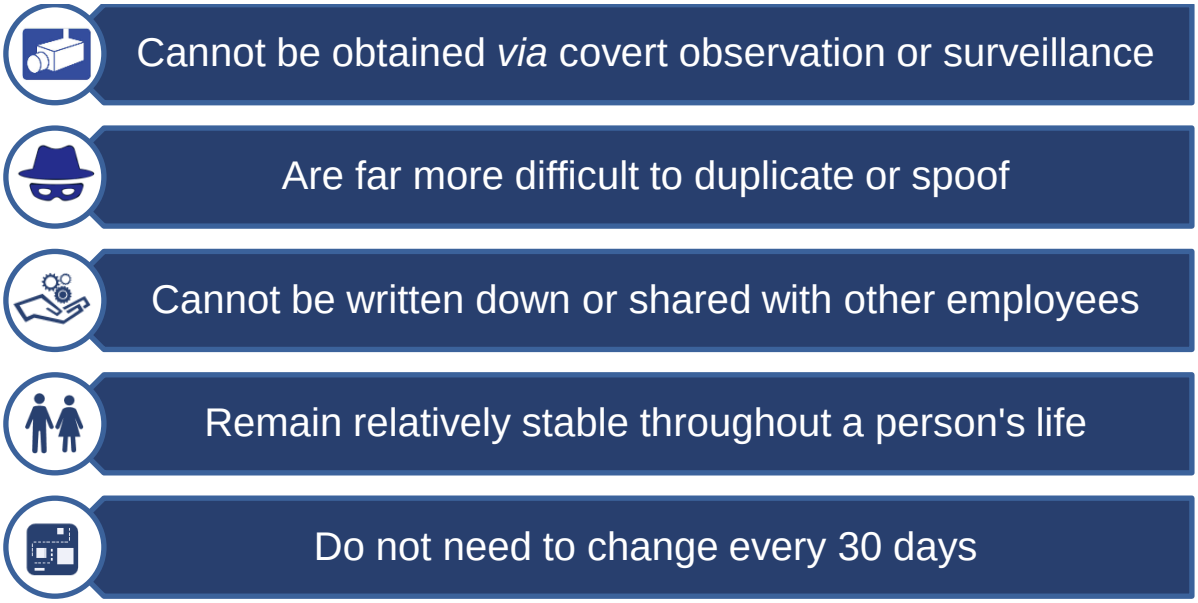
On the one hand, software-based security is more flexible than its hardware counterpart. A software firewall, for example, can be installed on an employee's desktop computer, laptop, and corporate server. The costs are significantly reduced and the functionalities are more versatile. On the other hand, hardware-based security is generally more expensive but has traditionally offered better protection, starting down at the root, something that software security lacks. For authentication, especially MFA, while the hardware option has been found in tokens or smartcards, the idea to root it in embedded hardware is the next stage of evolution.

At the very heart of the traditional authentication factor there is one fundamental actor: the humble password. Almost every authentication threshold an employee must go through will involve a password, from accessing their device, to logging in to the company network, to the signing on to VPN client. While password security can be augmented through complexity (numbers, letters, symbols) and requirements can be applied for change frequency, they remain inherently breakable. Rainbow tables, brute force, and increasingly powerful processors can

easily unlock passwords. There is, however, an existing technology with decades of research that can alleviate this problem: biometrics.

3.3. Biometric Deployments and Lessons Learned

Biometric Credentials:



Biometric applications are the answer to the password issue. In the past few years, the underlying technologies for a variety of modalities (with the fingerprint modality currently the primary one) have gone through quite a transformative evolution. Past failed deployments of biometric technologies across many industries have taught some valuable lessons:

- In 2002, Japanese cryptographer Tsutomu Matsumoto was able to spoof fingerprint sensors using gelatin-based sweets. The attack was effective about 80% of the time and could be attributed to poor quality sensors.
- In 2007, the Chaos Computer Club (CCC) managed to spoof a fingerprint sensor in a POS terminal in a semi-supervised retail environment by “lifting” prints off of everyday objects.
- Between 2004 and 2014, there have been several deployments and upgrades to the U.S. Automated Biometric Identification System (ABIS) program, deployed specifically for multiple conflict operations. According to official Department of Defense (DoD) reports, there have been at least four unsuccessful large-scale deployments of the ABIS. The DoD has noted the flaws and moved on to fixing the issues. In summary: a) the system could not perform optimally for user expectations, b) deficiencies existed in high-priority operations that affected mission accomplishment, c) there was significant failure probability when updating / replacing old fingerprint records with newer ones, d) interoperability issues along with failure to coordinate effectively and communicate biometric data across multiple agencies, e) legislation and policy issues regarding biometric data, f) unsatisfactory software development and distribution across multiple platforms.
- In 2009, India introduced the Unique Identification Authority of India (UIDAI) to combat identity fraud and infiltration using fingerprint registration. There were numerous problems ranging from connectivity issues that essentially caused the system to be unable to process a single authentication, to the lack of accuracy in the deployed solution. Another major problem was the failure to “see past” the technological deployment and anticipate problems by researching the user’s perspective first (*e.g.*, over the course of a few months the fingerprints of many manual workers did not resemble the template they registered).
- In 2012, users that still used the UPEK fingerprint software and had not upgraded to AuthenTec’s drivers (after AuthenTec acquired UPEK) were vulnerable to a major flaw. The fingerprint data was effectively

"sitting" in plaintext format in their systems. The sensors were deployed in a vast majority of laptop and notebooks, highlighting the importance of scheduled and mandatory driver and software updates.

- In 2013, the CCC managed to bypass Apple's iPhone fingerprint function shortly after the product was released by spoofing the sensor with prints obtained from a glass surface, prompting the development of new types of spoof-resistant sensors.
- In 2014, the CCC was able to extract a successful fingerprint from the German defense minister in a press conference by using a high-resolution camera, prompting the development of more liveness detection sensors, and setting it as a new standard for high-value sensors.
- During 2015 (and perhaps prior to that), millions of biometric credentials from the Office of Personnel Management (OPM) in the United States were stolen. Sources attribute the incident both as a major cyberattack from a different country and a product of successful social engineering.
- In mid-2015, researchers from FireEye found that OEMs like Samsung and HTC had major software design flaws when it came to storing biometric credentials properly. The data were stored in word-readable, unencrypted, plaintext files. The firm later reported that Samsung's KNOX and other OS updates did in fact receive the necessary patches, prompting the industry to rework the storage issue in the development phase.

The simple reader-storage combination issue that yielded a plethora of vulnerabilities a few years ago has now evolved into a primed-and-ready biometric security authentication protocol that is showcased in the core of the most valuable tech companies worldwide (Microsoft, Intel, Apple, Samsung). Further, it is supported and unified by a growing number of companies (FIDO Alliance) under a common standardization thread (UAF and U2F) and with increasing numbers of enterprise patents being filed every year.

The reader-storage combination has undergone further significant industry review regarding sensor capabilities, credential storage, and product certifications (*e.g.*, NIST, FBI, ISO, IEC, PIV / FIPS, ANSI). It is now subjected to highly sophisticated algorithm design, continues to enjoy funding and support from governments worldwide, and is constantly improved by dynamic R&D initiatives from companies determined to get a competitive edge in the security landscape.

3.4. MFA Hardware Security and Biometrics

As far as multi-factor hardware-based security is concerned, there are two main methods for endpoint authentication. The first is by using an external hardware token. These tokens are usually used as a secondary authentication factor alongside password-protected devices. They also share one crucial similarity and vulnerability with passwords: they can be shared.

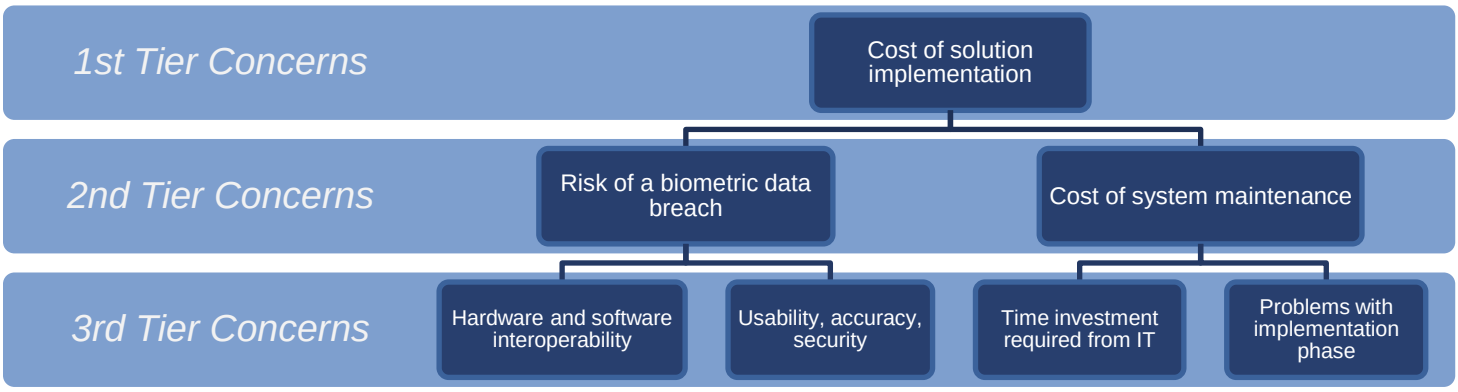
The second is by using a physically embedded solution. Intel's new MFA solution featured in the sixth-generation processor, for example, essentially allows companies to implement hardware-embedded authentication in one simple, interoperable solution. Biometric technologies boost Intel's solution for secure and precise hardware authentication.

4. A CONCISE GUIDE FOR DECISION MAKERS

4.1. Storing Biometric Data: Device-based *versus* Server-based

Safeguarding employees' data is one of the top priorities when deploying biometric authentication methods in the workplace. Insights obtained after multiple rounds of interviews point to the "risk of a biometric data breach" as one of the highest concerns of new implementations. This risk coincides with the latest updates regarding cybersecurity initiatives, but also with debates and developments revolving around data privacy issues. The incorporation of biometric data into the authentication process only exacerbates the privacy threshold. Companies should be adequately prepared to protect their employees' biometric data and to address these issues with a secure and streamlined solution.

Factor hierarchy for decision-makers:



Storing data in the cloud is most common when the deployed solution is taking place in the governmental sector where data management must be centralized.

There are two major technological perspectives regarding storing biometric data: a) server or cloud-based, or b) locally in the device or drive. According to the first, the data are encrypted before and after transmission from a reader, are protected by an enterprise's network security system with its own dedicated server, and are stored in a separate database from other corporate data. The major advantage of this solution is that administrators can have increased control over said data while at rest or in transit. Storing data in the cloud is most common when the deployed solution is taking place in the governmental sector where data management must be centralized. However, it also requires integration with a multitude of other national agency databases. In addition, governmental IT security issues are usually more concerned with the underlying security, usefulness, and accuracy rather than the budget itself.

The latter approach advocates that biometric data should be stored locally in order to protect users' identities in the event of a data breach or inadvertent leak. This perspective is supported by the FIDO Alliance and its members, which include, among others, Google, Intel, Microsoft, MasterCard, Alibaba Group, Samsung, Qualcomm, Nok Nok Labs, *etc*. Furthermore, under FIDO's ongoing standardization umbrella, along with an all-inclusive end-to-end MFA solution, implementers can be sure that interoperability issues can be minimized or even alleviated.

4.2. Fingerprint Authentication

As the *de facto* biometric technology, fingerprint recognition has been the subject of the vast majority of enterprise, governmental, and academic biometric research projects. Past biometric deployments have produced an abundance of valuable information regarding what constitutes a good fingerprint application. Companies advertise the false acceptance rate (FAR) and false reject rate (FRR) metrics almost exclusively as the primary selling point of their respective products. Decision makers must look beyond those metrics into other crucial issues:

- **Image Resolution—Pixels per Inch (PPI) Ratios**: Do they surpass the 500 PPI threshold set by the FBI certification? Have they obtained other certifications? Does the solution aim for PPI in the 800 to 1,000 range?
- **Sensor Specifications**: If the sensor is advertised as "thin" and "easy to deploy," is it robust enough? If the sensor is classified as "capacitive," "sweep," or "solid-state," is it accurate enough? Does it require more than three attempts to authenticate a user?

- **Embedded *versus* USB**: Statistically, external USB sensors are more prone to attacks and vulnerability exploits than embedded sensors. Is there a significant upside for using an external USB sensor? Is the extra cost reflected in the TCO?
- **Liveness Detection**: Does the sensor feature liveness detection or any other counter-spoofing features? Have there been other successful implementations so far?
- **Robustness**: What is the upper level of the sensor's electrostatic discharge (ESD) protection? Does the sensor have proper coating to protect it and prolong its lifecycle after multiple uses? Are the sensor and module easily replaceable?
- **Certifications and Algorithms**: Has the algorithm been tested by the National Institute of Technology (NIST)? Is the company satisfied with those results? Are there certifications from the FBI, ISO, ROHS, CE, or FCC?

4.3. Facial Authentication

There has been substantial concern in the industry regarding bypassing facial authentication, oftentimes with quite simple means. In the last 5 years, it was possible to print out a fairly good resolution photo of someone and use it to bypass the facial recognition software on their computer. Social media and networking sites practically offer a banquet of photos with various lighting and angles for adventuring hackers to alter, print, and attempt an ID bypass. Advances in the industry have sought to fix these vulnerabilities and expand on the features of facial recognition.

Intel's RealSense F200 camera and Microsoft's Windows 10 feature "Windows Hello" are two examples of evolved facial recognition security in personal computers. Intel RealSense is an infrared 1080 RGB camera equipped with 3D scanning due to multiple camera technology, ranging up to 1.2 meter recognition range, and equipped with a highly adaptive SDK. The technology offered by Intel allows for a thorough and sophisticated scan of the users' facial features providing the basis for the creation of a dependable facial biometric credential. Additionally, Microsoft has boosted Windows Hello with a supplementary security feature in order to safeguard users' devices even better. When this feature is enabled, it requires users to tilt their head slightly to each side in order for the algorithm to verify that there is an actual live person in front of the camera. This measure is added as an extra "liveness detection" test and can combat unauthorized authentication by fraudsters who can use a high-resolution photo of the victim.

4.4. Legislation and Education

Security revolving around biometric credentials, as previously mentioned, is one of the primary concerns and barriers for companies seeking a biometric implementation. Part of this technological anxiety, however, also stems from uncertainty regarding legislative changes. While new legislation regarding biometrics will undoubtedly affect the underlying technology and the way companies roll out their solutions to new and existing client base, it should be noted that most regulation regarding biometric technology is already in place. Companies, however, can always benefit by paying close attention to the way governments deal with biometrics issues in border control, citizen ID, and data breaches. Most indications regarding future legislation can be surmised according to which deployments performed as expected, which had significant failures, and whether there are any outstanding personal data or data ownership issues on the horizon.

One of the greatest achievements since the introduction of biometrics in consumer electronics (particularly smartphones) during these past few years is that the users have spent significant time educating themselves and getting accustomed to the technology itself. This fact, along with the commercial success of smart devices, has paved the way for improved versions of recognition modalities (especially fingerprint, face, and voice) to be featured in both commercial, governmental, and enterprise settings. Users are already quite familiar with most of the biometric

technologies and are more educated regarding how proper authentication should be incorporated in their devices (smartphones, computers, tablets).

5. CASE STUDY

Multiple rounds of interviews with market vendors in the biometrics ecosystem, from OEMs and algorithm developers to system integrators and software engineers, have provided insights regarding a wide spectrum of diverse but critical cybersecurity issues. Their input was cross-referenced alongside findings from secondary research and scientific publications in order to provide the following hypothetical case study featuring Intel's MFA solution.

5.1. Background

Following rising tensions between the C-level executives in a company (created from a composite of multiple other real companies), an internal conflict has emerged on the issue of upgrading the security systems. The first part of the case study depicts some of the system susceptibilities and concerns raised by management, employees, and IT. It is assumed that the system will not be compromised under certain low-level attacks, and that IT has fortified the infrastructure with fundamental network and endpoint protection solutions (antivirus, firewall, SIEM, password-protection, VPN). Even so, after digging a bit deeper, some serious vulnerabilities rise to the surface, which unfortunately are attributed to a large degree to the aging computer fleet that still clings to a modern workplace. The second part of the case study shows how Intel can provide a comprehensive solution without requiring a full overhaul of the existing network system or additional security costs, while improving employee productivity and endpoint security.

5.2. Challenges and Vulnerabilities

The company decides that the majority of IT security funds should be allocated towards network security. Prior to considering a new implementation, the IT department witnessed a few external threats but nothing that the existing security system could not handle. In the past, management has decided to forego several upgrade phases of their computer fleet in order to keep costs at a minimum. However, a few other seemingly minor incidents have recently caught the attention of the CIO and CISO. The system occasionally registered credential-entry from a few users during unusual times (*e.g.*, employees signing off and on during lunch breaks or after COB). In approximately one third of the time these instances were also accompanied with authorized users accessing previously retrieved resources from their computer device and transferring said files to unknown recipients not registered in the company database. The access was completely legitimate and even followed most behavioral patterns already registered by the users themselves. Employees denied performing any of the actions recorded on the backend log. Soon the entire picture began to take shape:

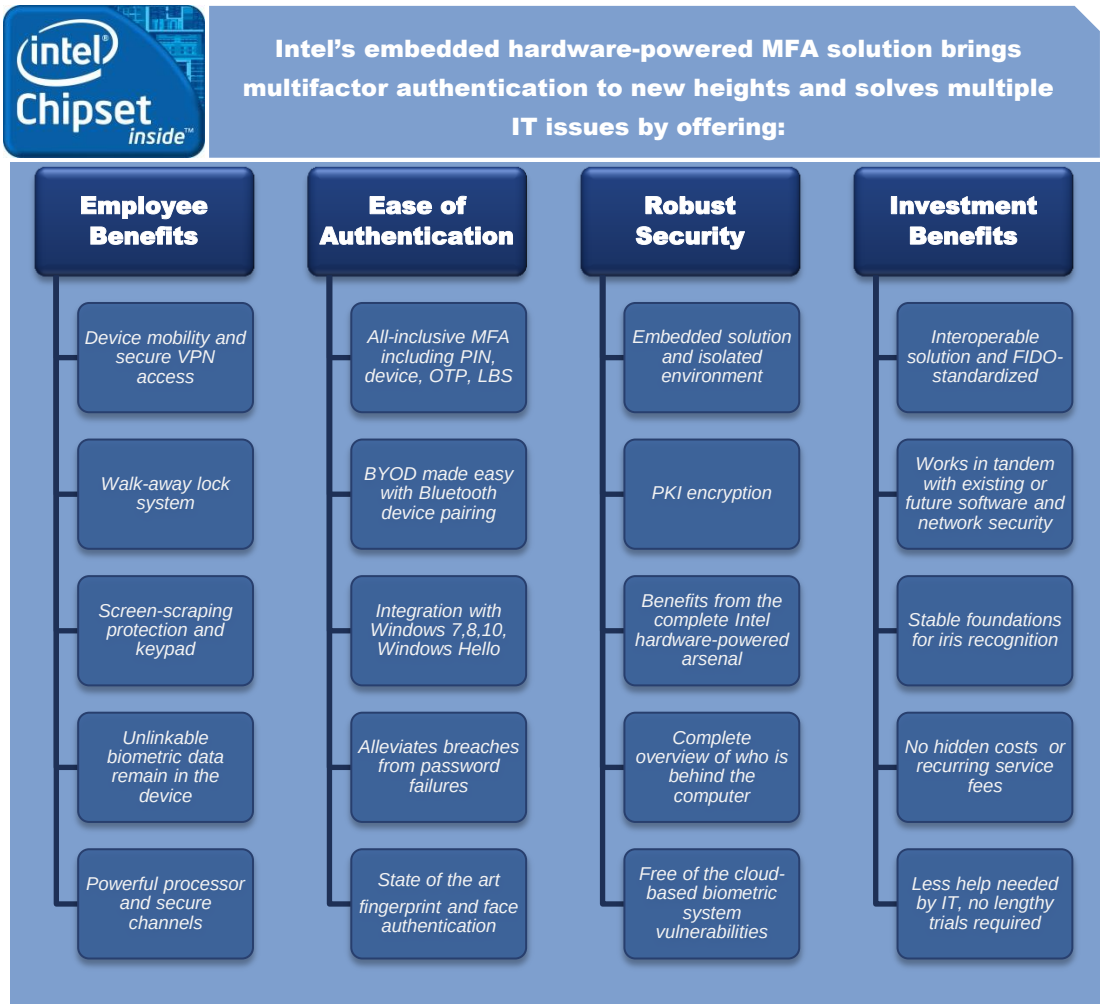
- Employees who had been with the company for three years had changed their passwords every four months according to company policy (*i.e.*, 12 password changes in 3 years). Careful examination revealed that the employee password creation process followed three main patterns: 1) employees rotate between three or four passwords, 2) these passwords are also used in social media, email, and other personal accounts, 3) a different letter is capitalized every time, 4) one number is introduced in front or back or in lieu of a character that makes sense visually (*e.g.*, 1 instead of I or L, 3 or 5 instead of E, 0 instead of O)
- Endpoint investigation on the devices themselves revealed that they had been infected with screen-scraping spyware and / or key-logger malware.
- Infection had remained in those endpoints for well over three quarters, completely undetected.
- Some employees had shared their password with a small number of their colleagues.

- Employees had begun bringing their own laptop devices into the workplace since management was unwilling to undergo the normal replacement circle for company computers. As a result, employees transferred their work to their own devices that held much more computing power.
- Most times, second-factor authentication did not prove to be of assistance since attackers were already in the system and quietly and slowly siphoning out corporate data available in the endpoints themselves. Rather than trying to compromise network security, attackers waited for the employees to transfer information from the network to the endpoint.
- Management and IT opposed the use of external USB biometric readers, along with cloud-based biometric data management on the basis that they might be unsecure, inaccurate, and susceptible to attacks.
- Management was unwilling to justify more expenses in network security, but is currently looking towards an implementation that will yield optimal ROI results.

5.3. Solution

A renewal and upgrade cycle for corporate computers is much needed and Intel's Authenticate arsenal proves to be the solution that both IT and management were looking for. Powered by hardware-enhanced security, Intel, among others, provides:

- A highly secure embedded multifactor solution for endpoint devices, employee satisfaction, data security, and overall increased TBO compared with other software-based solutions.
- Freedom from the vulnerability of passwords and screen-scraping by using biometrics credential input
- Freedom from biometrics-as-a-service costs, third-party system integration, and interoperability issues.
- Peace of mind to both employees and executives regarding the management of biometric-based credentials. FIDO solution ensures that the users' data never actually leave their devices, alleviating user concerns regarding biometric data cloud storage and third-party access.
- Isolated, processor-based storage means that threat actors cannot intercept users' biometric data during the numerous stages of the data trail: sensor data acquisition, data preprocessing, feature extraction, biocryptography and encryption, and database communication channels.



6. CONCLUSION

Both hardware and software security measures for authentication mechanisms need to be employed in tandem in order to provide the enterprise with the necessary tools to combat both internal and external attacks

Endpoint security, along with the lack of computer renewal and recurrent upgrade cycles, are two crucial security aspects that are often overlooked by enterprises. Furthermore, the prevalence of passwords as the primary form of authentication is one that is currently moving away from the spotlight. Both hardware and software security measures for authentication mechanisms need to be employed in tandem in order to provide the enterprise with the necessary tools to combat both internal and external attacks.

A significant number of endpoint vulnerabilities manifest only after careful examination. They can remain completely undetected and malware can often lie "dormant" for well over one whole year and rise to the surface only when its objectives are triggered. Management and IT are also beginning to acknowledge the fact that an aging computer fleet is not only a security risk and a burden to the employees, but also motivates them to migrate their work habits towards their own devices, off-railing any IT attempts to streamline asset protection. They are also more likely to fall prey to incoming phishing or social engineering attacks.

Furthermore, there are strong concerns from employees regarding server storage, management, and use of their biometric data. Biometric technologies have reached critical mass and are beginning to enjoy a plethora of implementations in a wide technological spectrum. MFA and

biometrics are powerful tools in the IT arsenal allowing for more thorough protection of employee data.

Passwords have been a staple of authentication for decades. However, high-scale cyberattacks, data breaches, system compromises, and the emergence of sophisticated cyberespionage campaigns along with the advent of superior malware suggests that a renewal cycle for corporate machines along with a comprehensive MFA implementation is essential in the modern workplace. It is, therefore, important for decision makers to consider the long-term benefits of any newly deployed solutions alongside the appropriate security options for ensuring optimal protection against unauthorized access.

7. TABLE OF CONTENTS

Published February 24, 2016

PO Box 452
249 South Street
Oyster Bay, NY 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com