Next-Generation Authentication
Keys to Balancing Security and Convenience

Executive Summary
The demands for heightened security through the use of multi-factor authentication are pressing, but so is the need to control budgets and give users convenient access to the data and services they need. It is growing increasingly clear that organizations can’t meet these demands with legacy platforms—they need next-generation authentication. This paper examines why this need for next-generation authentication is so vital, and it offers a detailed look at the key characteristics that distinguish these platforms from other alternatives.

Introduction: The Changing Technology Landscape
In recent years, those tasked with managing IT and security have had to contend with changes that have been fundamental and fast in coming. Today's technology environments bear little resemblance to those of even a few years ago, and the pace of innovation continues to accelerate. Following are a few of the characteristics that IT and security organizations are contending with:

• **Device ubiquity and consumerization.** Users have a plethora of devices and device types, both personal and company issued, and use them to access not only personal but corporate resources as well.

• **Continuous access.** Users are accustomed to 24/7 access to data and services, whether they want to check email, download a movie, or access a SaaS application.

• **“Shadow” IT.** Increasingly, business units and groups and even individual employees are taking it upon themselves to procure IT services, whether that means subscribing to a SaaS offering, downloading a productivity application, or renting cloud storage. For example, the move to cloud-based storage has quickly permeated the enterprise, largely without or even in spite of, IT involvement. In fact, Dropbox is reported to be in use by two million businesses and 95% of the Fortune 500.

• **Proliferation of data repositories.** Enterprises have entered a hybrid era, one in which corporate data is proliferating, both within the data center as well as across cloud and external service provider environments.

These trends have given rise to a threat landscape that is infinitely more complex than years before. This technology and threat landscape has created some fundamental implications for security professionals generally, and perhaps none more so profound than in the area of user authentication. Now more than ever, organizations need to employ strong authentication, without impeding any of the convenience and access that users have come to expect in recent years.

---

The Security Risks

The shifting trends outlined above have fundamentally altered the security landscape—and highlighted a critical gap that’s present in many organizations today. Often, access to critical corporate assets is only secured via static user name and password. While many organizations have employed multi-factor authentication, generally, adoption isn’t widespread among the employee population. For example, a recent SafeNet survey found that in more than half of organizations, less than 30% of employees use multi-factor authentication. Further, of the employees that do currently use multi-factor authentication, the vast majority solely use it for gaining VPN access. By and large, most organizations and most employees are not using multi-factor authentication to gain secure access through mobile endpoints or to access cloud resources.

This limited use of multi-factor authentication presents a critical vulnerability, one that is exploited in the majority of attacks, whether perpetrated through the Web, email, or other open services. In fact, according to the Verizon 2013 Data Breach Investigations Report, four out of five of the breaches reported stemmed from authentication-based tactics, where attackers attempted to guess, crack, or reuse valid credentials. Perhaps most disturbingly, many targeted attacks, including advanced persistent threats (APTs), are often initiated through these compromised passwords.

Given the prevalence of users bringing their own devices and even their own services to work, the risks to enterprise assets can be further exacerbated by static user names and passwords. Often users will employ the same password for both personal and corporate services and devices. As a result, a breach of personal passwords can pose a risk to the user’s employer. Compounding the problem is that the market for hacked credentials is large and growing. Today, anyone can do a general Web search and find entire databases of compromised user names and passwords.

Compromised passwords are devastating on multiple levels, perhaps most significantly because so much of the corporate infrastructure relies on these passwords for granting access. If a password is compromised, it can be difficult to uncover. The problem is that, while perimeter defenses are in place, these mechanisms are set up to accept only user name and password. Once attackers gain access to users’ credentials, they can get past existing defenses and gain access to corporate assets, completely undetected. Consequently, these breaches are often only uncovered when it’s too late, long after the attack occurs. The Verizon report found that 66% of breaches took months to uncover.

The Need for Next-Generation Authentication

The devastating breaches that are occurring highlight a fundamental reality: Organizations need to eliminate the critical security gaps associated with using static passwords. To address security gaps, emerging threats, and evolving infrastructures, security teams need to more broadly leverage multi-factor authentication.

Historically, organizations haven’t employed multi-factor authentication broadly for a very good reason: It’s been costly and complex to implement and support. While multi-factor authentication is a critical requirement, it is not one that can be addressed in a vacuum. Clearly, to start leveraging multi-factor authentication in a pragmatic manner, organizations have to strike a balance between security, user convenience, administrative efficiency, and cost. To meet these requirements, organizations need to begin leveraging next-generation authentication platforms. The following section provides an in-depth look at these platforms, offering details on their key characteristics and requirements.

---

3 Verizon 2013 Data Breach Investigations Report, page 34
4 Verizon 2013 Data Breach Investigations Report, page 6
Next-Generation Authentication: Key Characteristics and Requirements

End User Convenience

Over the past few years, advances in access models and interfaces have continued to raise the bar in terms of user convenience. To be practical, next-generation authentication platforms have to be aligned with these realities and the expectations users now have. Consequently, to be broadly deployed and consistently used, authentication mechanisms have to offer convenience and transparency for end users. Following are several of the capabilities required to achieve this convenience:

- **Device flexibility.** Next-generation authentication platforms have to enable user access from multiple devices, including tablets, laptops, and smart phones. This requires mechanisms for generating software tokens that can be run on any device.

- **Administrative controls.** Administrators need to be able to manage all users across all devices and resources. To meet this charter, they need automation, central management, and visibility into user access across multiple resources. To ensure users have an optimal experience, administrators need to be equipped with granular controls and flexible customization.

- **Frictionless authentication capabilities.** To ensure security controls are enforced, while streamlining user access, organizations should have the ability to enable frictionless authentication. With frictionless authentication, an organization can elect not to require the use of a token in specific cases, for example if a user is accessing a low-risk platform from a trusted device.

- **Software-based tokens.** By leveraging software-based tokens, organizations can simplify the user experience, and reduce the cost and help desk calls associated with hardware tokens.

- **Single sign on.** Next-generation authentication platforms need to enable users to sign on once to gain access to all corporate assets. Leveraging open standards like SAML, these platforms can, for example, enable a user to log on to Google apps, and when he subsequently goes to Salesforce.com, have the credentials automatically furnished to the application, so he can get straight in, without having to log in.

By delivering the capabilities above, next-generation authentication platforms allow organizations to implement strong authentication for many more users and use cases than would otherwise be practical.

Administrative Efficiency

Next-generation authentication platforms must deliver capabilities that help streamline administration. For example, these platforms need to provide an intuitive, customizable portal interface that allows users to manage tokens on their own, reducing help desk calls, administrative efforts, and support costs. Further, through support of software tokens, tokenless approaches, and context-based authentication, these platforms enable organizations to reduce their reliance on hardware tokens. This enables organizations to enforce strong security policies, while reducing the costs associated with procuring and shipping hardware tokens, following up in the event of lost tokens, reissuing and resenting tokens, and so on.

In addition, these platforms provide significant time and cost savings through automation of such efforts as user on-boarding, provisioning, and reporting. Through this automation, organizations can reduce administrative costs, while helping ensure more consistent policy adherence. For example, when users forget their passwords, typically, they’ll try several times and after the third attempt, they’ll be given a message indicating their account has been suspended, and that they need to call the help desk. The end result is that end users have to spend time calling the help desk and having their password reset, and the business suffers from lost productivity and high ongoing help desk costs.

Contrast this with the same scenario when next-generation authentication is employed. In that case, when a user attempts three logins unsuccessfully, an SMS message can automatically be delivered to the user’s mobile phone, notifying them of the logins, and asking them to verify whether it was them or someone attempting to access the account.
fraudulently. The user can obtain a one-time password to login, or notify the help desk if there’s been fraudulent activity—and all this effort can be automated, and take place without any administrator involvement.

Following are some additional requirements:

- **Multi-tenant support.** Next-generation authentication platforms should also offer multi-tenant support that makes it efficient for IT organizations to serve multiple business groups. Through a central platform, administrators should be able to apply policies, manage SMS gateways, and even branding, whether for an entire organization or a specific subset of users.

- **Directory integration.** To be practical, next-generation authentication platforms need to enable integration with an organization’s directory service, such as Active Directory or LDAP, so administrators can leverage their existing user groups and policies. This directory integration should be non-intrusive and offer full synchronization.

- **Standards adherence.** To provide IT organizations with maximum flexibility and efficiency, next-generation authentication platforms should adhere to common standards, such as SAML and Radius, and use standard authentication APIs.

**Robust Security**

In the end, any authentication deployment will be fruitless if it doesn't address an organization's critical security gaps. That's why next-generation platforms should provide maximum security, including strong protection of keys and dynamic generation of seeds.

Following are a few of the most critical security requirements a next-generation authentication platform should address.

- **Comprehensive Coverage.** Organizations need a unified authentication platform that can protect not only the data center perimeter, but cloud applications, databases, and business applications.

- **Context-driven Identity, Access Management.** Security teams need to be able to apply varying controls depending on the specific scenario, and automatically have stronger policies enforced when highly sensitive assets are being accessed or higher-risk situations arise. Security teams should be able to apply policies based on who the user is, what they're attempting to access, where they're located, and whether the device is trusted. In addition, policies should also be customized based on a user's past activities.

  For example, through such tactics as device identification, encrypted cookies, and browser fingerprinting, a specific user access attempt can be deemed low risk, and enable the users straight access to an asset, without even having to submit a user name and password. On the other hand, if that same user attempts to access the same asset from an untrusted network using an unregistered device, they can be required to do multi-factor authentication before being granted access.

- **Automated Alerts.** To ensure security administrators are alerted immediately if a breach or suspicious activity occurs, next-generation platforms should provide configurable, automated alerting capabilities.

- **Secure Platform and Deployment.** To ensure maximum security, next-generation authentication platforms themselves need to offer capabilities that safeguard sensitive assets and processes. These platforms should offer support for hardware-based storage of keys through the use of hardware security modules, protecting seed keys and storing all keys in an encrypted format. In addition, all seed keys should only be owned by the subscriber, rather than the token vendor, and be dynamically generated. Finally, the platform should offer robust reporting and auditing capabilities, so administrators can have a detailed history of user activity, and an audit trail that can be used for compliance and forensic purposes.
Flexibility
As recent years have amply illustrated, change and innovation don’t just continue, they continue to accelerate. Given these realities, an optimal next-generation platform needs to provide IT organizations with broad implementation and administration flexibility, so they can respond to changing demands and opportunities, while maximizing the utility of their investments. To provide this flexibility, next-generation authentication platforms should offer the following capabilities:

- **Support for all access needs.** The next-generation platform should address any near-term and long-term secure access needs, including support for VPNs, SaaS offerings, Web portals, and more.

- **Broad token support.** Platforms should offer support for a range of tokens, including hardware, software, SMS, and tokenless options, as well as tokens from a number of vendors.

- **Open integration.** The platform should offer flexible integration, with every feature accessible via an open API.

- **Easy customization.** Next-generation authentication platforms should offer easy customization, both to support modifications for the entire user community, as well as for specific groups. Virtually every area, including reporting, interface elements, roles, language, and alert messages should be easily customizable. Even password complexity should be flexible, for example, enabling the requirement of longer, more complex passwords in higher-risk cases, while enabling shorter and simpler passwords in other cases.

- **Cloud deployment.** Given the advantages they provide, cloud deployment models continue to be used for an increasing range of services and applications, and next-generation authentication platforms should be aligned with this opportunity—offering both private and public cloud deployment options. By offering support for cloud-based deployment, these platforms will enable companies to get up and running in minutes and realize the flexibility of a pay-as-you-go pricing model. However, to be viable, these cloud-based deployments need to offer the highest levels of resiliency and security. Look for platforms that offer 99.999% uptime SLAs and that ensure no personal or sensitive data is ever stored in the cloud.

**Conclusion**
By expanding their use of multi-factor authentication, organizations will be poised to address their most critical security gaps. By leveraging a next-generation authentication platform to deploy and manage multi-factor authentication, organizations can realize these security benefits while addressing their objectives for managing costs and delivering a quality user experience.
About SafeNet Authentication Solutions
With over 17 years’ experience in the market, SafeNet delivers authentication solutions that are proven and trusted by thousands of enterprises around the globe. SafeNet helps organizations address their business and security needs, while adapting to the challenges of the cloud, mobility, and escalating threats.

SafeNet authentication solutions offer flexible and simplified service delivery. Compared to traditional models, SafeNet authentication solutions streamline implementation and management through automated processes, which drastically reduces the time and cost of provisioning, administration, and managing users.

By offering a wide range of authentication methods and form factors—combined with Web-based, single sign-on capabilities and flexible pricing models—SafeNet makes it practical and cost effective to address numerous use cases, assurance levels, and threat vectors. SafeNet enables centralized policy management from a unified authentication platform that can be run in the cloud or on premise.

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.