SOLUTION BRIEF

Next-Generation Authentication:

Walk the Security Tightrope without Losing Your Balance

Quick Look

A recent Gemalto IT security survey shows a clear trend toward the broader adoption of two-factor authentication and its implementation across a wider range of use cases. This trend reflects acknowledgement among IT professionals that secure access to enterprise and cloud resources is a top priority. The challenge for IT is balancing security necessities with the need to keep costs down, and making sure that users are not overburdened with inconvenient security routines.

The balance between employees' satisfaction and protection has always been a struggle for IT administrators. The new challenges that arise from mobility, using multiple endpoints and trends such as Bring Your Own Device (BYOD), have only clarified that implementing stronger access controls beyond the easily compromised static passwords is a necessity.

This solution brief will explore the current realities and challenges that IT administrators face in terms of the adoption of new technologies and trends. It will explain how the latest innovations in two-factor authentication can help enterprises successfully walk the security tightrope without losing the balance between security and user experience, and still come out ahead on cost.

Mobility, Multiple Endpoints, and BYOD

Today's workforce environment is characterized by the blurriness created between employees' personal and professional lives.

According to a survey published in SC Magazine in June 2013, the average person carries 2.9 devices. Indeed, employees walk around, on or off duty, with multiple devices that are either supplied by their employer or are their own. In parallel, organizations are increasingly taking advantage of SaaS delivery models, creating hybrid environments in which some applications are in the cloud, while others reside in the corporate data center. The transition to cloud-based applications is simplifying remote work and access, but is also creating greater security challenges.

> By year-end 2016, more than 30% of enterprises will use contextual authentication for workforce remote access
>
> Gartner User Authentication Magic Quadrant 2013

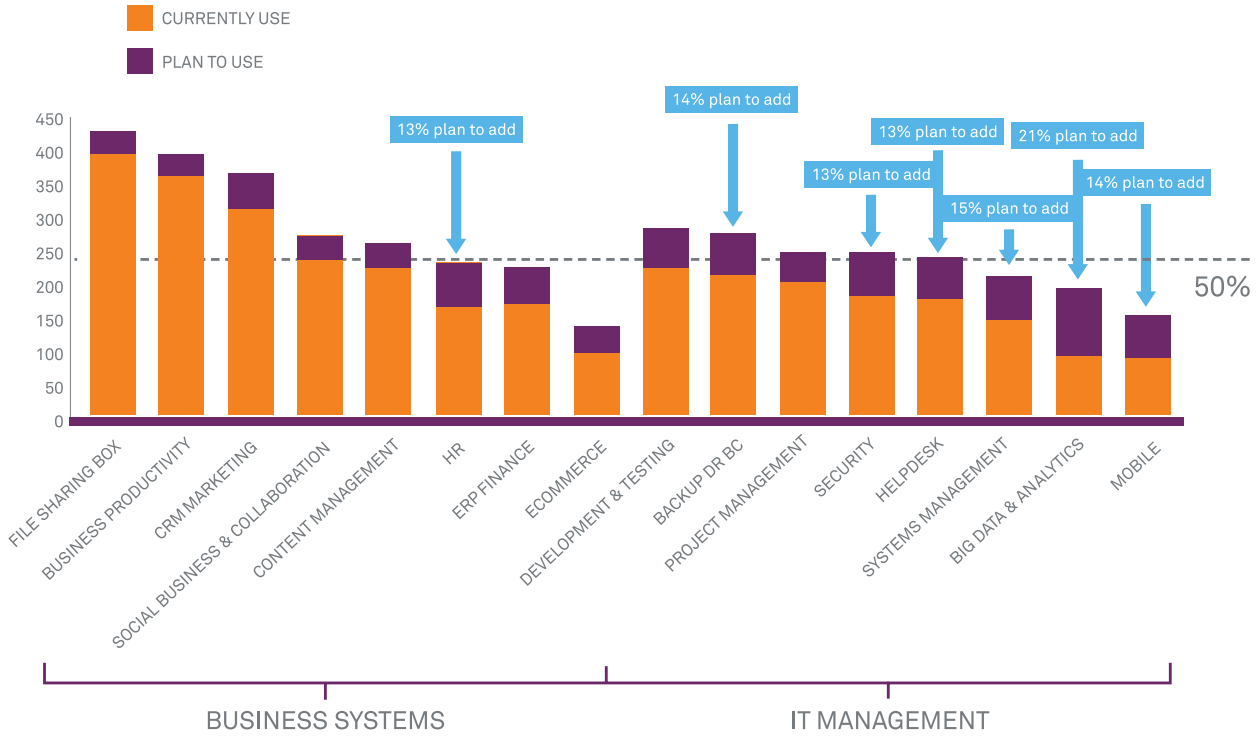
The need to enable secure access from multiple devices to multiple applications, whether they reside on premises or are hosted in the cloud, is an issue facing IT and security professionals.

Several factors come into play when addressing this issue:

- **Unified Access:** The need to implement unified access policies to SaaS applications, cloud-based solutions, and on-premises environments is essential in order to set and maintain secure access in current workforce environments, highly influenced by mobility.
- **User Satisfaction:** The desire to maintain acceptable levels of access security without burdening end users, combined with the need to support multiple devices, is leading organizations to adopt solutions that have minimal impact on the user experience.
- **Streamlined Management:** Under pressure to reduce costs and prove value, IT administration staff is on a constant quest to reduce their TCO. Streamlined management includes user management, provisioning, federated login, strong authentication, authorization, reporting, auditing, and policy alerts integrated with LDAP/Active Directory.

In the figure below, you can clearly see the adoption (and growth) of SaaS applications, covering all aspects of enterprise business and IT needs.

Lots of growth in SaaS application use to come



North Bridge Venture Partners and GigaOM Research, June 2013

Step Up Authentication, Step Down IT Costs

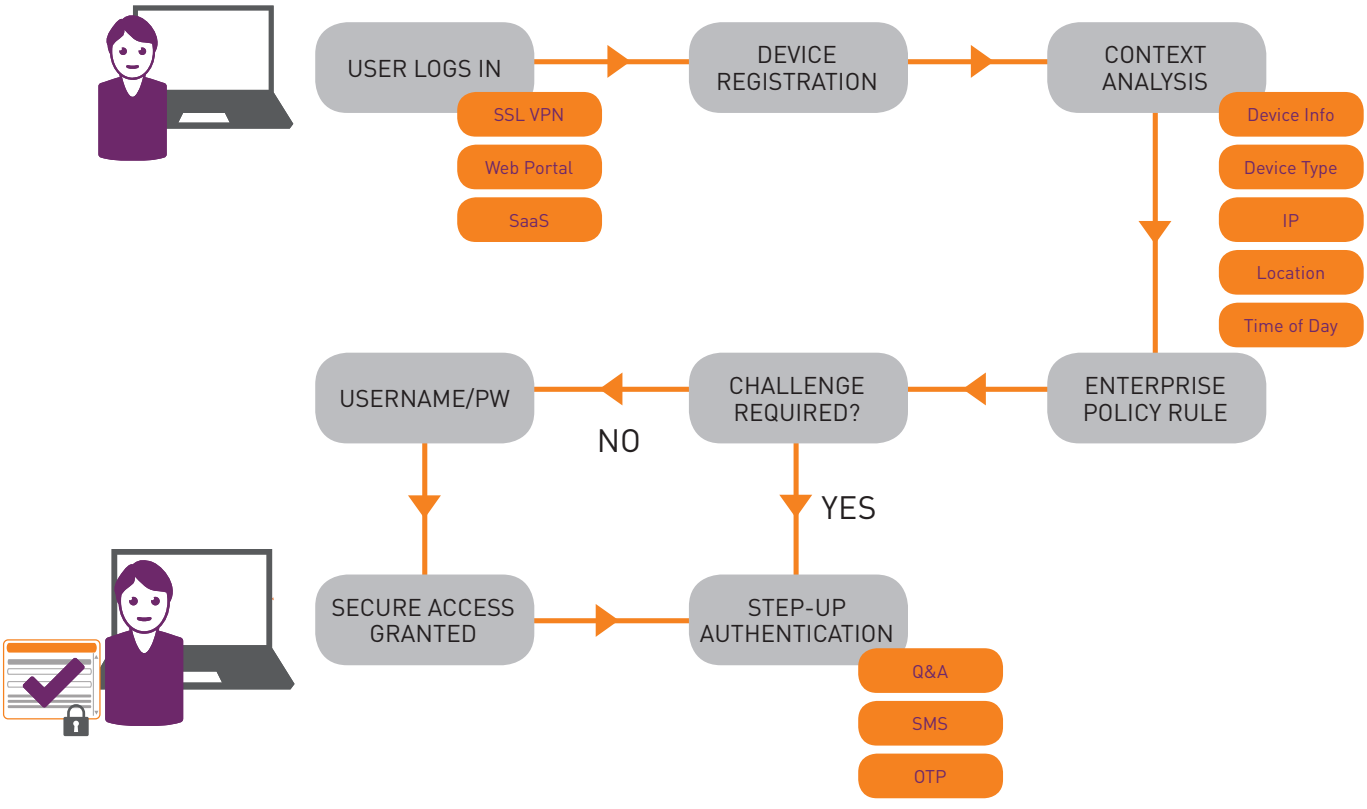
Gemalto's Next-Generation Authentication Solutions offer IT administrators a multi-layer approach to access control. Context-based secure access with "step-up" strong authentication allows organizations to achieve convenient, cost-effective secure remote access, while maintaining the flexibility and agility to add protection with stronger methods of security when required.

Employees can easily and securely access enterprise and SaaS applications, as long as they meet pre-defined policy rules set in advance by the administrator. If a user does not comply with the access rules in place, they might be requested to provide an additional authentication factor before they are granted access. This could be an SMS or a one-time passcode generated by a phone token, or a hardware token, depending on organizational policies.

Gemalto's Next-Generation Authentication leverages configurable policy rules to enable granular control over the level of authentication required each time a user logs on to an online resource. The context engine analyzes a user's logon attributes based on a set of configurable parameters—including geographical location, IP address, time of day, and device recognition—and generates a context assurance level. Each context assurance level requires a different level of authentication as administrators optimize security for any given logon instance.

Phone as a Token

Software tokens designed for smart phones generate a new password that can only be used once, each time a person logs into an account. An application is installed on the mobile device providing a viable alternative for organizations that do not want to rely on the availability of an SMS network for secure delivery of one-time passcodes. Gemalto smartphone tokens connect to Gemalto's existing management platforms, offering a phone-based "step-up" authentication method.



SMS Delivery

SMS delivery of one-time passwords is the fastest and easiest way to turn any mobile phone into a token. There is no software to install or hardware to distribute, significantly reducing the acquisition and operating costs of a strong authentication solution, and reducing the burden on users. Passcodes are sent to SMS-capable devices using either one of the pre-configured SMS service providers or by attaching an SMS modem/gateway to the Gemalto authentication platform.

Secure Access to Multiple Resources

Gemalto's Next-Generation Authentication addresses an organization's need to secure access to numerous resources, including cloud and SaaS applications, SSL VPNs, Web-based portals, local networks, and thin clients—with the broadest range of authentication methods, from tokenless solutions through SMS and one-time passwords. By implementing a single authentication platform for all authentication needs, organizations can implement unified authentication policies, cut TCO, reduce IT administration overhead, and improve convenience and usability for their users.

Streamlining Secure Access with Automated Management

Organizations are constantly looking to streamline administration costs. Gemalto's Next-Generation Authentication enables organizations to reduce the time, effort, and costs associated with deployment, maintenance, and support through automated processes and flexibility.

Gemalto authentication platforms secure unified access by automating everything, drastically reducing the time and cost of provisioning, administration, and management of users and tokens compared to traditional authentication models. Adding users, defining step-up policies, deploying new authenticators, adjusting form factors, and connecting risk levels with user requirements, are all tasks that are flexible, easy to manage, and transparent.

Benefits

- **Easy for users:** Unobtrusive and transparent for end users
- **Granular control:** Out-of-the-box or fully configurable policy rules give you visibility and control over risk levels and authentication methods
- **Comprehensive solution:** Part of a comprehensive strong authentication platform that supports the broadest range of authentication options and lets organizations address all secure access needs: VPNs, SaaS apps, Web portals
- **Lower TCO:** Reduces IT administration overhead, as well as token deployment costs and hassles related to client-side software installations
- **Device agnostic:** Offers secure access for mobile devices and standard desktop OS
- **Automated processes:** Reducing the time and cost of provisioning, administration, and management of users and tokens

About Gemalto's Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

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

GEMALTO.COM

gemalto
security to be free