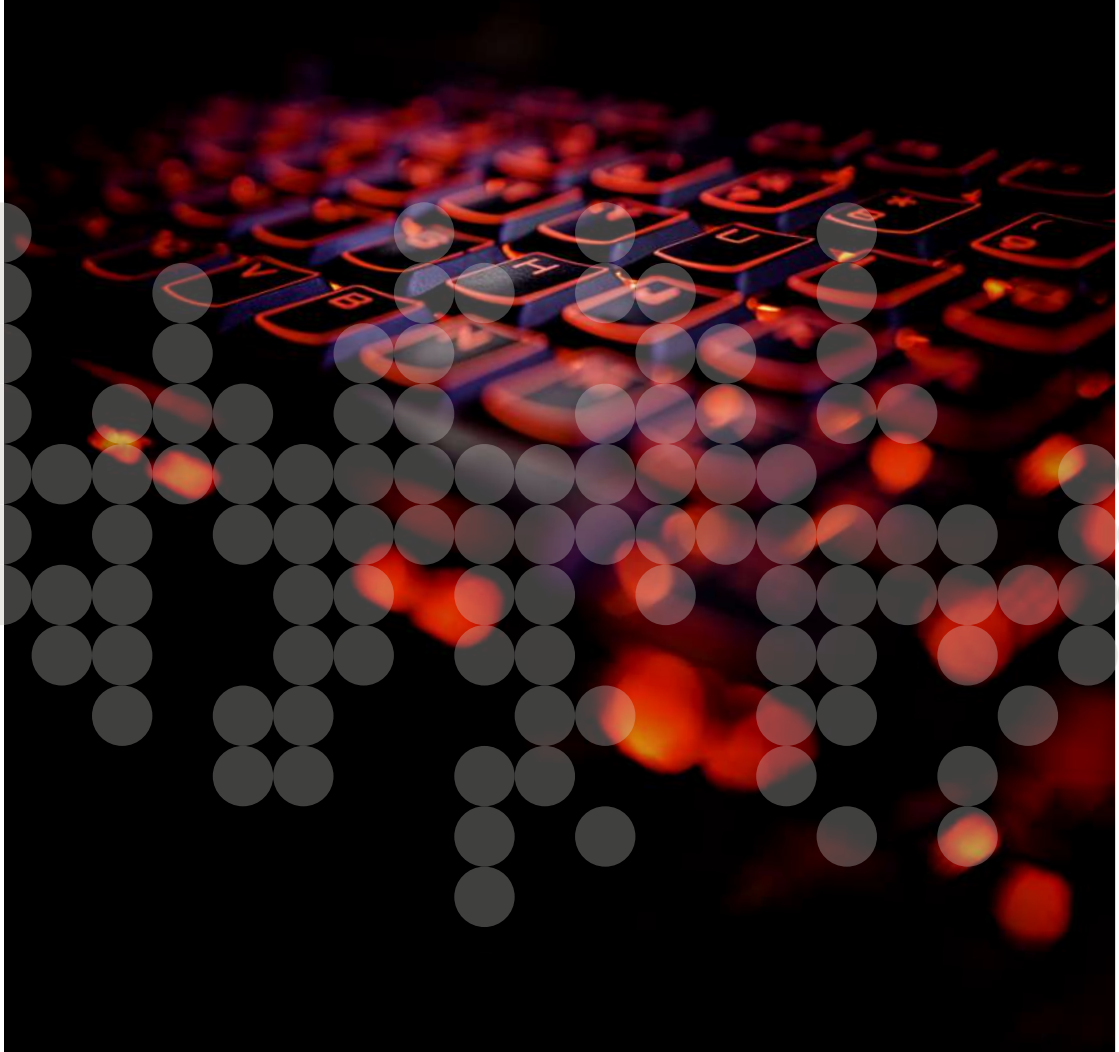
Security Report

The Perimeter: An Identity Crisis

Understand IAM and its challenges, and what it takes to implement a strong IAM solution



What's inside

Section 1: Rethinking identity and access management 3

Section 2: What is IAM? 6

How IAM works 7

Section 3: The challenges of managing identity and access 10

Distributed applications 11

Password problems 11

Bring your own device (BYOD) 12

Regulatory compliance 12

Section 4: IAM best practices 13

Single sign-on (SSO) and federated identity 14

Multifactor authentication (MFA) and adaptive access 14

Attribute exchange 15

Lifecycle management 15

Monitoring and visibility 16

Compliance 16

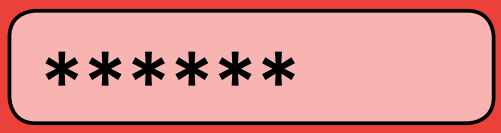
Section 5: Identity is the front line of defense 18

01

Rethinking identity and access management

Sixty-three percent of data breaches involve weak, default, or stolen passwords.[1]

Why? To put it simply, password fatigue. Think of all the passwords you keep track of for your personal needs—your mobile banking app, your Gmail, your Facebook account, your Amazon Prime… the list goes on. Best practices tell us that we should use a unique and complex password for every service, but due to increased cloud adoption—enabling anytime access to applications from any device—users lean toward convenient but risky password practices.



"123456," "password," and "qwerty" are among the most common passwords used, demonstrating password fatigue.[2]

80% of organizations employ a hybrid cloud architecture.[3]

Let's apply the phenomenon of rapid cloud adoption to the enterprise. Four out of five organizations employ a hybrid cloud architecture, and 20 percent plan on delivering more than half of their applications from the cloud by 2017.[4] For users, this means more passwords to create and remember. For IT, this means developing a plan that ensures secure authentication and appropriate access in a very complex app landscape. With an increasing number of accounts now residing outside the organization, there's less visibility, and let's not forget that users will likely use easy-to-recall passwords versus strong ones. Given this, the applications themselves become increasingly important to protect—in addition to the identities of the people who access them.

The phrase "applications are the new perimeter" may be tired, but it's not wrong. Fifty-eight percent of companies' sensitive data is stored in Microsoft Office documents, and nearly 80 percent of companies are using or plan to use Microsoft Office 365.[5] Office 365 may be a big one, but it's just one of many cloud-based applications where sensitive data resides. The proliferation of cloud-based apps didn't bring with it an easy and automatic solution to identity and access management (IAM) challenges. Management of identity and access across all applications has become too burdensome for users and IT.

We must rethink, re-invent, and re-architect our IAM strategies to ensure secure authentication for all apps, wherever they reside, and address the inherent risks associated with decentralized access controls and identity sprawl. The most important benefits of a complete IAM solution—including centralized management, single sign-on (SSO), reporting, and risk-based application of security policies—can help you empower your employees and partners to deliver real business value while minimizing risk to your organization.

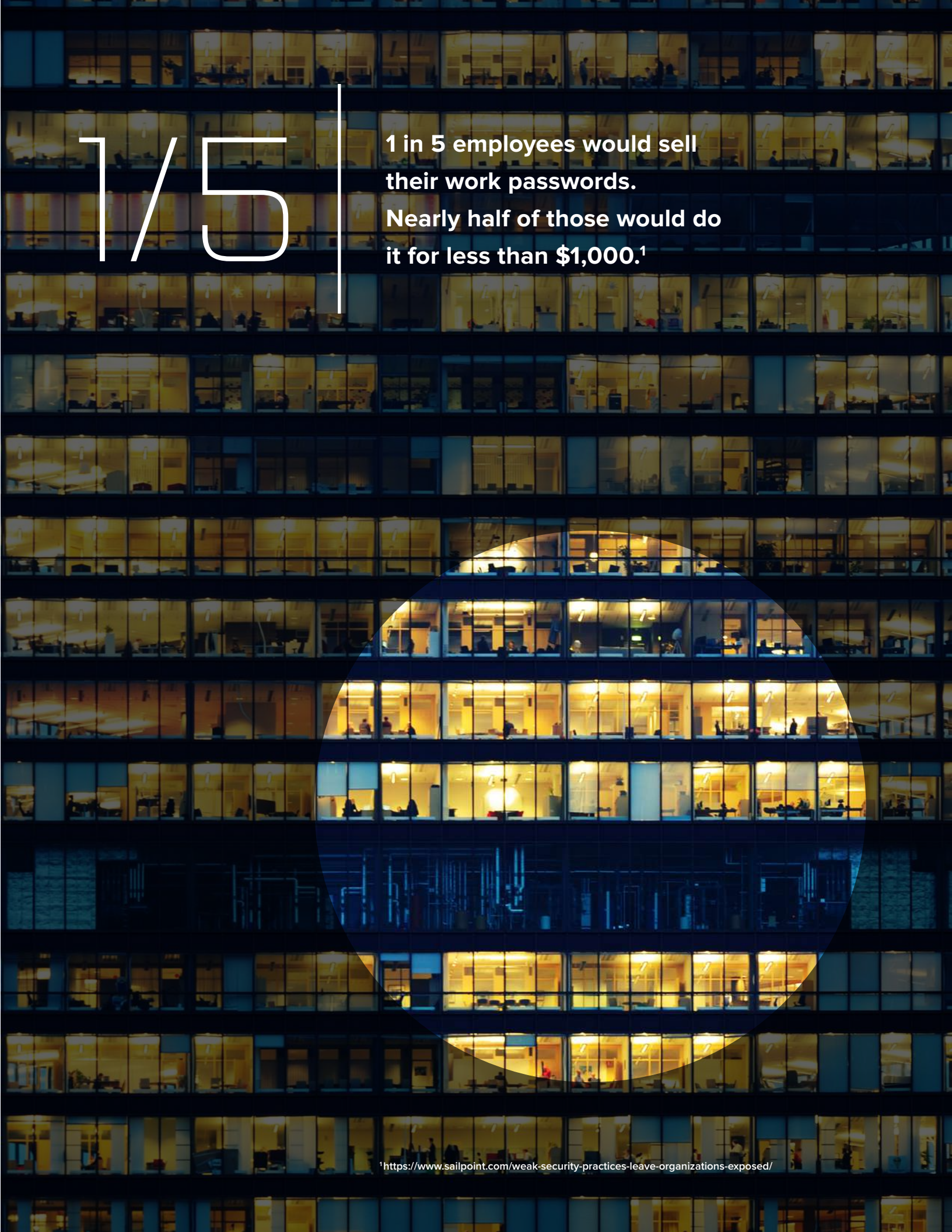
[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[2] http://www.telegraph.co.uk/technology/2016/01/26/most-common-passwords-revealed---and-theyre-ridiculously-easy-to/

[3] https://f5.com/about-us/news/the-state-of-application-delivery

[4] https://f5.com/about-us/news/the-state-of-application-delivery

[5] https://www.skyhighnetworks.com/cloud-security-blog/7-charts-reveal-the-meteoric-rise-of-office-365/



1/5

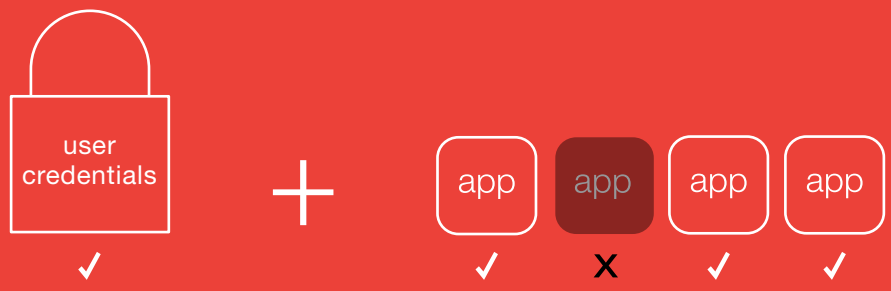
1 in 5 employees would sell their work passwords. Nearly half of those would do it for less than $1,000.[1]

[1] https://www.sailpoint.com/weak-security-practices-leave-organizations-exposed/

02

What is IAM?

Identity management (authentication) and access control (authorization) are two sides of the same coin. At the most basic level, identity and access management (IAM) is about verifying a user's identity and granting/denying access.



AUTHENTICATION **AUTHORIZATION**

In any organization, a specific user may have multiple identities for various corporate resources and web applications. Add to that the many devices and locations users connect from, and it is evident that many organizations are dealing with a different sort of identity crisis.

Identity management involves keeping that user's identity information consistent among all his or her different roles. In addition, an IAM solution ensures that each user has the right amount of access to various applications, which can be hosted on-premises, in a private or public cloud, or delivered via a SaaS provider.

How IAM works

The two general components of IAM are authentication—proving you are who you say you are— and authorization—granting permissions. Traditional IAM systems were housed in an on-premises server room and physically controlled by IT staff to manage applications hosted in the same data center. In that model, all the decisions about authentication and authorization were made in-house. While this solution has the benefit of simplicity, it's just not applicable to most enterprises today, which are hosting more and more applications in the cloud or relying upon SaaS providers.

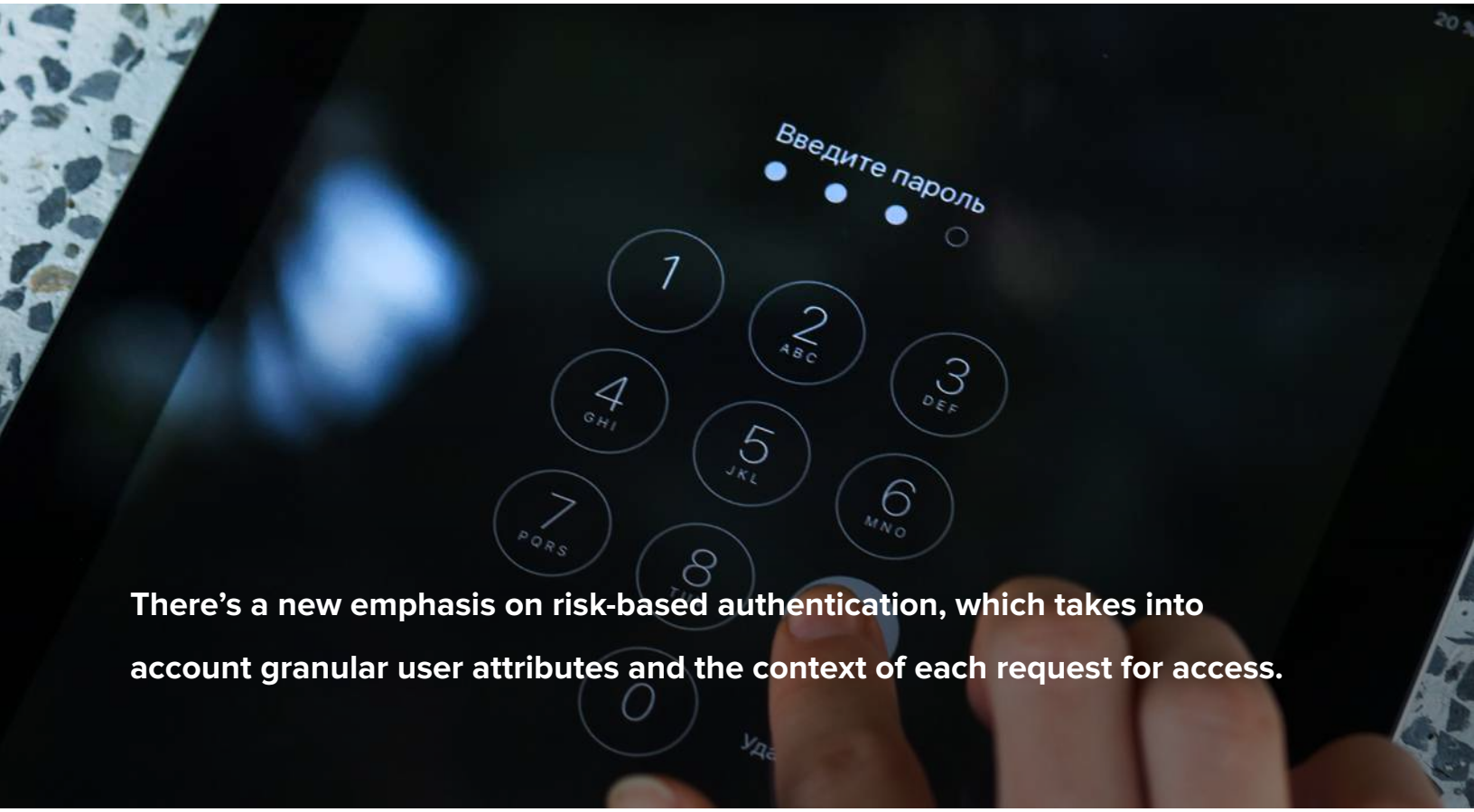
A modern IAM solution must meet the needs of a hybrid cloud environment and validate a user's identity, then map each access request to a specific policy to decide whether the user can access the requested resource. To do this, the IAM solution relies on several sub-components of authentication and authorization. Note that the location of each sub-component may differ based on your deployment architecture.

- **Authoritative source** Every organization must have a so-called "source of truth" to ensure the integrity—and consistency—of identity information across different systems. Basically, the authoritative source answers the question "Who are you?" for each user within the system. Typically, the corporate authoritative source is the Human Resource Information System (HRIS), which stores all the details about each user. Those without an HRIS may use Microsoft Active Directory or LDAP, dictated by HR and controlled by IT.

- **Identity provider** An identity provider (IdP), such as Microsoft Active Directory, an LDAP server, or an Identity as a Service (IDaaS) cloud provider, pulls information from the authoritative source to communicate with a relying party (see below) to grant or deny access.

- **Attribute provider** An attribute provider (AP) functions similarly to an IdP. However, instead of relying upon user-provided passwords, the AP employs user attributes such as phone numbers, credit card numbers, or birthdates to identify the user.

- **Relying party** The relying party is typically an application that validates information provided by an IdP or an AP and then uses them to validate identity and provide access to a specific application or system.



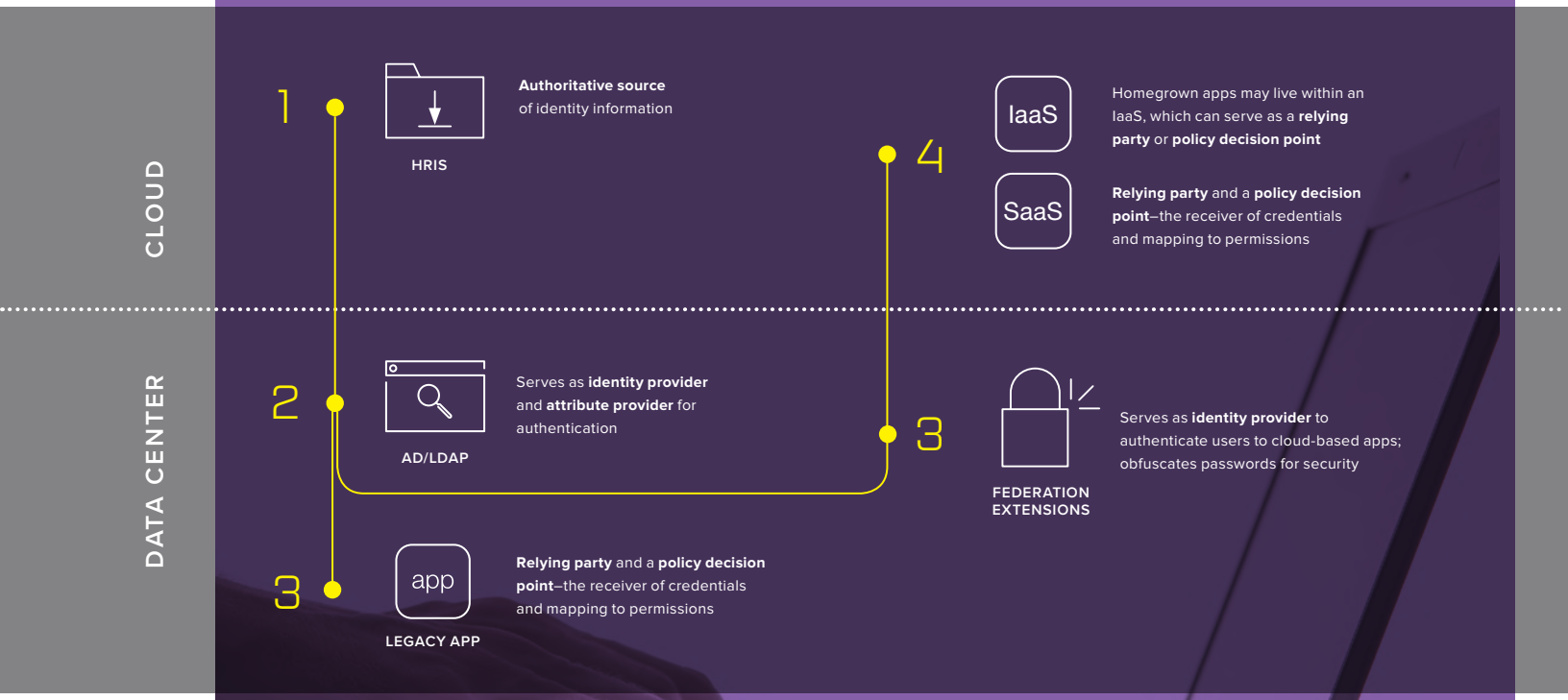
There's a new emphasis on risk-based authentication, which takes into account granular user attributes and the context of each request for access.

- **Policy decision point** In a well-defined IAM system, each access request is mapped to a specific policy by a policy decision point (PDP), which determines whether a user will be granted access to the requested application or system. The PDP uses information from the IdP and the attribute provider to map users to the appropriate policy.

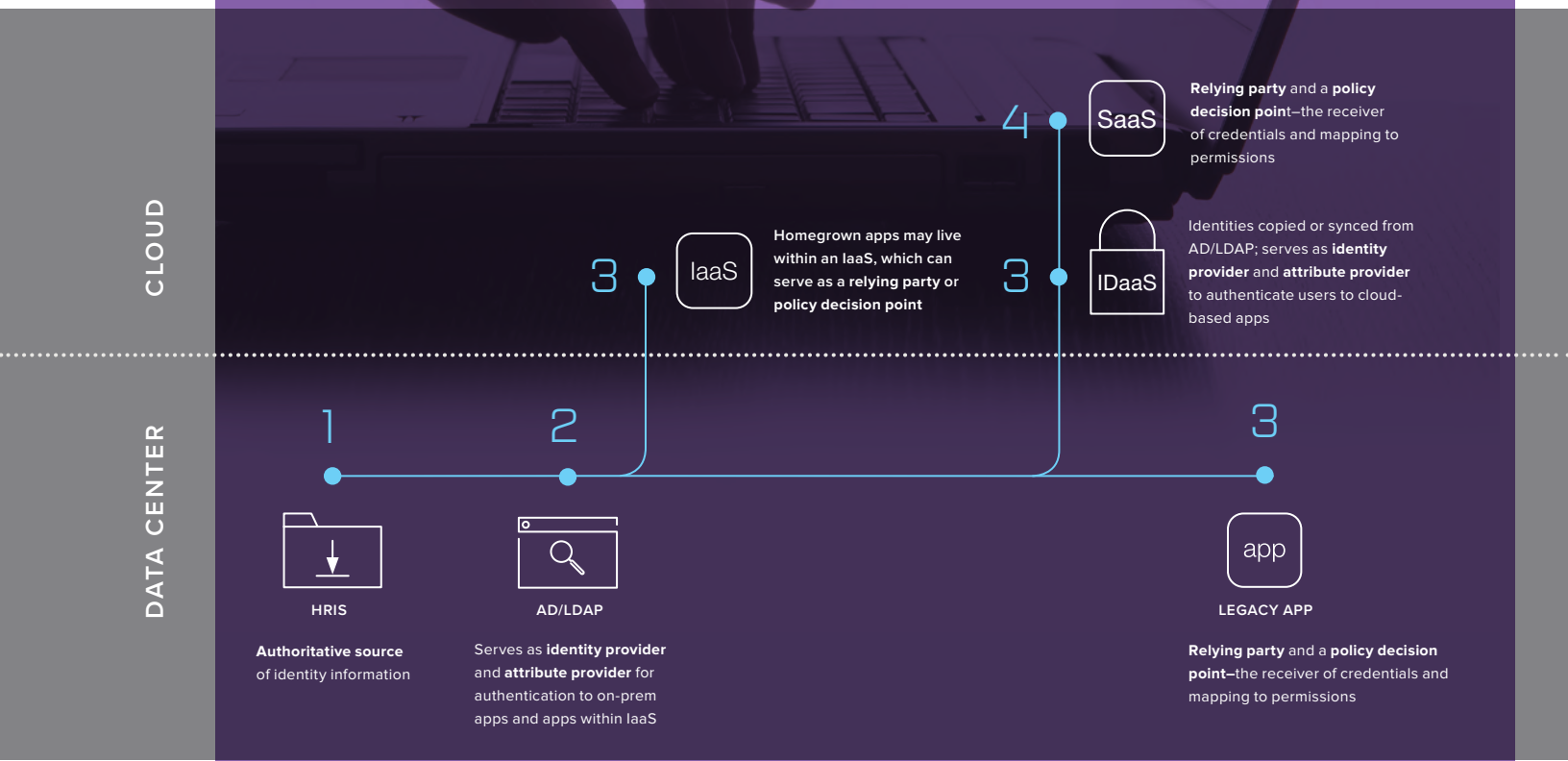
Regardless of the architecture, enterprise IT must keep all user identities both consistent and distinct—as well as manage the evolving levels of application access required for each user to work productively. With the application as the new perimeter, IAM becomes a bigger focus for security risk management. There's a new emphasis on risk-based authentication, which takes into account granular user attributes and the context of each request for access. The end goal remains giving the right users secure access to all applications (mobile, VDI, web, SaaS, and traditional client-server) from any network and on any device—and to do it simply and quickly while protecting corporate resources from unauthorized access. It's a big task, and the challenges are complex.

Nearly 80 percent of companies use cloud vendors as well as hosting apps on-premises. IAM architectures vary greatly; these are two high-level examples of what those architectures could look like.

EXAMPLE A



EXAMPLE B



03

The challenges of managing identity and access

The proliferation of cloud applications and mobile devices has helped enterprises gain many efficiencies; however, those without a complete IAM solution take on additional security and compliance risks.

Over a quarter of companies surveyed cite the inability to have consistent security policies across multiple environments as a top security challenge.[1]

[1] https://f5.com/about-us/news/the-state-of-application-delivery

The growth of mobile computing means that IT teams have less visibility into and control over employees' work practices. Leveraging a remote workforce allows businesses to boost productivity while keeping expenses in check—as well as untethering employees from a traditional office setting.

However, with employees scattered all over the country or even the world, enterprise IT teams face a much more daunting challenge: maintaining an available, consistent experience for employees connecting to corporate resources without sacrificing security.

Distributed applications

Your applications have gone mobile. Gone are the days of all your enterprise apps living safely within the cozy confines of the corporate data center. The increase of SaaS applications such as Salesforce and Office 365, as well as the trend of moving in-house developed apps to Amazon Web Services (AWS) or other Infrastructure as a Service (IaaS) providers while leaving some apps on-premises, escalates the complexity of managing user identities and access for all applications.

The decentralization of applications and identities has created additional overhead in the lifecycle of user IDs. IT staff must provision access manually or through disconnected IAM solutions. The longer it takes for a user to gain access to crucial business applications, the less productive that user will be. On the flip side, failing to revoke the access rights of users or third parties who have left the organization or transferred to different departments can have serious security consequences. Manual provisioning and de-provisioning of access is labor-intensive and prone to human error or oversight. Especially for large organizations, it is not an efficient or sustainable way to manage user identities and access.

To ease some IAM frustrations, federated identity solutions such as Active Directory Federated Services (ADFS) are used to allow on-premises user authentication and token-based login for SaaS applications. However, the total cost of ownership of ADFS can be expensive, and using it can be time-consuming due to the number of servers and the load balancing it requires to scale. Additionally, ADFS doesn't help mitigate the risks of the mobile workforce, as it cannot perform health checks on the devices connecting to your applications.

Without a consistent and seamless way to access these applications, users have a bad experience and IT is faced with rising support costs from frustrated users, not to mention a potential security nightmare.

Password problems

The growth of cloud-based applications means that employees have been trained to enter their passwords all over the place. Add to this an increasing number of passwords for applications that may have differing complexity requirements, and the challenges multiply. And, because only a small percentage of users employ

password managers, frustration can mount when an employee spends more and more time managing the resulting lists of passwords—which, for some applications, may require changing every 30 days.

This password fatigue pushes users into bad management practices including using simple, easily stolen passwords such as “123456” or “password,” writing passwords down, or, arguably worse, re-using passwords. The increase in username and password compromises included in data breaches (e.g., LinkedIn, Yahoo!) has spotlighted the security risk that password re-use creates. For browser-based applications, many users have their browsers save passwords, which are at risk of being scraped by malware. When one set of stolen credentials can give an attacker or phisher access to multiple apps, the perils of poor password management can keep IT teams up at night.

Bring your own device (BYOD)

Users want to connect to their applications whenever it is convenient, from wherever they are, and from whatever device they want. Employees, contractors, partners, and others bring in personal devices and connect to the corporate network for professional and personal reasons.

The challenge with BYOD is not whether outside devices can access the network, but whether IT can react quickly enough to reduce the risk of malware infecting the network from a corporate or personal mobile device—without disrupting employee productivity and while offering freedom of choice. Nearly every company has some sort of policy that ensures devices connect securely and adhere to a security posture baseline, regardless of ownership. However, accessing internal and SaaS applications on a mobile device can be more cumbersome for users than doing so from a networked laptop or desktop workstation. In addition, IT staff may struggle to manage who has access privileges to corporate data and which devices they’re using to access it.

Regulatory compliance

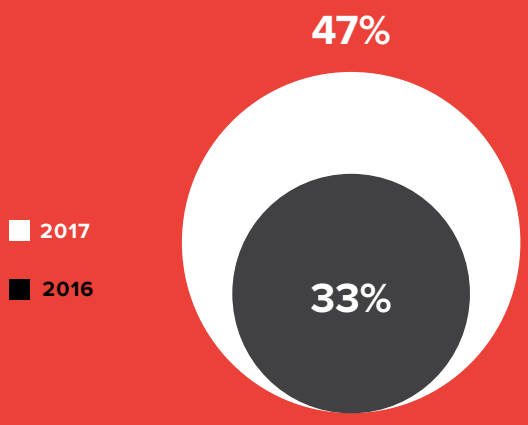
Compliance and corporate governance concerns continue to be major drivers of IAM spending. For example, much of the onus to provide the corporate governance data required by Sarbanes-Oxley regulations falls on IT departments. Ensuring support for processes such as determining access privileges for specific employees, tracking management approvals for expanded access, and documenting who has accessed what applications and data and when they accessed them can go a long way to easing the burden of regulatory compliance and ensuring a smooth audit process.

04

IAM best practices

IT has traditionally not given much attention to IAM, as it has long been dominated by Active Directory or LDAP, and on-premises LDAP-compliant applications.

Over the past few years, though, we have seen a proliferation of new IAM vendors offering solutions aimed at helping organizations reposition their IAM strategy given the current realities of the cloud and the new security perimeter.



"Cloud first" strategies jumped to 47% in 2017, with more organizations evaluating cloud-based IT solutions before making new IT investments.[1]

[1] https://f5.com/about-us/news/the-state-of-application-delivery

To keep employees productive and the business secure, your IAM solution needs to offer fast and secure connections to maximize productivity, and seamless integration to minimize cost and optimize user experience. You must also ensure that your IAM solution can scale with your business growth and the explosion of devices taxing the corporate network. A holistic IAM strategy can help administrators consolidate, control, and simplify access privileges, whether the critical applications are hosted in traditional data centers, private clouds, public clouds, or a hybrid combination of these spaces. In this section, we'll examine the key components of a strong IAM solution.

Single sign-on (SSO) and federated identity

As the part of your IAM strategy that affects every user, SSO is the most visible—and most important—component of any IAM solution. If it's not implemented well, users may be more inclined to initiate "Shadow IT" projects that can affect the integrity of your identities and ultimately the confidentiality and integrity of the data within your applications. However, if your user experience is smooth, application owners will be far more likely to fall in line with corporate policy.

With a solid SSO strategy, you can readily make password fatigue issues a thing of the past by federating user identity and extending secure SSO capabilities to SaaS, cloud-based, web-based, and virtual applications. In addition, identity federation and SSO can integrate password management across multiple domains and various authentication and attribute-sharing standards and protocols.

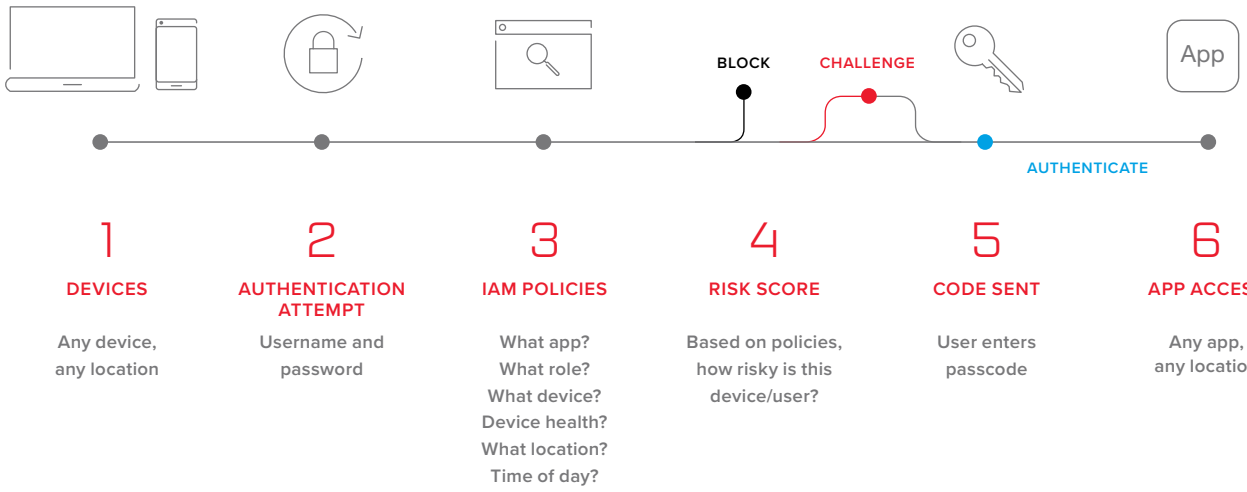
SSO and identity federation can also dramatically reduce OpEx and IT labor costs while increasing the productivity of your users. By providing seamless access to all corporate resources and instantly provisioning and de-provisioning access to cloud applications, identity federation and SSO enhance the user experience while enabling your organization to more easily stay compliant with your access-related security controls.

Multifactor authentication (MFA) and adaptive access

While identity federation and SSO may offer the most benefits to your users, they alone cannot provide the risk-based security an organization requires. To avoid the perils of phishers gaining unfettered access simply by stealing a username and password, configure MFA for extra security. MFA consists of something you know (password), and something you have (token), or even something that you are (biometrics). By requiring users to enter a unique code from an authentication service or device or to provide a fingerprint scan, MFA helps ensure that only approved users have access your applications or network resources.

Adaptive access adds an extra layer of security by evaluating user data from multiple sources to analyze the risk associated with the attempted login.

Strong IAM solutions streamline access and secure apps



This data can include the user's role, the health of the device attempting to connect to your application, location of the user, time of day, and others, as well as combinations of these factors. If your system detects an anomaly, it can respond to the user access request with a demand for additional authentication criteria, typically referred to as step-up authentication.

Attribute exchange

Authorization, based on role alone, is no longer good enough. Enterprises must implement a strategy that makes it quick, easy, and secure to sync relevant data points (e.g., department code, employee ID, employee name, etc.) with an application to determine which access policies apply. Your IAM solution should provide a way to perform granular authorization or attribute exchange. This is essential because you don't want all your users having access to unnecessary functions within an application simply because they can authenticate. However, this is difficult to implement in many SaaS applications since the policy decision point is controlled by the SaaS provider.

Lifecycle management

A robust IAM solution can automate the user provisioning and de-provisioning process, giving IT full power to create, update, and delete the access rights of employees, partners, contractors, vendors, and guests.

Automated provisioning and de-provisioning speed the enforcement of strong security policies while helping to eliminate human error. It's also important to make sure you have an automated audit process to help with compliance-related access controls.

Monitoring and visibility

A well-functioning IAM strategy must consider the reality of users who start their own Shadow IT projects. More and more users are taking it upon themselves to spin up virtual machines and access cloud resources without going through the appropriate corporate procurement channels. This allows agile DevOps teams to respond to the needs of the business for ever-faster release cycles—but it can create havoc within your IAM system.

Rogue applications provisioned on the fly can introduce new security vulnerabilities and cost you control over your confidential data. It's important to write policy to restrict which users can spin up resources and under what circumstances. Policy alone won't completely protect your network from Shadow IT, but it's a good first step. If you're continuing to experience difficulties, other options include using a managed service that monitors differences in spend, which can point to the use of unauthorized resources.

Another option is to monitor activity on an internal application-aware firewall, although that will only show you the application activity of users connected to the corporate network.

Compliance

A strong IAM solution can support compliance with regulatory standards such as Sarbanes-Oxley, HIPAA, and the Payment Card Industry Data Security Standard (PCI DSS). In particular, a solution that automates audit reporting simplifies the processes for regulatory conformance and can also help generate the comprehensive reports needed to prove that your systems are in compliance with regulations.

Now is the time to build your centralized IAM team that can architect and enforce organization-wide identity and access management policies.

05

Identity is the front line of defense

It's time for enterprises to rethink their IAM systems.

With your applications as the constantly shifting security perimeter of your organization, managing identity and ensuring appropriate access are an essential part of your overall security strategy. As your employees and their devices become the main targets of attacks that can disrupt or even destroy your business, your IAM system must be a stout front line of defense.

90% of today's security budgets are still spent on protecting everything but user identities and applications.[1]

[1] F5 marketing sizing estimates aggregated from global research firms.

Enterprises searching for IAM solutions must consider the realities of an increasingly mobile workforce and a highly distributed and complex network of applications. A robust IAM solution can ease management pains, streamline provisioning and de-provisioning, boost user productivity, and secure your applications and data—all while lowering costs, reducing demands on IT, and providing the enterprise with comprehensive data to assist in complying with regulatory standards.

Furthermore, as identity and access management becomes increasingly complex, the ability to create policies based on granular, contextual information will become more and more important. IAM solutions that can collect and make decisions based on user identity, user location, device type, device health, time of day, requested resource, and more will allow enterprises to deliver quick access to bona fide employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users.

While the benefits of deploying a robust IAM solution are clear, the expense and complexity of implementation can derail even the most well-intentioned organization. However, when you consider the cost of a potential security breach, analyze your rising cyber security insurance premiums, and study the inefficiencies inherent to the manual provisioning and de-provisioning of access to corporate resources, the imperative is clear: Now is the time to build a centralized IAM team that can architect and enforce organization-wide identity and access management policies.

More information

To learn more, visit **f5.com/iam**.

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. DC0217
RPRT-SEC-126013647