SafeNet | THE DATA PROTECTION COMPANY

# Authentication in the Modern World

## 4 Best Practices for Adapting to the Shifting Paradigms in IT

**WHITEPAPER**

### Based on the Webcast, "The Token is Dead! Long Live the Token!"

This white paper leverages the insights delivered in a webcast that featured Mike Rothman, Analyst and President of Information Security Research and Advisory Firm Securosis; Andrew Moloney, Independent Security Consultant; Doron Cohen, Vice President Technology, CTO Office, SafeNet and chaired by Mike Smart, Solutions Director, SafeNet. The Webcast was entitled "The Token is Dead! Long Live the Token!", is available on demand, and offers a wealth of pragmatic guidance for adapting authentication to meet current challenges. For more information or to view the webcast, visit **http://www.brighttalk.com/webcast/6319/31581**

### Executive Summary

To contend with the implications of heightened risks, mobile device proliferation, and cloud-based service adoption, organisations will become increasingly reliant on authentication—but the tactical approaches applied in the past will no longer suffice. This white paper reveals several key strategies organisations need to employ in order to effectively contend with the authentication challenges in today's complex, dynamic IT environments.

### Introduction: The New Authentication Paradigm

In recent years, the IT and threat landscape has changed radically, and these new realities present fundamental implications for an organisation's authentication approaches:

- **More sophisticated threats.** Increasingly common and sophisticated man-in-the-middle (MitM) and man-in-the-browser (MitB) attacks have successfully hijacked the transactions of users, even after users completed some form of multi-factor authentication. In addition, a large security vendor was the victim of an advanced persistent threat attack that exposed the seed data of the company's authentication offerings. Subsequently, several of the firm's clients have encountered attacks intending to exploit this seed data.
- **More use cases.** In the past, many organisations had to contend with a single use case: remote employees connecting to a corporate network via VPN. In this scenario, one type of authentication method would support this one use case. Today, the landscape has changed fundamentally, forcing security teams to contend with environments that are much more dynamic and complex. The increased prevalence of cloud-based services and mobile devices has ushered in a wide range of new and evolving use cases—and opened up a host of new vulnerabilities.

While multi-factor authentication has been used extensively for years, what most organisations will see is that these authentication methods will need to be employed for an increased percentage of users, and for a growing number of use cases. Thus, authentication investments and deployments will be increasing. To get real dividends from these authentication investments, organisations will need to ensure that their infrastructure can adapt to current and emerging threats, and today's evolving IT landscape.

The following section explores the two fundamental paradigm shifts occurring in IT, and the implications these trends hold for authentication.

## Shifting Paradigms in IT: The Implications for Authentication

### Cloud-Based Computing Adoption

Historically, much of the emphasis in security was in guarding internal assets from external threats. Firewalls, intrusion detection, intrusion prevention, and many other technologies were employed in this regard. However, given the rise of cloud computing models, the fundamental distinctions between internal and external are blurred, if not rendered meaningless completely. Now, many sensitive assets may be housed externally, and accessed by employees in corporate offices, coffee shops, and home offices. Quite simply, users, data, and applications can be anywhere.

As Mike Rothman, Analyst and President, Securosis explained, "Now's a time where organisations must determine what kind of authentication infrastructure they need to have because the concept of 'our computing, our stuff, our building' has gone away for good."

One of the problems stemming from all the hype surrounding the cloud is a blurring of definitions. Because it is so common to group the range of services available under a singular "cloud" category, much confusion in the market persists. It's important to realise that within the cloud category, there are several distinct models, with unique authentication demands. For example, two of the more prominently adopted models, software as a service (SaaS) and infrastructure as a service (IaaS), present fundamentally different challenges from an authentication perspective:

- **SaaS.** With SaaS, the primary objective is extending enterprise identities to cloud applications. Organisations need to give employees seamless, single sign-on access to SaaS applications, while at the same time ensuring only authorised users with valid credentials are granted access.
- **IaaS.** When organisations adopt IaaS models, the primary objective is extending the enterprise directory infrastructure to external environments, while retaining the controls needed—particularly to apply policies surrounding privileged user access.

"In working with clients, I'm struck by the fact that the cloud, particularly SaaS, is a reality for many organisations, and it's a reality that's taken many security teams by surprise," explained Doron Cohen, Vice President Technology, CTO Office, SafeNet. "These groups are struggling to come up with a comprehensive solution that addresses these new realities, and the pressures of business users, risk management, and auditors."

Authentication remains, and will continue to be, a critical layer within an organisation's security framework. Today, however, authentication needs to be employed in a far more nuanced fashion. Some non-sensitive assets may be protected via basic user name and password, whereas other highly sensitive assets may need to be guarded via three- or four-factor authentication and out-of-band (OOB) verification mechanisms. This more granular application of security mechanisms will be paramount in enabling organisations to fully exploit the benefits of the cloud.

### Mobile Device Proliferation

The widespread adoption of mobile devices has ushered in a fundamental paradigm shift in enterprise IT. In the past, IT would be responsible for procuring and issuing standard computing devices, typically laptops or smart phones, and building security mechanisms based on those standard profiles. Today, however, users and businesses demand access to corporate assets from any device, including the smartphones and tablets purchased by users. This has profound implications for authentication:

- **Expansion of device support.** Where in the past, each user would have at most two devices used to access corporate networks, that number now may be more like four or five. The result is an order of magnitude increase in the number of unique devices that IT must contend with.

- **Heterogeneous device proliferation.** Today, smartphones and tablets based on iOS, Android, Blackberry, Windows Mobile, and a host of other platforms and devices need to be supported.
- **Risk of loss and theft.** The risks posed by a lost or stolen smartphone or tablet may be just as damaging as a lost laptop, and given their form factor and usage, these mobile devices are much more prone to loss and theft.

"Security teams simply can't take the ostrich approach and put their heads in the sand on this," Rothman stated. "Apple shipped over 200 million iOS devices. IT simply can't ignore this reality. These mobile devices are a user demand and a significant risk, and these issues must be addressed proactively."

To manage the shifting paradigms outlined above, organisations need to adopt several best practices. The following sections outline four keys to efficiently, securely, and cost effectively managing this evolution.

## Best Practice #1: Take Strategic, Holistic Approach

For years now, IT and security teams have been caught in a seemingly continuous bind, contending with increasing demands and decreasing resources and budgets. Consequently, it's no surprise that many authentication projects have been tactical and reactive in nature: get alerted to a new security gap or business use case, procure a point solution, deploy, and repeat.

Organisations need to break out of these spirals if they are to contend with the demands they confront today. Before embarking on new investments and projects targeting specific issues, organisations need to start taking a broader, more strategic approach.

"Most security teams don't feel they have the time to operate strategically, they are forced to keep operating tactically and fighting fires," Rothman said. "But the reality is that by taking this tactical approach, they end up building specific capabilities 3 or 4 times, at 3 or 4 times the cost. It's incumbent upon security teams to take a step back and rethink their authentication infrastructure."

Security architects need to start by identifying key use cases the organisation needs to support, and look at building an infrastructure that supports these different use cases. This requires taking a holistic look at where users are, where data is, how users are going to access information, and how sensitive specific applications and data are.

Toward this end, leveraging such industry-standard approaches as the International Organization for Standardization (ISO) framework can be invaluable. This framework can help organisations define common use case profiles and manage accessibility in a standardised manner across disparate platforms.

"Trying to plug a gap every time a new one appears gets us nowhere," explained Andrew Moloney, Independent Security Consultant. "We're now moving into an age where the complexity of the environment in which data resides requires thinking about security more holistically. We need to apply controls in a more adaptive, risk-based way so we get the right level of security at the right time."

## Best Practice #2: Build a Flexible Foundation

As fast as the change has been in recent years, it's safe to assume it will only continue to accelerate. Adapting to today's demands, and those sure to come around the corner tomorrow, will place an increasing premium on flexibility in the authentication infrastructure. This entails meeting the demands of evolving use cases, technologies, business models, and delivery models.

To meet this objective, security teams should endeavor to separate their policy framework from security controls. In the past, many organisations have implemented architectures that were silo'd in nature, with policy management and security controls architected around a

## Strong Authentication Mechanisms: The Alternatives

When it comes to strong authentication mechanisms, decision makers can choose from hardware and software, and within each of these high level categories many different options are available. Following is an overview.

### Hardware

Organisations can choose from a range of hardware devices, including USB tokens and credit-card form factors. While the variances of hardware-based authentication mechanisms are many, in general, these offerings can be grouped into one of the following categories:

- **One-time password (OTP).** These solutions present the user with a temporary, randomly generated set of alphanumeric characters that constitute a password that only permits one login.
- **Certificate-based.** Certificate-based authentication employs public key infrastructure (PKI) and digital client certificates on a smartcard chip for identifying users and controlling access.
- **Hybrid.** Finally, there are also hybrid tokens that provide a combination of approaches. For example, some alternatives combine OTP and certificate-based authentication within a single device. Others combine OOB transaction signing and OTP authentication.

### Software

Today, there are many multi-factor authentication solutions that do not require hardware components. These software-based solutions fall into the following categories:

- **OTP.** Software-based OTP solutions can be installed on desktops and mobile devices. When activated, a solution generates a password for one-time use.
- **Certificate-based.** These software alternatives leverage PKI to generate digital certificates that are stored on the PC or mobile device (rather than on a dedicated hardware key) and that are used for authentication.
- **OOB.** OOB authentication employs two channels of communication, for example, delivering a passcode via an SMS message to a user's authorised phone.

specific use case or subset of use cases. By separating the policy framework from specific security controls, organisations can react more nimbly to change. Put another way, they don't need to reinvent the wheel every time a new use case arises, or make updates in many disparate places to adapt to a global change in policy.

## Best Practice #3: Leverage Context and Risk Levels to Tailor Approaches

In the past, when a minimal number of use cases were supported, authentication could be applied in a simple, more binary fashion—either it was employed or it wasn't. Today, much more contextual intelligence needs to be brought to bear in authentication. This entails tailoring the authentication approach and strength based on who users are, where they are, what they're doing, what device they're using, and what they're interacting with.

For example, if a user is logging in from the same end point, location, and network that they've been using on a regular basis, there is more likelihood that the access request is legitimate, so an organisation may want to enable access through a standard base-line authentication method. On the other hand, if an attempted login comes in from a device or geographic location that hasn't been previously used, a policy may be enforced that steps up the authentication mechanisms required.

Similarly, the approach should be tailored based on the sensitivity and risk associated with the assets and transactions of a given use case. Thus, that same user, even if accessing from an established endpoint, may be allowed initial access via simple authentication, but then be required to submit additional credentials when performing a sensitive transaction.

For a highly sensitive set of assets or transactions, an organisation may require three-factor authentication plus some form of OOB transaction validation. So for example, after furnishing a token and the required credentials through the user's laptop, an SMS message may be sent to the user's mobile phone that provides the details of the transaction along with a one-time password. If the transaction details are correct, the user could then submit the password to signify the transaction has been validated and approved.

To effectively tailor their authentication approaches, organisations will need to leverage a blend of different multi-factor authentication devices and methods, including such mechanisms as USB hardware tokens, PKI-based digital client certificates, OOB, and more. (See sidebar for an overview of the types of alternatives available.)

## Best Practice #4: Centralise Administration

To make all of the above strategies work in the real world, organisations simply cannot continue handling authentication administration in a one-off, disparate fashion. Today, it is essential to leverage a single management platform that provides the visibility and controls for all use cases, policies, and authentication devices. Today, a critical piece of this is the ability to unify the management of mobile devices and their respective credentials, along with those of traditional computing devices.

"We're now seeing a lot of people looking for management platforms that allow administrators to assign credentials to mobile devices and register those devices, along with laptops and desktops," Cohen explained. "This is essential if security teams are to maintain visibility and control, while at the same time satisfying the demands of the user community."

## Conclusion

Strong authentication is vital today—and is only growing more so as organisations contend with the increasing use cases, devices, and computing models that are emerging. To contend with cloud-based services and mobile device proliferation, organisations need to take a strategic approach to authentication, and build an authentication infrastructure that provides the flexibility, security, and efficiency today's businesses demand.

## About the Contributors

Mike Rothman, Analyst and President, Securosis

Mike Rothman's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Rothman specialises in the sexy aspects of security, like protecting networks and endpoints, security management, and compliance. Rothman is one of the most sought after speakers and commentators in the security business and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space. Rothman published "The Pragmatic CSO" in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional.

Andrew Moloney, Independent Security Consultant

Andrew Moloney is a prolific speaker in the IT security industry. Prior to founding his own independent consulting practice, Moloney spent 20 years in a variety of corporate roles spanning the technology sector. Most recently, he was with EMC Corporation serving as EMEA Marketing Director for their security division, RSA, as well as being a key spokesperson for EMC on the evolution and impact of cloud computing.

Doron Cohen, Vice President Technology, CTO Office, SafeNet

Doron Cohen works in the CTO office of SafeNet and leads the technology strategy for the company's authentication and identity protection solutions. Cohen has over 25 years of experience in IT security, directing development of enterprise-class systems and applications. He joined SafeNet in April 2009 following the acquisition of Aladdin Knowledge Systems, where he served as CTO of the eToken business unit.

## SafeNet: Fully Trusted Authentication

SafeNet authentication solutions deliver the protection organisations require, while giving customers a wide range of options that offer optimal efficiency, improved visibility, and unparalleled agility for adapting to changing needs. Only SafeNet delivers a fully trusted authentication environment that gives customers these capabilities:

- **Complete token control.** SafeNet offers organisations the option of creating and controlling their own token data. As a result, customers can enjoy greater flexibility and control, and not be exposed by any compromises at the solution vendor.
- **Centralised management.** All SafeNet authentication solutions can be managed through SafeNet Authentication Manager, a central management server that enables ID federation, access controls, and strong authentication to both on-premise and SaaS applications. As a result, customers enjoy improved control and visibility, simplified administration, and reduced costs.
- **Broad authentication options.** SafeNet delivers the broadest choice when it comes to authentication methods—enabling any enterprise to effectively address the needs of all use cases and risk levels. SafeNet provides a broad range of hardware offerings, such as OTP, certificate-based, and hybrid tokens—including optical tokens that offer out-of-band transaction signing and OTP authentication. In addition, the company's software offerings include OTP, SMS, certificate-based, and out-of-band authentication.
- **Support for innovation and evolution.** SafeNet uniquely supports customers in their ability to embrace today's emerging trends—offering strong authentication and SSO for cloud applications as well as credentialing for mobile device management.

- **Layered data protection.** SafeNet offers a broad range of solutions that enable organisations to employ multi-layered security. For example, with SafeNet HSMs and data encryption appliances, administrators can encrypt and secure sensitive data, as well as the associated cryptographic keys.

## About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

**Contact Us:** For all office locations and contact information, please visit **www.safenet-inc.com**
**Follow Us:** www.safenet-inc.com/connected