STACK ANALYSIS

Modernizing Identity Management

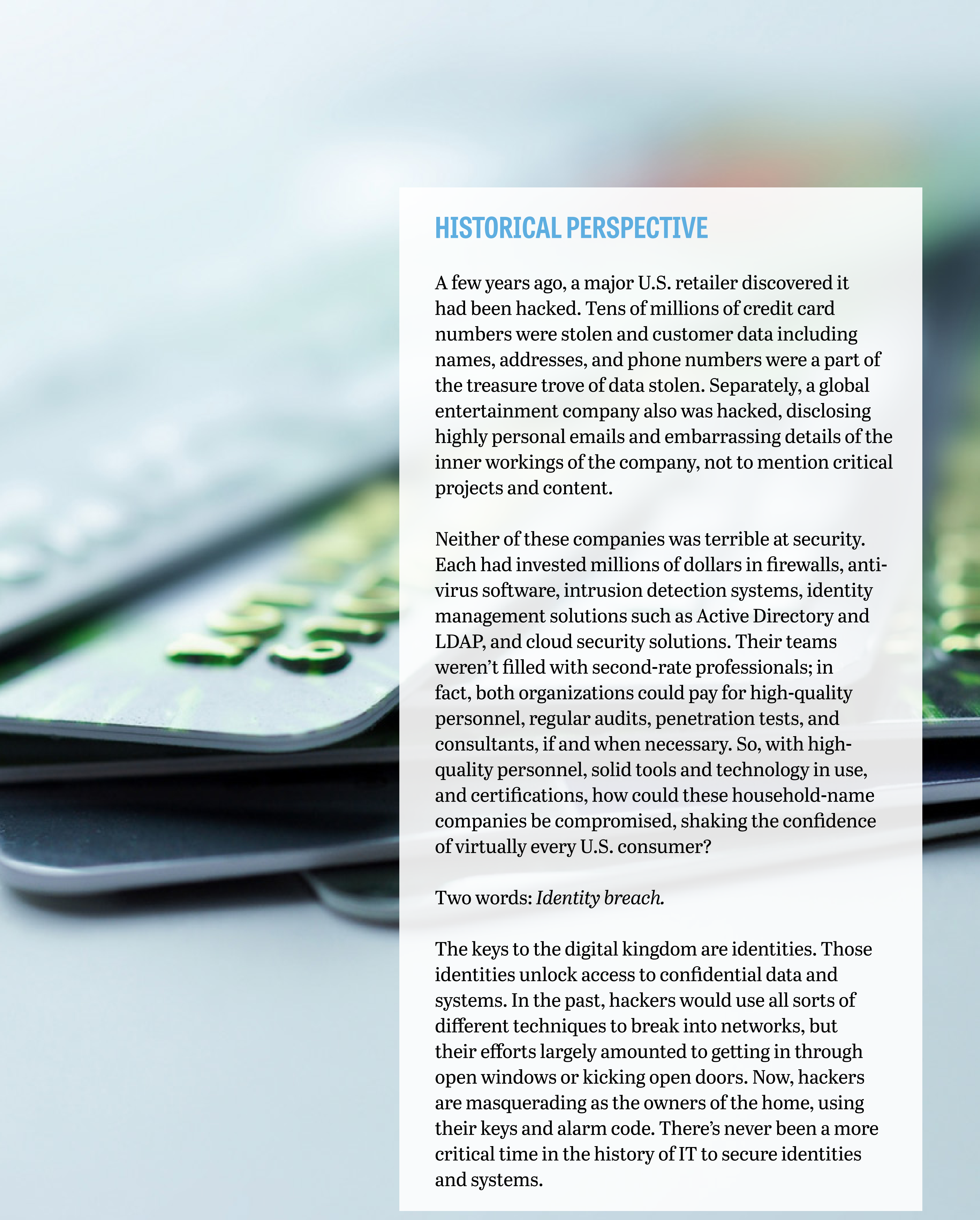
EXECUTIVE SUMMARY

There is no shortage of examples of major corporate security breaches due to a lack of identity security. Identities have become the keys to the digital kingdom and are the fastest way in for bad actors.

Today, the infrastructure of IT organizations is more critical than ever, with virtually all companies relying on them to do business. Unfortunately, the historical approach to controlling access to IT environments has hardly evolved in the last 20 years, despite massive changes to the IT network.

Organizations are still leveraging Microsoft Active Directory (AD), a solution that was introduced in 1999. Yet, even with the significant changes in networks, IT admins have leveraged add-on solutions built on top of AD to solve their identity and access management (IAM) challenges.

Innovative IT leaders are realizing that a new approach to identity management is needed that provides deeper control, increased efficiency, and better security. A new generation of cloud identity management solutions is emerging to provide IT leaders with a neutral, SaaS-based approach to core directory services for the modern era of IT.



HISTORICAL PERSPECTIVE

A few years ago, a major U.S. retailer discovered it had been hacked. Tens of millions of credit card numbers were stolen and customer data including names, addresses, and phone numbers were a part of the treasure trove of data stolen. Separately, a global entertainment company also was hacked, disclosing highly personal emails and embarrassing details of the inner workings of the company, not to mention critical projects and content.

Neither of these companies was terrible at security. Each had invested millions of dollars in firewalls, anti-virus software, intrusion detection systems, identity management solutions such as Active Directory and LDAP, and cloud security solutions. Their teams weren't filled with second-rate professionals; in fact, both organizations could pay for high-quality personnel, regular audits, penetration tests, and consultants, if and when necessary. So, with high-quality personnel, solid tools and technology in use, and certifications, how could these household-name companies be compromised, shaking the confidence of virtually every U.S. consumer?

Two words: *Identity breach.*

The keys to the digital kingdom are identities. Those identities unlock access to confidential data and systems. In the past, hackers would use all sorts of different techniques to break into networks, but their efforts largely amounted to getting in through open windows or kicking open doors. Now, hackers are masquerading as the owners of the home, using their keys and alarm code. There's never been a more critical time in the history of IT to secure identities and systems.

CURRENT STATE OF IT & IDENTITY

The security risks for organizations have shifted. Digital assets are more critical than ever—and arguably far more important than physical goods. The IT landscape is more chaotic and frenetic than ever; there are more security breaches occurring every day than anytime before. Billions of dollars are lost annually to cybercriminals.

While a few of these are sophisticated, new approaches to compromising organizations, the vast majority of these security compromises are straightforward in prevention. The challenge for IT organizations is knowing how to put these prevention systems and processes in place while juggling the intense needs of the business.

IT is no longer a cost center or afterthought for an organization. IT organizations and infrastructure correlate directly with driving revenue and saving costs. IT historically has been thought of as the department employees would call to fix their computer when it broke; today, however, IT organizations are enabling employees with cloud infrastructure, SaaS applications, virtual data storage, and much more. Users are pushing IT organizations by leveraging their own computers, mobile devices, social media services, and more as part of their business.

In this fast-evolving market, how do IT admins control and secure their confidential data, keep their users safe online (and, by extension, their organization), and be efficient enough to be able to focus on IT projects that drive more revenue and profit?

CRITICAL REQUIREMENTS FOR IT LEADERSHIP

IT leaders increasingly are pushing for modern, open approaches to building their IT infrastructure. The traditional on-prem, Microsoft-centric network is largely an artifact of the past. Forward-leaning IT admins and organizations are pulling out all of the stops with infrastructure-as-a-service (IaaS) solutions; web applications; mixed-platform environments; mobile solutions; data and files that are available anywhere, anytime, through any device; and a work-from-anywhere-with-anything mentality. IT organizations are focused on making it frictionless for employees to work in whatever way is best for them.

In this new era of modern IT, heterogeneous environments add significant issues of control, security, and efficiency.

- **Control** – Traditionally, IT was able to manage everything within an organization. All IT purchases ran through the IT group; hardware and software were located onsite; and IT was responsible for the upkeep of all the systems and processes. Even if a solution was being delivered for another group within the organization, IT was responsible for its uptime and operation.

  With the democratization of IT, every employee or contractor within a company is now a purchaser of IT solutions. There are SaaS applications for literally every job profile and group within an organization. For IT, the scary part is that these solutions don't need IT to be purchased and implemented. That means that confidential data and login IDs are floating around the internet without IT being aware of them.

- **Security** – IT organizations are fighting the constant attacks on their IT networks and users. For many of those threats, the IT department is helpless. With every employee heavily leveraging IT tools and technology, IT admins are dependent upon users to protect themselves and company assets. Although the technology literacy of today's workforce is increasing quickly, attacks are becoming more sophisticated, requiring more knowledge, and prevention from users.

  Perhaps the No. 1 challenge facing IT organizations is the theft of user credentials. The right credentials can cause irreparable harm to an organization if stolen. There are countless examples of an executive's identity being stolen and used to access highly confidential information. With the proliferation of IT solutions and internal data, this risk is difficult to quantify and even more difficult to manage.

- **Efficiency** – IT infrastructure is meant to enable scaling, productivity, and efficiency. With the proliferation of IT solutions, workers are indeed more productive, but there also is more friction. There isn't one place for employees to access everything they need.

  For IT admins, it is even worse. They are on the hook to connect their employees to all of these different types of solutions. Even more, they are often called upon to help manage and troubleshoot this wide array of hardware and software. The context-switching alone can be mind-numbing for IT personnel. Modern IT should drive more efficiency than it does, but the wide range of solutions and approaches negatively impacts that efficiency.

There are no easy answers for forward-thinking businesses. These challenges need to be met head-on with solutions that span people, processes, and technology.

IMPACT OF IT CHALLENGES

At the core of solving these significant IT problems is securing and managing user access. In a heterogeneous environment and with identity security so critical, IT organizations need to step back and assess how they will secure and control their user identities.

As discussed above, a lapse in identity security could put the organization in a catastrophic state. In today's modern era of IT, there may not be a more important subsystem for IT organizations to manage than their identity management infrastructure. IAM is at the core and the foundation of how employees access information—and more importantly, what information they are allowed to access.

Many IT organizations and senior management assume that this problem has been solved. And, for many existing organizations, it was solved. But it's not anymore. IT organizations need to take a hard look in the mirror and assess their true state. Are all IT resources connected to a central identity provider that controls access? Are all user identities in one central, secure system, or are identities strewn across the enterprise within multiple systems? How are non-traditional platforms and approaches handled? Are cloud, web, and mobile as easily managed as on-prem?

LEGACY SOLUTIONS BUILT FOR A DIFFERENT ERA

For almost 20 years, IT organizations have been leveraging a core identity management solution from Microsoft called Active Directory. In the era of Windows-based desktops, laptops, servers, and applications, AD was the ideal solution. IT admins could centrally control user access as well as Windows devices to increase security. Of course, there were fewer variables involved in securing a network as there are now. AD delivered on the concept of single sign-on without even a focus on it. Users could access whatever they had rights to if it was Windows-based. This was largely frictionless for users and an easy management approach from IT's perspective.

With the advent of web applications, IT organizations needed to alter their approach and added the concept of a web application single sign-on solution into the mix. These solutions would leverage Active Directory identities and extend a user's access to web applications. This added overhead to IT, but it solved a significant need for IT organizations and their users.

The challenges started to compound as IT environments continued to morph with new device platforms, cloud infrastructure, different file storage options, the shift to WiFi and café-style networks, and, of course, more mobile users. All of these changes put pressure on the core approach to identity management. Even worse, hackers knew that the fastest way to confidential data was a person's digital identity and now those identities were all over the internet—and potentially more easily accessible.

For many organizations, the traditional approach with Microsoft Active Directory at the core was starting to look dated and a new, more modern approach was sought.

TODAY'S SOLUTIONS FOR CURRENT AND FUTURE PROBLEMS

This more modern, cloud-forward approach to solving fundamental IT problems is called cloud identity management. Unlike most cloudwashed solutions, simply moving Active Directory to the cloud wasn't going to work in an IT landscape that has changed dramatically since AD was introduced almost 20 years ago.

The concept of cloud identity management centers around some core principles:

Cloud delivery

Location and provider independent

Multi-protocol central authentication

Heterogeneous systems management

Single identity, multiple forms

Bulletproof identity security

In short, a new wave of cloud identity management solutions are shaking up the traditional IAM industry. No longer is the path predetermined to be Microsoft-based; rather, IT organizations are deeply analyzing their needs to centralize and control user access to their wide range and types of IT resources.

Cloud identity management platforms are multi-platform, vendor-neutral, mixed protocol, and location-agnostic. As a result, IT organizations can pick the right IT solutions for their organization rather than being tied to a particular vendor's solutions, as they have in the past.

MODERN SOLUTIONS RISE TO THE CHALLENGE

IT leaders are demanding cloud identity management solutions that meet many of the criteria above. At their core, modern approaches to solving the identity management needs include:

- **SaaS delivery** - IT organizations largely do not want solutions on-prem anymore. With the transformational shift to the cloud, SaaS-delivered solutions are a more attractive option. SaaS provides IT organizations with greater flexibility, less cost, and quicker time to value with less implementation effort.
- **Cross-platform support** - IT leaders do not want to be tied to particular vendors, so an identity management platform needs to enable users connecting with a wide range of solutions from different vendors.
- **Embedded security** - Identity breaches are one of the most significant risks for an IT leader, so cloud identity management simply needs to step up security in a way that on-prem solutions can't.

The cloud identity management space can be quite vast, and there are a number of different players providing these benefits to IT organizations in a variety of areas. In the web application single sign-on space, Google, Microsoft, and Amazon all provide cloud-hosted solutions. For app developers, cloud authentication services can be found from players including Okta, Auth0, and Microsoft's Azure Active Directory B2C. In the directory services space, major players include Microsoft Active Directory/Azure AD and JumpCloud's Directory-as-a-Service platform.

CUSTOMERS CHOOSE JUMPCLOUD

In speaking with numerous enterprise and SME customers, JumpCloud is noted as a leading entrant in the cloud identity management market. This Boulder, Colorado-based venture-backed business is pioneering a concept called Directory-as-a-Service®. This first-to-market cloud directory service is a direct competitor to legacy solutions focused on being the identity provider within an organization.

Largely, organizations that are leveraging this new concept of directory services in the cloud are mixed-platform, cloud-interested organizations. JumpCloud's customers range from large enterprises to small and medium-sized enterprises. Their ideal customers are leveraging a variety of on-prem and cloud solutions such as AWS, G Suite or Office 365, Mac and Linux systems and more. In our customer checks, the greater the number of non-Windows IT solutions, the more value JumpCloud provides to the customer.

With the cloud identity management sector increasing in popularity, there was some confusion regarding where the various solutions added value. JumpCloud should be viewed as an alternative to Active Directory or Azure Active Directory, with the ability to support mixed-platform environments, and is quickly becoming a leader in this emerging sector. JumpCloud's core capabilities include cloud authentication services via native APIs, LDAP, SAML, RADIUS, and other protocols; systems management for Mac, Windows, and Linux; multi-factor authentication; and identity security.

In our research, JumpCloud as a cloud identity provider isn't likely an acceptable solution for military or large financial services organizations that require on-premises equipment and control, and likely are all Windows shops. These organizations often are subject to a large number of regulatory requirements forcing them to build their own data centers and forgo many cloud-hosted solutions. JumpCloud does participate in regular compliance activities including SOC 2, penetration testing/vulnerability scanning, and PCI.

JumpCloud appears poised for success with a significant cash infusion from OpenView Partners and Foundry Group Next at the end of 2017. We expect JumpCloud to continue to push the envelope in giving IT leaders the powerful solutions that today's demanding identity management challenges demand.

Stack Analysis is a leading analyst firm that is focused on the next generation of enterprise IT. With particular interest in DevOps, security, infrastructure tools, and next generation architectures, Stack Analysis has unique insight into how organizations can leverage their people, modern processes, and world class technology to drive their business forward through extensive research, surveys, and primary interviews. For more information, contact Stack Analysis at research@stackanalysis.io.