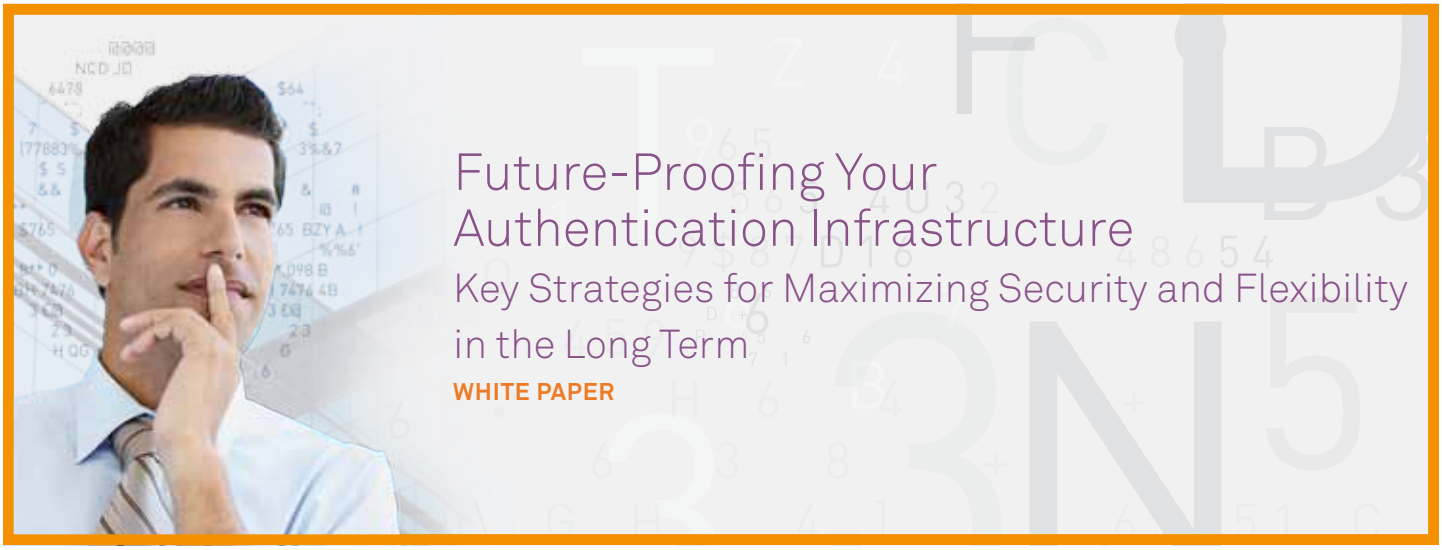

# Future-Proofing Your Authentication Infrastructure

## Key Strategies for Maximizing Security and Flexibility in the Long Term

**WHITE PAPER**

### About This White Paper

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, and Andrew Young, Vice President of Authentication at SafeNet. Entitled "The Token is Dead! Long Live the Token!", the webcast is available on demand, and offers a wealth of pragmatic guidance for adapting authentication to meet current challenges. To view the webcast, visit http://www.brighttalk.com/webcast/2037/29337

### Executive Summary

Sophisticated attacks have placed a heightened premium on strong, multi-factor authentication. However, as the proliferation of cloud services and enterprise-connected mobile devices continues, the process of deploying and maintaining authentication threatens to grow more costly and complex. This paper uncovers key strategies organizations can employ in order to adapt to today's evolving IT dynamics, while persistently safeguarding sensitive corporate assets.

### Introduction: The High Stakes for Effective Authentication

For years now, the need for organizations to secure private and proprietary information has been a critical endeavor. Strong, multi-factor authentication—the use of several factors, such as a password and a token, to grant access to corporate systems—has long been a critical component in an enterprise security framework.

Several recent events call the need for multi-factor authentication—and the means with which this authentication gets employed—into stark focus. Over the course of just a few weeks, a number of high-profile breaches have made headlines:

- A large security vendor was the victim of an advanced persistent threat attack that exposed the seed data of the company's authentication offerings.
- A large military contractor was the target of attacks, which ended up necessitating the suspension of remote access and the reissuance of tokens for many users.
- An email marketing services firm had a breach in which criminals gained unauthorized entry into its systems, exposing 60 million consumer email addresses.

During this same period, a host of other global brands also suffered high-profile, extremely costly breaches in which sensitive corporate and consumer assets were exposed. These events make clear that the security landscape is changing. Cyber criminals continue to grow increasingly sophisticated in their approaches, and this presents significant implications for enterprises and the security vendors that serve them.

## How IT Trends are Changing the Demands on Security and Authentication

Today, the enterprise security teams tasked with guarding against the type of breaches outlined above must contend with two significant trends: cloud adoption and mobile device proliferation. The following sections explore these trends and their implications for organizations' authentication approaches.

### Cloud Adoption

The broad and rapid adoption of cloud-based services poses significant implications for those tasked with administering authentication: How can they move forward with such initiatives as single sign-on (SSO) and identity federation when their IT services are fueled by a mix of cloud and on-premise infrastructures? How can organizations migrate to the cloud while ensuring ongoing compliance with all relevant regulatory mandates?

"When customers move applications from on-premise infrastructures to the cloud, they still want to maintain control over identity stores like Active Directory," said Andrew Young, VP of Authentication at SafeNet. "This presents fundamental changes in the makeup of the user community that authentication must support."

Following are a few of the most significant implications the cloud has on authentication:

- **Increased demand.** In the past, many enterprise security teams would only require multi-factor authentication for remote users. When cloud services are employed, effectively every user becomes a remote user. Therefore, organizations need to employ and support strong authentication for all users of cloud applications.
- **Blurred boundaries.** The move to the cloud also erodes traditional boundaries. Now, an application can leverage data from internal and external sources, and support a mix of trusted and untrusted users. Thus, highly virtualized cloud infrastructures require the support of heterogeneous users and systems.
- **Heightened insider threats.** For years, insider threats have been a persistent and difficult challenge. Particularly with the move to virtualized, public cloud offerings, organizations must contend not only with privileged access of internal employees, but of the administrators employed by the cloud providers themselves.
- **Diversified cloud models.** Authentication controls need to be mapped to the specific characteristics of each type of cloud deployment, whether software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS).

*"In working with clients, I always underscore the importance of asking questions," stated Mike Rothman, Analyst and President, Securosis. "Currently, many enterprise decision makers are at the stage in their cloud migrations where they don't know what they don't know. For example, leadership will be unclear on such areas as standards in public cloud environments and where data integration points will be. It's important to continue to get educated about the impact various cloud models will have on authentication infrastructures."*

"In working with clients, I always underscore the importance of asking questions," stated Mike Rothman, Analyst and President, Securosis. "Currently, many enterprise decision makers are at the stage in their cloud migrations where they don't know what they don't know. For example, leadership will be unclear on such areas as standards in public cloud environments and where data integration points will be. It's important to continue to get educated about the impact various cloud models will have on authentication infrastructures."

### Mobile Device Proliferation

Within many enterprises, the use of smartphones and tablets to access corporate networks and assets was a nightmare scenario for IT and security organizations. As such, the acceptance of these devices was understandably blocked for as long as possible. Yet, at some point, especially as senior management began to demand access from their mobile devices, the flood gates were opened, giving way to what Young calls a "Wild West" scenario, in which it is difficult for security staff to gain visibility, let alone establish control, over access to corporate assets.

Clearly, the risk posed by these scenarios is great. Rather than malware, the key issue confronting security staff is management: ensuring only trusted devices can access corporate resources, contending with lost devices, managing security policies, and enabling and monitoring access. These devices also present password vulnerabilities: passwords stored on mobile devices can be easily compromised because they are stored in a password cache.

## 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

**Organizations 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 have screens that display a randomly-generated set of alphanumeric characters that constitute a password that can be used once.
- **Certificate-based.** Certificate-based hardware offerings use public key infrastructure (PKI) and digital client certificates for identifying users and controlling access.
- **Hybrid.** Hybrid tokens that provide a combination of approaches. For example, some methods combine OTP and certificate-based authentication within a single device. Others combine out-of-band 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 for the generation of digital certificates that are used for authentication.
- **Out-of-band.** Out-of-band authentication employs two channels of communication, for example, delivering a passcode via an SMS message to a user's authorized phone.

Finally, IT organizations need to establish visibility and control over what assets can be accessed by, and saved onto, mobile devices.

As Rothman revealed, "When it comes to mobile device proliferation, whatever the platform—whether Android, iOS, or Windows Phone 7—the issues are remarkably consistent. In spite of their small form factors, these mobile devices are, in effect, computers. If lost, they can present the same potential damage as a lost laptop—and it's a lot easier to lose a handheld device than a laptop."

## Key Strategies for Modern Authentication

To contend with the new realities outlined above, new authentication strategies need to be employed. The following sections uncover some of the fundamental approaches that can help enterprise security teams effectively and efficiently adapt their authentication mechanisms to the critical challenges being confronted today.

## Strategy #1: Tailor Authentication Approaches to Use Cases

Both across organizations and industries, and within a given enterprise, the nature of threats, the value and risk associated with IT assets, and the nature of the way users work with and access IT resources varies substantially. Consequently, the nature of authentication mechanisms employed needs to vary substantially as well.

In some cases, if information in play is non-sensitive in nature, authentication using simple username and password may still suffice. Today, however, for most enterprise users and applications, some form of strong, multi-factor authentication is required. In these cases, security teams can choose from a broad array of mechanisms and form factors. (See sidebar for a summary of these different approaches.) These alternatives provide security management with a host of benefits and trade-offs, factors that will determine their suitability for a given use case. Quite simply, what may work best for one use case may not be suitable for another.

Following are a few critical areas for consideration when choosing among authentication alternatives:

- **Information.** What is the type of information that is at stake, and how much value does it hold? The more value assets have, the more secure an authentication solution should be.
- **Threats.** What are the potential attacks that can be perpetrated, and how does one go about defending them? Organizations need to ensure the authentication mechanisms employed provide the strongest defense against the threat profiles in play.
- **Users.** How technologically sophisticated are end users? How do they conduct primary business functions today? What kind of devices do they carry around? Security organizations need to make sure the authentication mechanism employed is practical for the way end users work. (See the section below, "Strategy #3: Balance Security and Practicality", for more information on this topic.)
- **Total cost of ownership.** What are the upfront costs of various solutions, and how expensive are they to support over time? Security organizations need to balance the need to establish comprehensive access strategies, while effectively managing their budgets and resources.

Based on these considerations, organizations need to employ the solution that most effectively and efficiently achieves their objectives.

## Strategy #2: Centrally Manage Authentication, Across Tokens and Use Cases

As outlined above, within an enterprise, a host of varying use cases may be in play, and security administrators need to select the type of authentication solution that best meets the needs of each specific use case. For example, sales people might need strong mobile authentication when remotely accessing corporate resources; privileged users, such as system administrators, who have access to critical applications, would need a more robust level of multi-factor authentication. Given that, a range of authentication mechanisms may need to be employed in a specific enterprise. However, from a budget, security, and time management perspective, organizations simply can't afford to manage each type of authentication mechanism through a different management platform. It's essential to leverage different authentication mechanisms that can be managed through a central, unified platform.

"Management leverage is critical," Rothman explained. "Organizations should use the right form factor for the right use case, but do so without introducing a lot of overhead in terms of management. Establishing a more flexible infrastructure, while providing efficient management, is of paramount importance."

"Organizations should use the right form factor for the right use case, but do so without introducing a lot of overhead in terms of management. Establishing a more flexible infrastructure, while providing efficient management, is of paramount importance."

## Strategy #3: Balance Security and Practicality

Given the trends and threats outlined above, enterprises will need to support more, not fewer, authentication deployments. Given that, it's essential that management balance security objectives with what's truly practical. This is vital across two fundamental areas: cost and convenience.

### Cost

When assessing cost, decision makers need to factor in both upfront solution cost and total cost of ownership, which includes configuration, deployment, management, and ongoing support and help desk costs. For example, when weighing between hardware and software solutions, most organizations find that software solutions have a much lower total cost of ownership-costs associated with lost tokens, shipping replacement tokens, and a host of other efforts and costs are eliminated when software solutions are deployed. (See sidebar for more information on the tradeoffs and advantages of various authentication mechanisms.)

### End User Impact

Security can't be implemented in a vacuum with respect to end user impact. Organizations have to implement security in way that the end user will accept.

If security teams don't consider the impact on end users, organizations are often confronted with a worst-case scenario in which time and money are invested in security mechanisms, but users ignore or circumvent those processes and mechanisms because they don't want to deal with the inconvenience.

Traditionally, there's always been some level of end user inconvenience or effort associated with the deployment of security and authentication, but there isn't always a direct correlation between higher security and greater inconvenience. In some cases, security solutions can help maximize security while actually boosting ease and efficiency, both for administrators and end users. For example, by enabling capabilities like SSO across both cloud and on-premise applications, end users can actually enjoy greater convenience.

## Key Considerations When Choosing Authentication Solutions

As mentioned earlier, security teams should choose the authentication approach that best meets the needs of specific use cases. When choosing authentication solutions, following are a few key factors to keep in mind:

- **Security.** While software-based authentication mechanisms can effectively address a host of security threats, hardware tokens typically will offer the highest levels of security.
- **Token control.** Some authentication solutions randomly generate passwords, so token vendors never have access to customer passwords. Other solutions offer enterprises the flexibility to program tokens themselves. The benefit of these approaches is that customers don't have to rely on their security vendor for ongoing programming—and they won't be exposed to risks if the vendor experiences a breach.
- **Cost.** By virtue of the fact that they eliminate the need to procure, mail, and replace physical tokens, software-based solutions offer significant cost savings, both up front and in the long term.

## Strategy #4: Deploy Authentication as Part of Multi-Layered Security Approach

It may be a well-worn adage, but it's true nevertheless: the security chain is only as strong as the weakest link. That's why multi-layered security defenses are so vital. Rather than relying on a single point of failure that can compromise the entire business, organizations need to treat authentication as part of a multi-layered security framework.

When organizations manage valuable information assets, they need to also employ encryption to secure those assets. That way, if unauthorized users do somehow gain access to sensitive information repositories, they won't be able to use that information. Further, when encryption is employed, strong security of cryptographic keys is also essential. This often should include the use of hardware security modules (HSMs) that store cryptographic keys in secure, purpose-built devices, and that encrypt the keys themselves, so the highest level of security is realized.

## Strategy #5: Leverage Standards

As organizations look to ensure their authentication infrastructures have the agility needed, they'll be well served by leveraging open standards wherever possible. For example, as organizations employ cloud applications from multiple vendors, having separate authentication mechanisms means users have to login separately for each application.

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties. SAML not only provides a bridge between enterprise identity and SaaS applications, it also enhances the end-user experience by providing SSO capabilities across applications. OAuth (Open Authorization) is another open standard for authorization. Long term, leveraging standards like SAML, OAuth, and the like will be become critical success factors to managing a consistent identity framework across on-premise and cloud environments.

"I would advocate decision-makers really learn about emerging standards and interfaces," Rothman declared. "The reality is that, for most companies, there will be a lot of applications and services in use, which requires a lot of integration work. The more security teams understand and work with standards, the better equipped they'll be to enable new services and ensure interoperability."

## Strategy #6: Manage Risk and Expectations

The days of complete control over IT security are long gone. Even if they wanted to, IT security teams couldn't stop the proliferation of mobile devices or the increased adoption of cloud services. These trends need to be embraced, while mitigating their risks.

"There is risk in any kind of new application or architecture," Young explained. "Today, the security practitioner's role isn't to decide what is adopted and what isn't. Practitioners need to communicate to senior management what the risks of new services and technologies are, and let the business decide what level of risk tolerance is acceptable."

## SafeNet: Fully Trusted Authentication

SafeNet authentication solutions deliver the protection organizations 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 organizations 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.
- **Centralized 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 organizations 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 the Contributors

### Mike Rothman, Analyst and President, Securosis

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security, like protecting networks and endpoints, security management, and compliance. Mike 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.

Starting his career as a programmer and a networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held VP Marketing roles at CipherTrust and TruSecure–providing experience in marketing, business development, and channel operations for both product and services companies.

### Andrew Young, VP of Authentication, SafeNet

Andrew Young is responsible for setting the strategic direction of SafeNet's commercial and government-related authentication products. He oversees a team of product managers responsible for setting go-to-market strategies and technical requirements for the product line.

Andrew joined SafeNet in March 2004, through the acquisition of Rainbow Technologies, where he led a team of software development engineers. During his 13 years with SafeNet and Rainbow, Andrew has focused on identity access and strong authentication-related solutions, including certificate-based authentication (CBA) and one-time password (OTP) solutions. He has successfully brought numerous hardware and software products to market. Prior to Rainbow Technologies, Andrew managed a consulting practice for Spectria, focusing on building custom applications for wireless WAN and LAN networks.

## Conclusion

Strong multi-factor authentication is vital today—and is only growing more so as organizations continue to embrace more mobile devices and cloud-based services. To address these trends—while safeguarding sensitive corporate assets—security teams must employ several core strategies. With solutions that offer unrivaled breadth, manageability, and control, SafeNet enables organizations to effectively and efficiently employ these strategies.

## About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

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