SafeNet | THE DATA PROTECTION COMPANY

Smart Phones and Tablets in the Enterprise

Embracing the Opportunities while Eliminating the Risks

WHITEPAPER

Executive Summary

Whether IT organizations choose to embrace, resist, or deny them, the reality is that the increased prevalence of mobile devices in the enterprise presents a range of fundamental implications. This paper examines the paradigm shifts taking place in enterprise IT organizations today, and then focuses on the key implications the proliferation of mobile devices has for authentication. The paper then uncovers some of the key strategies for making mobile authentication work effectively and securely in today's IT environments.

Introduction: Evolving Paradigms and Security Challenges

For the people tasked with security in today's enterprises, the job keeps getting tougher and the stakes keep getting higher. Following is an overview of some key trends that are raising the pressures for IT and security teams.

...the sensitive information on social networks enables an array of social engineering attacks, further exposing organizations

Attacks Growing More Frequent and Sophisticated

Today, organizations are under siege, getting hit by a virtually continuous onslaught of attacks that target sensitive corporate information and assets. Cyber criminals continue to get more sophisticated and have more advanced tools at their disposal, targeting corporations with continuously evolving threats and approaches. Now, the sensitive information on social networks enables an array of social engineering attacks, further exposing organizations. Consequently, it's no surprise that in the past year, some of the top brands in financial services, consumer electronics, retail, and even security have been the victims of devastating attacks.

Corporate Boundaries Growing Cloudy

Years ago, organizations looked to leverage technologies like VPN to provide remote users with access to all enterprise assets, effectively expanding the corporate perimeter. Today, the perimeter hasn't expanded, it's dissolved completely. This is due in no small part to the widespread adoption of cloud offerings and other online services. Increasingly, software, computing, and infrastructure are being subscribed to as a service, rather than being installed within a corporate data center.

This move has fundamental implications. In the past, an organization may have to contend with a single multi-factor authentication use case: a remote employee accessing the corporate network through a VPN. Today, the number of use cases has expanded substantially, encompassing more users, computing models, risk factors, and more.

Plus, the number of passwords, and associated administration effort, increases substantially. For years, organizations have struggled to consolidate passwords and accounts and deliver a single sign-on experience to users. Now, an employee may have dozens of different logins and passwords, one for corporate networks, one for each SaaS offering, and so on. Consequently, in many organizations, initiatives around identity federation and SSO need to be rethought completely.

Consumers Growing More Involved in Endpoint Procurement

Not too long ago, most IT organizations enforced strict standards around the endpoints that could access corporate networks and resources. This typically meant the IT group led the procurement, configuration, and updating of company-issued laptops and desktops. Today, in most organizations, the endpoint picture looks very different, with end users increasingly driving the procurement and use of their own devices. Many users now want to work with their own personal laptop, and, as detailed further below, also demand some form of access from their mobile devices. Consequently, the number of potential variations of operating systems, applications, and devices grows exponentially more complex.

Many users now want to work with their own personal laptop, and, as detailed further below, also demand some form of access from their mobile devices. Consequently, the number of potential variations of operating systems, applications, and devices grows exponentially more complex.

In addition, the line between personal and professional use gets blurred, with most endpoints now housing a mix of assets. The use of social networks for both professional and personal purposes further serves to blur these boundaries.

Now, instead of accessing networks through a single company-issued endpoint, users now are accessing corporate applications from just about anywhere, with their phones, tablets, and other personal devices. In some organizations, this has been by design: IT groups have made a conscious decision to open access policies to more devices. In others, organizations have tried to keep tight reins on the devices that can access corporate networks, but they have met with limited success. Most often, end users find ways to circumvent policies and security mechanisms, so they can still access corporate resources with their own personal devices.

Mobile Devices Growing More Prevalent in the Enterprise

The sophistication and ubiquity of mobile devices have fundamentally changed user expectations and demands. Users have increasingly lofty expectations when it comes to being able to access corporate networks, thinking they should be able to do so any time, from any place, using any device. On a given morning, a user may start by checking email with a smart phone and then want to modify and email a document using a tablet. Then, on the way into the office, he or she may want to use a laptop and a coffee shop's Wi-Fi network to access one of the company's cloud services.

The proliferation of these kinds of scenarios has posed a host of significant implications for security, and specifically around the management and enforcement of authentication policies. In the following section, the paper looks at these implications in detail.

Mobile Devices: Security and Authentication Implications

The increased prevalence of mobile devices in the workplace has several key implications from a security and authentication standpoint. As smart phones and tablets grow more prevalent, employees are increasingly looking to use these devices to access corporate networks and resources. This can present risks in several key areas:

- **Usage.** If a device is lost, how do organizations prohibit unauthorized users from working with the device, whether to make calls, access the network, or any other purpose?
- **Data.** Users may store a wide range of information assets on their mobile devices, including emails, documents, and more. If a device is lost or stolen, how do organizations ensure this potentially sensitive data is protected? How can organizations control access to this information, or do a remote wipe of the device to ensure data doesn't fall into the wrong hands?
- **Credentials.** Like data, credentials are also often stored on mobile device memory. This can pose risks, potentially compromising not only the devices themselves, but any corporate network or asset that the user has access to.

Strategies for Effective Authentication in Modern IT Environments

To contend with the trends and risks in effect in today's enterprise IT environments, organizations need to employ several strategies. Following are the three key strategies enterprise IT organizations need to execute on in order to both mitigate the risk and embrace the opportunity posed by mobile devices in the enterprise.

Strengthen Security through Multi-factor Authentication

It is highly common for users to have their credentials cached on their mobile devices. However, this can pose obvious security risks: if the device falls into the wrong hands, those cached credentials can open the door to unauthorized access to corporate networks and assets. Consequently, organizations need to guard against the unauthorized use of these credentials if a device is lost or stolen.

> If the device falls into the wrong hands, those cached credentials can open the door to unauthorized access to corporate networks and assets.

Further, to address compliance mandates and security best practices, organizations can't continue to rely on basic username and password when it comes to authenticating users. Instead, organizations need to secure sensitive assets and processes through the use of strong, multi-factor authentication.

To address this need, mobile devices are increasingly being used as a means to do multi-factor authentication. Where in the past, many organizations invested in various hardware tokens, such as USB tokens and smart cards, now organizations are turning to mobile devices as a software authenticator for accessing corporate networks. For example, organizations are increasingly employing out-of-band authentication approaches using mobile phones. Through these approaches, organizations can better secure access to a corporate service, either from traditional laptop or from a smart phone. Plus, since users don't have to carry a hardware token, they enjoy greater convenience.

Maximize Convenience for Users and Administrators

Federate Identities

A big challenge for organizations is optimizing ease of use for employees. As mentioned earlier, the adoption of cloud services, along with the expanded use of mobile devices, has impeded the efforts of many IT organizations looking to get to the point where users can leverage a single sign on to gain access to all corporate assets and services. Quite simply, with today's mix of cloud and on-premise services, we now have too many passwords to remember. To combat these trends, organizations need to begin federating identities across all corporate services.

> Quite simply, with today's mix of cloud and on-premise services, we now have too many passwords to remember.

Mitigate Administrative Complexity of Cached Credentials

The caching of passwords on mobile devices may offer some convenience for users, but, as outlined above, it poses fundamental security challenges. Further, this caching of passwords also presents administrative complexity. For example, if a user changes his or her password in Active Directory, how does that update get reflected in the cache? How can these updates get propagated effectively and securely to ensure organizations are protected, while end users are assured unimpeded access to required resources. What happens if a user tries to gain network access with an expired password in their cache?

Organizations need to address these challenges while ensuring easy, consistent, reliable access for end users. Further, administrators need to extend this ease of use to users of on-premise as well as cloud-based offerings. To address these demands, administrators need a centralized platform for controlling credentials and ensuring they are propagated across device caches and authentication systems.

Enable Self-service Provisioning for Users

Over the years, enterprises and their vendors have developed effective solutions and processes for managing desktops and laptops, but those capabilities are lagging when it comes to mobile devices. For example, many organizations aren't able to provide users with self-service access to sign up or receive updated mobile device credentials. To streamline administration, organizations need to be able to deliver self-service capabilities that are fast and easy for employees to work with, that are fully integrated with self-service desktop or laptop provisioning systems, and that ensure consistent policy enforcement.

Enable Remote, Over the Air Management

Mobile devices can't be ignored by IT and security teams, but given the exponential increase in the number of endpoints in use, administrators simply can't manually support each device. To effectively and efficiently manage authentication and security of mobile endpoints, administrators need to leverage remote management and over-the-air deployment of credentials.

Unify Management and Policy Enforcement

To address their organization's budgetary and security objectives, security teams simply can't treat the authentication of mobile devices in an isolated fashion. If they do, they will find themselves in a situation in which they'll have to deploy and use multiple controls and management systems in order to provide the coverage of all different channels of service that need to be accommodated, which leads to high complexity and cost—and inconsistent policy enforcement. Consequently, it is essential for security administrators to have a centralized, unified way to manage authentication:

- Across smart phones, tablets, desktops, and laptops.
- Across multi-factor authentication devices and approaches, including smart cards, USB tokens, software-based authentication, out-of-band authentication, and more.
- Across use cases, including cloud and on-premise, with the flexibility to tailor authentication to specific risk levels.

How SafeNet Authentication Manager Addresses Today's Authentication Requirements

SafeNet Authentication Manager provides organizations with a comprehensive platform to manage the full authentication life cycle and to extend strong authentication to the cloud. SafeNet Authentication Manager makes it fast and practical to employ strong, multi-factor authentication mechanisms—so organizations eliminate the risk of having users rely on cached credentials. SafeNet Authentication Manager automates the provisioning of credentials, and delivers visibility and control over which devices can access the network. SafeNet Authentication Manager enables administrators to deploy and provision over the air, across all mobile devices.

SafeNet Authentication Manager makes it fast and practical to employ strong, multi-factor authentication mechanisms—so organizations eliminate the risk of having users rely on cached credentials.

A Unified Platform for All Authentication Needs

With SafeNet Authentication Manager, organizations can avoid having to address mobile device authentication as a silo'd, stand-alone effort. To the contrary, the solution enables organizations to address authentication in a cohesive, efficient, and secure manner for their entire workforce. SafeNet Authentication Manager delivers a single platform and console for managing:

- **All devices and platforms.** SafeNet Authentication Manager can manage mobile access for each user, whether they're using a company-issued laptop, their home laptop, their iPad, or their smart phone.
- **All authentication mechanisms.** SafeNet Authentication Manager can centrally manage all authentication mechanisms, including x509 certificates, USB tokens, smart cards, out-of-band authentication mechanisms, and software-based one-time passwords.
- **The entire credential lifecycle.** SafeNet Authentication Manager enables administrators to manage the spectrum of authentication efforts from a single console, including provisioning, renewal, and revocation.
- **All use cases.** SafeNet Authentication Manager can give administrators visibility and control into all the authentication use cases the business requires, whether it's a user trying to gain access to a SaaS application, an employee working on premise with a company-issued laptop, a telecommuter looking to gain VPN access from a home desktop, or a traveling executive wanting to access a corporate portal from their iPad.

Delivering Unified Visibility and Control

SafeNet Authentication Manager is a comprehensive platform that enables flexibility, consistency, and control. This platform offers a common policy and management layer that gives visibility to all certificates and credentials a given user has obtained. SafeNet Authentication Manager enables administrators to view, manage, and revoke all credentials—from a single console. SafeNet Authentication Manager offers a common framework for administrators to decide which types of certificates need to be used in each use case, what renewal schedules there should be, what PIN policies should be enforced for different devices, and so on.

With these capabilities, SafeNet Authentication Manager enables administrators to practically enforce tailored policies to a range of usage scenarios. For example, in some cases if a user is on a corporate laptop and within the corporate premises, they may be authorized to access the corporate network through a startup ID and password. On the other hand, to conduct a highly sensitive transaction, such as a large fund transfer, they may be required to authorize the transaction through out-of-band authentication. Alternatively, if they are accessing the network remotely from a mobile device, they may need to use a certificate, or a one-time password generated by a smart card, before they are granted access. In addition, SafeNet Authentication Manager makes it practical to deploy multi-factor authentication for privileged accounts, such as cloud or network administrators.

This central platform means organizations can embrace cloud offerings, while at the same time federating identities and delivering single sign-on access to users, both when they are accessing on-premise and cloud-based applications.

SafeNet Authentication Manager Benefits

SafeNet Authentication Manager delivers a host of benefits to organizations, enabling them to effectively address the critical authentication challenges they confront. With SafeNet Authentication Manager, organizations can realize these benefits:

- **Visibility and control.** With SafeNet Authentication Manager, organizations gain the visibility and control they need to consistently and effectively enforce security policies, so they can guard against the risks associated with mobile devices accessing corporate networks.
- **Streamlined management.** With SafeNet Authentication Manager, organizations can leverage a unified console and platform that enables administrators to efficiently manage authentication across use cases, end points, and more.
- **Low total cost of ownership.** Because it represents a single platform that can manage an enterprise's authentication, organizations can eliminate the cost and administrative overhead of procuring, deploying, and maintaining multiple authentication management platforms.

How SafeNet Authentication Manager Works

The following sections offer more detail on how SafeNet Authentication Manager is used within an enterprise, describing the deployment of certificates on iOS devices and end user enrollment via a self-service portal.

Deployment of Certificates on iOS devices

SafeNet Authentication Manager leverages the native, iOS configuration profile features available for Apple mobile devices. As a result, administrators can use the standard tools and interfaces that Apple provides in order to configure authentication policies.

SafeNet Authentication Manager fully supports the simple certificate enrollment protocol (SCEP). This protocol allows users to work with the browser on their mobile device to connect with the organization's certificate authority. Then the solution generates a certificate and automatically deploys it on the device.

To get started, administrators would create enterprise configuration profiles using Apple configuration tools. Then administrators would use SafeNet Authentication Manager to deploy and enforce additional policies, whether for certificates, PINs, or data encryption. Those configuration profiles would get integrated into SafeNet Authentication Manager and associated with enterprise security policies.

For example, an administrator can deploy a specific set of configuration profiles for a specific user group. These configuration profiles can specify whether users can access a Wi-Fi network, VPNs, and so on. Once administrators have completed the required configuration, SafeNet Authentication Manager automates a lot of the processes that would otherwise require a lot of time-consuming, manual work for administrators. SafeNet Authentication Manager enables certification provisioning, enrollment of user credentials on devices, and credential renewals. Further, if an employee leaves the organization, the administrator can revoke that user's credentials with a single click in the console.

an administrator can deploy a specific set of configuration profiles for a specific user group. These configuration profiles can specify whether users can access a Wi-Fi network, VPNs, and so on.

End User Enrollment via a Self-service Portal

SafeNet Authentication Manager equips organizations with a Web-based portal that enables users to easily enroll their device in order to enable it to gain access to corporate networks and assets. Following is an overview of the how the process works.

First, a user can only enroll a device if the administrator has defined the proper policies for that user, device, and so on. Before getting started, the user would also need any required approvals, based on the user's organizational structure, and group and role membership. Once any established criteria have been met, the user can then enroll their device, get their certificate, and, based on the established configuration profile, have it deployed on the device.

With SafeNet Authentication Manager, users can enroll for certificates as well as OTP authentication software. Further, OTP security can be enabled through SafeNet MobilePass, a software OTP generator, which employees can use to access services both from their mobile device as well as their desktop or laptop. The MobilePass application is available to be downloaded, and it can be activated via a Web browser or over-the-air activation. If organizations are using BlackBerry devices, they can use the BlackBerry enterprise server to deploy the MobilePass application, which supports configuration in one click.

Generation of one-time passwords always involves a secret, typically referred to as a seed. The benefit of the deployment methods SafeNet Authentication Manager offers is that the seed is generated on the device when users register, and the activation of the MobilePass software token is initiated at the backend server and activated over the air. As a result, this streamlines implementation, and eliminates the need to ship seeds via email or other channels that may be susceptible to loss or interception.

Conclusion

If security teams ignore the increased usage of smart phones in their organizations, they'll do so at their business' peril. However, while these mobile devices pose significant security risks, the reality is that they can be managed in a way that is secure, efficient, and effective. With SafeNet Authentication Manager, security teams gain the comprehensive capabilities they need to manage authentication across all end points and use cases, so businesses can leverage the opportunities of mobile computing, while mitigating the risks.

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