RETHINK SECURITY
A massive paradigm shift in the age of access
For years, we have relied on well-defined boundaries to protect our sensitive assets.

These proven digital walls, bolstered by extensive technology and guarded by tough gatekeepers, kept our information safe and out of the hands of cyber criminals. We knew where the perimeters of our networks and endpoints were, and we kept our important assets on the safe side.

These perimeters have disintegrated.

With 90% of all enterprises moving to the cloud, and billions of users accessing data across millions of applications, enterprises face a complex digital canvas of identities.¹ These identities live in and out of the enterprise, creating a new dimension in security. A dimension accessed by one simple permission: the password.
Over $75B was spent on cyber security last year to prevent unauthorized access of our important assets.²

The results? The number of breaches skyrocketed in recent years. Two-thirds of enterprises were breached an average of five or more times in the past two years.³ This technology of the past—including firewalls, virtual private networks (VPNs), and antivirus software from security vendors like Cisco, Symantec, Palo Alto Networks, Check Point, and others—has proven to be an ineffective form of protection.

As a result of these breaches, nearly **six billion** data records were lost or stolen in the past few years—that’s an average of over **165,000** records compromised every hour!⁴ We’ve also witnessed the consequences of a successful data breach significantly increase over the same time period, billions of impacted consumers, a hacked election, and major outages of many well-known companies.

**165,000** records compromised **EVERY HOUR**
According to the latest projections, global cybercrime-related damage costs are expected to exceed $6 trillion annually by 2021.\textsuperscript{5}

\textbf{$6 \text{ TRILLION}$ would buy you 840 BILLION hours of labor}

In order to safeguard our important assets and reduce the risk of breaches in the midst of this new threatscape, \textit{we must rethink how we approach security—and we need to do it now.}

Learn more about the massive shift occurring in the enterprise landscape, the security challenges this shift creates, the emergence of Next Dimension Security\textsuperscript{TM}, and how this new paradigm secures access to the modern boundaryless hybrid enterprise.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter 1:</th>
<th>THE AGE OF ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2:</td>
<td>THERE IS NO LONGER A SAFE SIDE</td>
</tr>
<tr>
<td>Chapter 3:</td>
<td>NEXT DIMENSION SECURITY IS BOUNDARYLESS</td>
</tr>
<tr>
<td>Chapter 4:</td>
<td>DEFENDING THE BOUNDARYLESS ENTERPRISE</td>
</tr>
<tr>
<td>Chapter 5:</td>
<td>THE BREACH STOPS HERE</td>
</tr>
<tr>
<td>Conclusion:</td>
<td>THE FUTURE OF CYBER SECURITY</td>
</tr>
</tbody>
</table>
Chapter 1

THE AGE OF ACCESS
The rapid introduction of new technologies, platforms, applications, and practices expedited the disintegration of the legacy enterprise perimeter, resulted in a complex digital canvas of identities, and fundamentally changed the way we access and interact with data.

The rise in popularity of cloud computing and the explosion of the Internet of Things (IoT) headline the list of technology trends enabling employees to access network servers and sensitive information from outside of the enterprise.

According to the State of the Market: Enterprise Cloud Report from Verizon, 84% of respondents reported an increased use of the cloud and roughly half of companies surveyed expect to use the cloud for at least 75% of their workloads by 2018.\(^6\)
As more employees use the cloud to access data remotely, the global mobile workforce will reach **1.87 billion by 2022**—or **42.5%** of the entire global workforce.⁷

And as these employees use smartphones and other mobile devices to access this data, the latest IoT market projections expect that nearly **30 billion connected devices** will need to be secured by 2020.⁸

Statistics paint a bleak picture for organizations with a static perimeter-based security method of the past. In the past two years, **two-thirds** of companies experienced an average of **five or more** data breaches.⁹ Cyber criminals take aim at identities, from all types of users; from employees and partners, to privilege users and vendors. These identities are easier to steal than ever before—and traditional security measures like passwords prove no match for these attacks.
No password is safe.

Nearly two-thirds of all recently confirmed data breaches involved weak, default, or stolen passwords.¹⁰ Cyber criminals have many resources at their disposal to get their hands on both end user and privileged user identities. Targeted social engineering attacks allow hackers to manipulate individuals into disclosing sensitive information by impersonating a trustworthy source. Two subsets of social engineering attacks; phishing and spear phishing, trick individual employees and enterprises into opening a malicious link and disclosing sensitive information. In the first quarter of 2016 alone, there were an estimated 6.3 million phishing emails and 93% of all phishing emails contained ransomware.¹¹ In addition to these methods, hackers can always purchase credentials from the Dark Web, or rely on a motivated insider to willingly share access credentials.

Enterprises are faced with a complex digital canvas of identities living in and out of the enterprise, creating the next dimension of security. The consequences are dire for those that are slow to realize this new security reality.
Chapter 2

A HISTORY HACKED WITH CONSEQUENCES
The security perimeter has disintegrated. There is no “safe” side of the traditional digital wall.

The boundaryless hybrid enterprise of today is made up of millions of scattered connections across infinite space, creating an environment in which identities are especially vulnerable to attack. It is now easier than ever for hackers to get their hands on end user and privileged user credentials—and no organization is safe.

**Major consequences for consumers**

*No consumer is safe*—in 2016, Yahoo revealed that the account information of over **one billion** consumers—including names, email addresses, and encrypted passwords—was compromised by a data breach that occurred in 2013. In light of this new information, Verizon, which had agreed to buy Yahoo’s internet business for nearly five billion dollars, is asking for amendments to the terms of the acquisition agreement. Yahoo stands to suffer significant economic damage as terms are renegotiated. Now, the internet company is in the news again, as it faces a SEC probe into whether the hack was properly disclosed.
Major consequences for governments

The first hacked election—during the peak of the U.S. presidential primaries, groups of hackers gained access to the Democratic National Committee’s (DNC) servers and the email account of John Podesta, campaign chairman for Hillary Clinton. These hackers, believed to be from Russia, used phishing scams and malware to breach the servers and email systems and steal opposition research, private email exchanges with the media, and sensitive financial information on high-profile contributors to the Clinton campaign.15 16

This information, along with other damaging correspondences between members of the Democratic Party, was released through WikiLeaks in July of last year—the same month as the 2016 Democratic National primaries. News of these breaches dominated news cycles, cast a cloud over the Democratic Party, and had a major impact on the presidential election.
Major consequences for enterprises

Ubiquitous companies go dark—dozens of well known companies experienced major outages after the DNS provider Dyn experienced a severe and extended DDoS attack. The cause? Passwords. Millions of IoT devices with the same unchanged default password were hijacked to create the so-called Mirai botnet. Major brand-name companies like Netflix, Spotify, Twitter, Slack, Etsy, and a ton of other major sites were knocked offline for hours, and even days. Even months after the attack, Mirai is still alive and evolving.17

Cyber criminals continue to target identities at an alarming rate. Forrester found that the least “identity secure” organizations experience twice as many breaches as enterprises considered the most “identity secure.”18 Minimizing our attack surfaces and protecting identities as our networks continue to expand requires a paradigm shift when it comes to security strategy.
Chapter 3

NEXT DIMENSION SECURITY
The status quo isn’t working.

The boundaryless hybrid enterprise is not protected against breaches. It’s time for a massive rethink of security, this is next dimension security. What does next dimension security look like? How does it stop the breach?

Rethink and challenge the perimeter-based approach

Cyber criminals are breaching systems with direct access via a compromised credential—the password. The perimeter-based approach that focuses on protecting endpoints, firewalls and networks completely ignores the vulnerability of identities and passwords.

Redefine security to follow identity

Next dimension security is boundaryless—safeguarding the millions of scattered connections in and out of your enterprise. Protect identities as they access applications, devices, and infrastructure—both on-premises and in the cloud.
Adapt as the boundaryless landscape evolves
Next dimension security adapts as new threats emerge. Cyberthreats are constantly getting more targeted and sophisticated, and static security methods of the past simply can’t keep up. Next dimension security expands as your enterprise continues to incorporate cloud, mobile, IoT, and other technologies—a seamless defense effortlessly following users as they work across applications, tools, and environments.

Power next dimension security with identity services
Identity services automatically provision user accounts, seamlessly manage and authorize access with context-aware controls, and record activity. Identity services control access by all users, from employees to contractors to partners and privileged users, to the information and apps that are appropriate for their role and function. Next dimension security protects access to applications and infrastructure for all users, from any device, anywhere.

Organizations with the highest IAM maturity experience HALF THE NUMBER of breaches as the least mature.22
Identity is the foundation of the massive security rethink taking place.

Adopting Identity and Access Management (IAM) best practices significantly reduces the likelihood of a data breach enabling secure access to applications and infrastructure, from any device, for all users inside and outside of your enterprise. Additionally, the more mature your enterprise’s IAM practices and technology are, the more security, productivity, transparency, and efficiency benefits you can expect to achieve.
A new Forrester study, commissioned by Centrify, examines the IAM maturity of more than 200 enterprises based on 15 essential IAM best practices that make next dimension security possible:

- Enforcing context-aware MFA
- Consolidating identity stores into a single directory
- Implementing single sign-on
- Conducting periodic access reviews for administrative and privileged users
- Limiting access for remote administrators, contractors, and outsourced parties to just the apps and systems they immediately require
- Governing access through time-bound and temporary privileged access
- Automating role-based provisioning to apps and infrastructure
- Automating mobile application provisioning and deprovisioning
- Automatically deprovisioning privileged users’ access as they terminate
- Implementing least-privilege access for administrators
- Centrally controlling access to shared and service accounts
- Eliminating the use of shared administrative accounts
- Managing privileged elevation at the granular command or app level
- Actively monitoring privileged sessions and/or commands
- Recording all privileged sessions and/or commands

Based on how many of the 15 best practices are successfully employed, enterprises are grouped into one of four maturity levels: Level 1 (Low), Level 2 (Mid-Low), Level 3 (Mid-High), or Level 4 (High).
Level 1 organizations experience 2x the breaches
According to the study, enterprises with lowest IAM maturity employ **two or fewer** IAM best practices. These enterprises expose too many passwords and too much privilege, leaving them especially susceptible to data breaches. In fact, Low IAM maturity organizations averaged **more than twice** the number of breaches (12.5) than those with High IAM maturity (5.7) in the past two years.

| LOW MATURITY | 12.5 breaches |
| HIGH MATURITY | 5.7 breaches |

Level 2 organizations are not much better
Businesses with Mid-Low maturity employ **three to five** IAM best practices. While these enterprises are on their way to IAM maturity, only **20%** of Mid-Low organizations implement single sign-on, compared to **43%** of their counterparts with High IAM maturity.

| IMPLEMENT SINGLE SIGN-ON | 43% |
| 20% | |
| LOW IAM MATURITY | |
| HIGH IAM MATURITY | |
Level 3 organizations deliver new products and services faster

Businesses with Mid-Low maturity employ five to eight IAM best practices. 45% of organizations with Mid-High IAM maturity experienced improved time to market for new products and services vs. only 21% of organizations with Low IAM maturity.

Unfortunately, only 20% of the High-Mid group enforce context-aware MFA, in contrast to 57% of the most mature enterprises.
Level 4 organizations save millions in breach and technology costs

The most mature enterprises employ an average of 8 or more IAM best practices. An overwhelming majority of organizations on the highest rung of the maturity ladder record all privileged sessions and/or commands (77%) and actively monitor them (71%). More than two-thirds (69%) conduct periodic access reviews, limit access for remote parties, and centrally control access to shared and service accounts.

Enterprises with High IAM maturity save 40% in technology costs, average $5 million in breach cost savings, and are two to three times more likely to experience improved end user productivity.

Climbing the IAM maturity ladder and achieving next dimension security requires adopting the right practices and technology. Unfortunately, 83% of organizations surveyed have not achieved high IAM maturity—and that is why Centrify is here to help.
Chapter 5

THE BREACH STOPS HERE
THE BREACH STOPS HERE

Centrify stops breaches with an unified identity platform to deliver a seamless defense, effortlessly securing every user’s access to apps and infrastructure in today’s boundaryless hybrid enterprise through the power of identity services.

Centrify Identity Services ensure identities are protected through an integrated solution across applications, devices, and infrastructure. Centrify helps customers reduce IT overhead and improve compliance by providing users with a consistent log in experience and eliminating identity siloes.
Centrify Identity Services Platform is a common set of foundational shared services. App Services, Endpoint Services and Infrastructure Services are built upon this Centrify Identity Services Platform. Let’s dive deeper into some of the key capabilities that make Centrify the only recognized leader in both Privileged Identity Management (PIM) and Identity as a Service (IDaaS) by Forrester and Gartner.²³ ²⁴

---

**ANALYTICS SERVICES**

Risk Scoring › User Behavior › Anomaly Insights

---

**Application Services**

- Single Sign-on
- MFA for Apps
- Lifecycle Management
- App Gateway
- Mobility Management
- On-Premises Apps

---

**Endpoint Services**

- MFA from Endpoints
- Device Management
- App Management
- Local Account Passwords
- Comprehensive Mac Management

---

**Infrastructure Services**

- Identity Consolidation
- MFA for Servers
- Shared Passwords
- Secure Remote Access
- Privileged Access Request
- Privilege Elevation
- Auditing and Monitoring

---

**IDENTITY SERVICES PLATFORM**

- Directory › Authentication › MFA › Policy › Certificate › Federation › Workflow › Reporting
Application Services
Stop the breach before access to apps

As both enterprise cloud usage and the number of mobile workers continue to increase, it is more critical than ever for you to be able to secure all the applications integral to your business. With Centrify Identity Services, you can deploy Single Sign-On to thousands of preconfigured web and mobile applications, and add new applications, in a matter of seconds. Centrify Identity Services also strengthens security for cloud and on-premises applications with adaptive MFA that enables you to choose your authentication methods and elevate privilege based on real-time user risk scoring from the Analytics Services. Integrated Enterprise Mobility Management (EMM) provides IT administrators with a single portal to manage users and mobile devices, and promotes context-aware access to all of your enterprise app and infrastructure.
Endpoint Services
Stop the breach from endpoints

Centrify Identity Services also help you manage access from PCs and Macs. Integrated Mac and mobile device management allows your enterprise to design and deliver a consistent and secure BYOD policy. Centrify Identity Services enforces Robust Smart Card Support for PC and Mac and derived credential support for mobile devices enabling a strong authentication environment.
Infrastructure Services
Stop the breach via privilege

In the Forrester IAM maturity study, a key marker of IAM maturity is preventing unauthorized use of privileged accounts—Forrester predicts that 80% of breaches involve privileged credentials.\(^\text{30}\) Centrify Identity Services helps your organization consolidate identity, authentication, and access management across over 450 platforms—including Linux and UNIX.\(^\text{31}\) Privilege elevation security, based on roles and responsibilities, is swift and seamless.\(^\text{32}\) Secure remote access enables you to secure all administrative access, regardless of location, with context-aware MFA. Record privileged sessions to audit exactly who did what, when and on which system.\(^\text{33}\)
Analytics Services
Stop the breach in real-time

Centrify Identity Services uses machine learning to assess risk based on constantly-evolving user behavior patterns, then assigns a risk score, and enforces an appropriate decision real-time—determining whether the user’s access is granted, requires step-up authentication, or is blocked entirely. Potentially compromised accounts are flagged and elevated to IT’s attention—speeding analysis and greatly minimizing the effort required to assess risk across today’s hybrid IT environment.
Conclusion

THE FUTURE OF CYBERSECURITY
Today’s security is not secure.

It doesn’t matter if you’re one of the largest multinational technology companies, or one of the most powerful and well-known political parties in the world. In the current cyber security landscape, no enterprise or organization is immune to the threat of a data breach—or the catastrophic consequences that follow.

The modern enterprise has moved beyond the traditional perimeter to become boundaryless. With the rapid introduction of new technologies, platforms, applications and practices, a different security reality has set in. Our corporate data is at great risk of being compromised. Although statistics and headlines paint a grim picture of the status quo, the primary vector of attack is well known—compromised identities.

Rethinking your approach to security can keep your enterprise’s complex digital canvas of identities protected in the age of access. It’s time to redefine security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise through the power of identity services. It’s time to take action today.

Let Centrify help you rethink your approach to cyber security.

For more information about how Centrify Identity Services can secure access to your boundaryless hybrid enterprise, visit www.centrify.com/rethink-security
1. www.logicworks.net/blog/2015/03/difference-private-public-hybrid-cloud-comparison
3. Centrify/Forrester report
4. www.breachlevelindex.com
9. Centrify/Forrester report
15. www.wired.com/2016/06/hack-brief-russias-breach-dnc-trumps-dirt
17. www.wired.com/2016/11/web-shaking-mirai-botnet-splintering-also-evolving
18. Centrify/Forrester report
19. Centrify/Forrester report
SOURCES

21. Centrify/Forrester report
27. www.centrify.com/products/identity-service/emm
30. Centrify/Forrester paper citation
Centrify redefines security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise. As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user’s access to apps and infrastructure in today’s boundaryless hybrid enterprise through the power of identity services.

This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California.

To learn more visit www.centrify.com.

The Breach Stops Here.