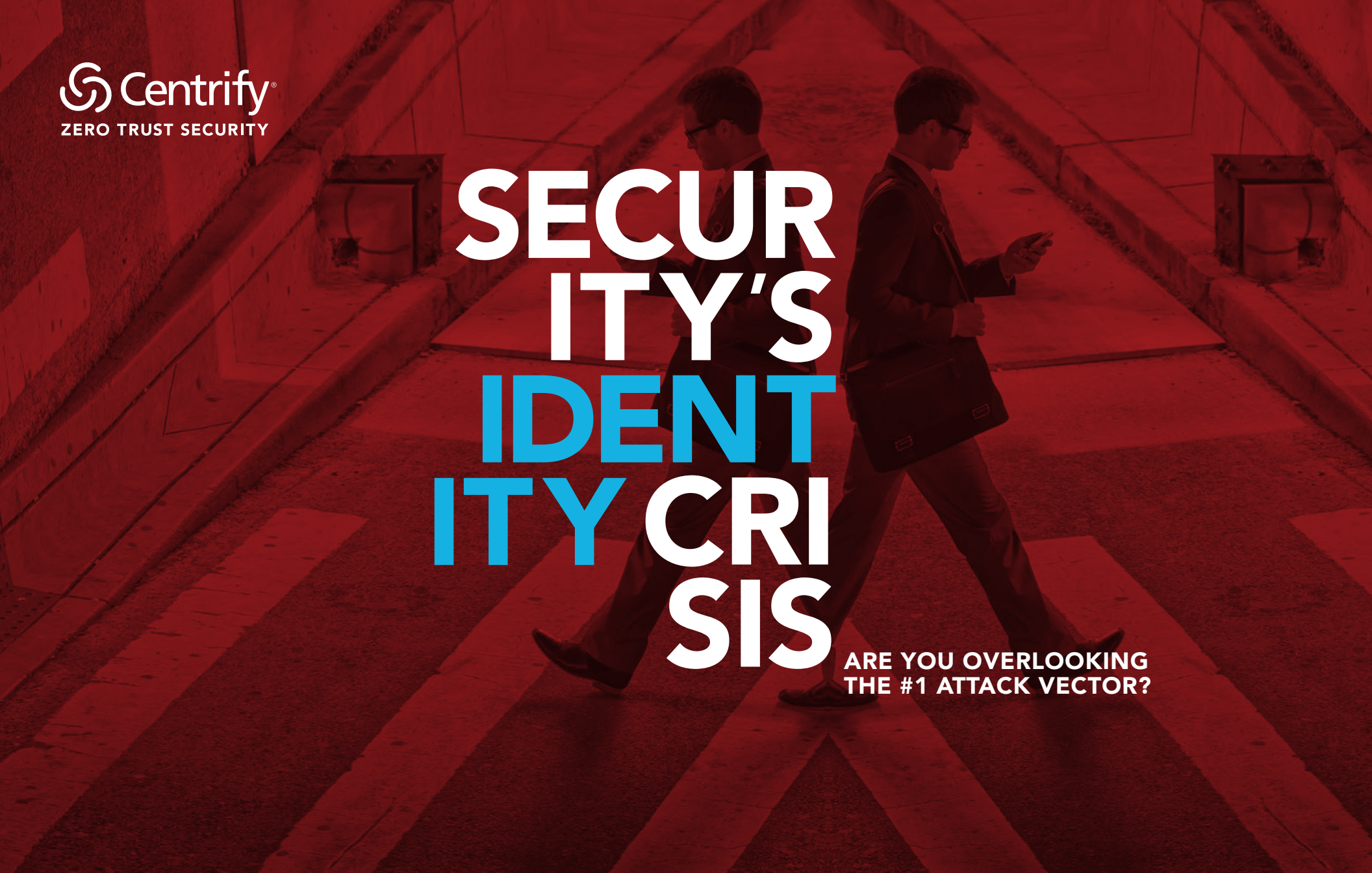

Centrify
ZERO TRUST SECURITY
SECURITY'S IDENTITY CRISIS
ARE YOU OVERLOOKING
THE #1 ATTACK VECTOR?

INTRODUCTION

Despite spending tens of billions of dollars on cybersecurity, there's been no shortage of headlines about massive security breaches. But while most security companies focus on how the breach happened, they're missing a critical part of the story. They're not talking about what's being targeted in order to get to the data. The fact is, most breaches ultimately leverage compromised identities, stolen passwords or privileged access. Access that's essential to the modern boundaryless enterprise and to the way work gets done today. So, it stands to reason that when it comes to breaches, **all roads lead to identity.**

This eBook takes a look at what's behind Security's Identity Crisis and helps you assess how your security strategy stacks up and how to rethink your approach. We'll explore ways to strengthen your company's identity controls along with analysts' best practices.

TABLE OF CONTENTS

CHAPTER 1
Why Today's Security Isn't Secure

GO

CHAPTER 2
Rethink Security for the Current Threatscape

GO

CHAPTER 3
Reduce Risk with Zero Trust Security

GO

CHAPTER 4
Approaches to Achieve Zero Trust Identity Maturity

GO

Chapter 1

WHY TODAY'S SECURITY ISN'T SECURE

Massive security breaches are occurring, and at such an alarming rate, they're beginning to lose their shock value — shocking in itself. **The impact is immense,** despite security's best efforts.

Breaches were up in 2017[1]

164%

THE COST OF FAILED DEFENSE

Despite spending over $80 billion on security last year, two-thirds of companies are still getting breached an average of five or more times.[2] While it's not for lack of effort or investment, it's clear something has to change. And that starts by looking at what's changed to render traditional security approaches less effective.

RECENT CHANGES THAT LEFT SECURITY BEHIND

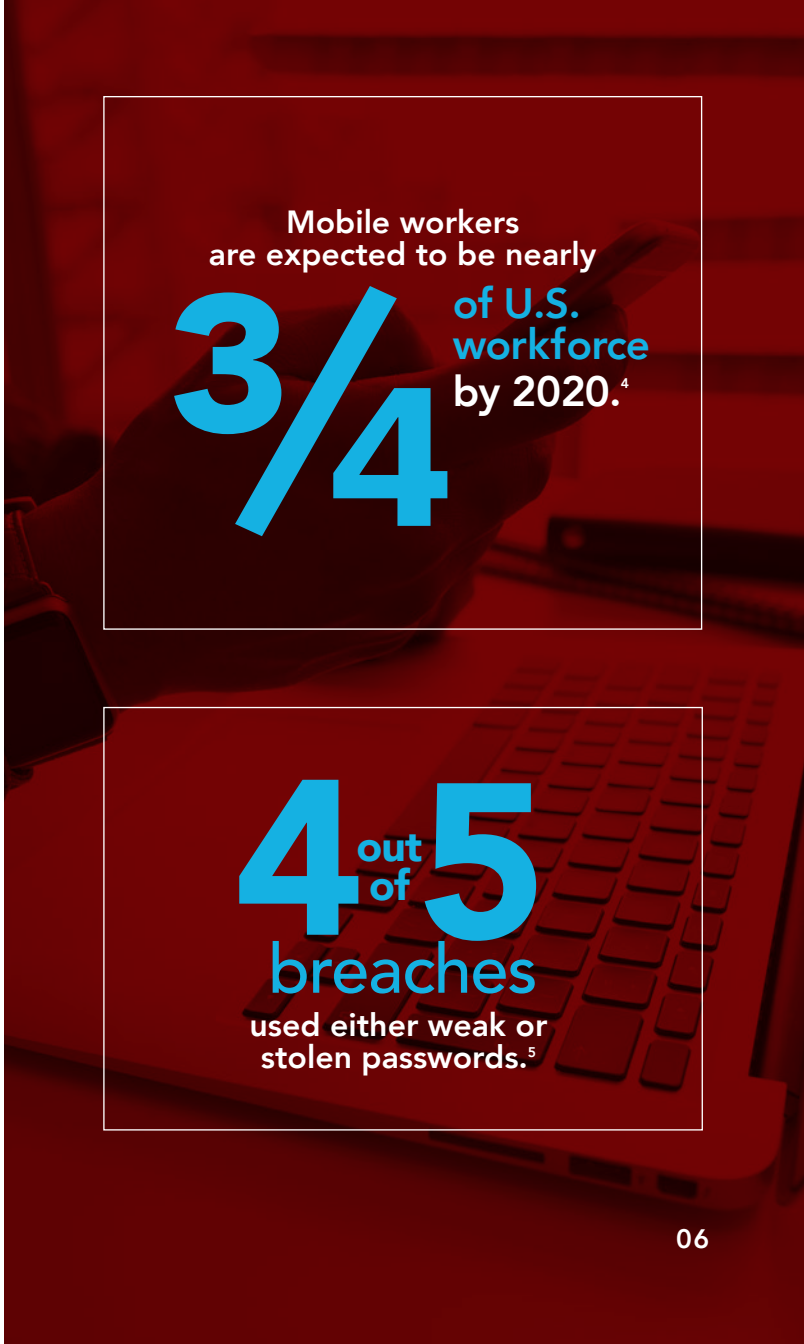
What is the security perimeter?

The workplace today barely resembles what it did even five years ago. Massive amounts of workload are headed to the cloud, the mobile workforce is expanding along with their devices and outsourcing to third-party vendors is all the rage. Add the explosion of IoT, and the traditional security perimeter, which separates trusted users from untrusted users, we knew it has all but vanished. Consequently, security models that rely on the notions of boundary and therefore trust no longer work.

Identity. The #1 attack vector.

Stolen, weak or default passwords are now hackers' number one breach tactic — ahead of malware or social attacks. Why? Because connections are the lifeblood of the boundaryless enterprise. Untethered end users rely on access to tools secured by passwords, provisioned by a host of point solutions, woven together by a thread of complex policies, permissions and processes.

It's little wonder that identity is in the crosshairs. And traditional security measures like passwords are simply no match.



WHAT'S YOUR COMPANY'S RISK?

Think of the things in use at your company that may not be adequately protected by your current security. The more boxes you check, the larger your vulnerable attack surface — creating the foundation for a *Security Identity Crisis*.

Size Up Your Vulnerable Attack Surface

The more of these your company uses, the greater your risk.

- ☐ CLOUD ADOPTION (IaaS/PaaS)
- ☐ REMOTE WORKERS
- ☐ OUTSOURCED IT
- ☐ PARTNER ACCESS
- ☐ SaaS APPS
- ☐ MOBILE DEVICES (and BYOD)
- ☐ BIG DATA PROJECTS
- ☐ IoT DEVICES

A GLARING DISCONNECT

Most security companies concentrate on defending against how breaches happen: phishing, malware or SQL injection attacks.[6] It's not wrong, it's just not working so well.

Security Spend vs. Security Reality

Over the past decade, a major shift in security spending flowed from intrusion detection to intrusion prevention controls, such as unified threat management and next-gen firewalls. This shift has proven effective at reducing risk due to vulnerabilities. However, the current security reality is that 10x more breaches are coming from identity tactics, not vulnerabilities.[7] The disconnect between security spend and actual risk is clear. You can't continue to spend your way to security. And piecemealing multiple identity solutions creates its own **set of challenges**, which we'll explore.

RETHINK YOUR SECURITY PRIORITIES

When you look across your company's attack surface, how confident are you in your ability to protect against compromised passwords throughout your organization — for all users, for all access and privilege across your hybrid environment? If identity is a vulnerable entry point, all the security you've so carefully planned is at risk of being evaded. A new strategy is needed to defend the current security reality.

Are Your Security and Spending Priorities Aligned?

Rank both your security priorities and security spend for the year.

Security Priorities	% Security Spend
____ Next-gen Firewall	_____
____ Security Incident and Event Management	_____
____ Identity and Access Management	_____
____ Endpoint Protection	_____
____ Anti-malware	_____
____ VPN	_____

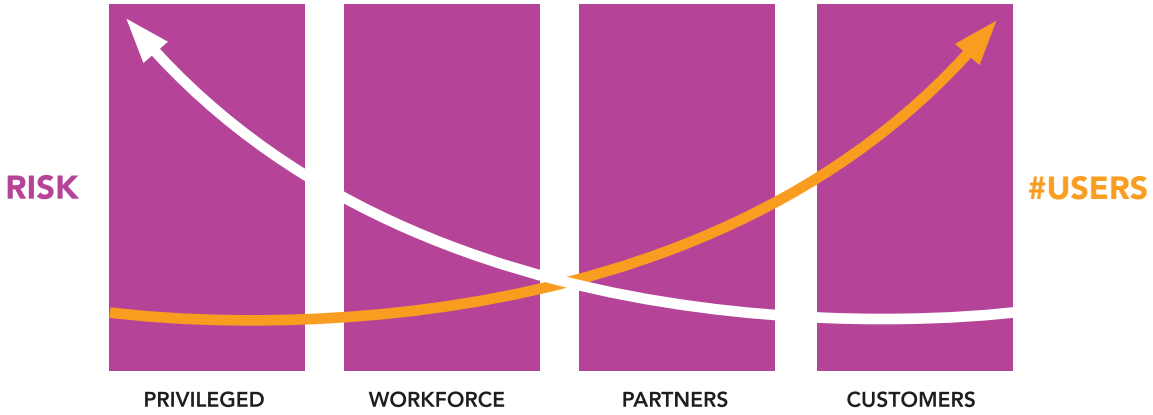
Chapter 2

RETHINK SECURITY FOR THE CURRENT THREATSCAPE

With identity as the vulnerable target for today's attacks, a critical security rethink is needed. One where security follows identity — wherever it exists in your organization. Discard the old model of "trust but verify," which relied on well-defined boundaries. Instead, embrace a new model of "never trust, always verify". Strengthen security levels by implementing a "Zero Trust" approach for everything — including users, endpoints, networks, servers and applications. Zero Trust Security reduces the risk of breaches and enables business agility by dynamically controlling access through knowing the user, knowing their device, giving just enough access, while continuously learning and adapting without hampering access to the tools and information that workers need to get their jobs done.

SECURE ACCESS FOR ALL IDENTITIES

Consider all the different types of identities across the enterprise that need secure access — privileged, workforce, partners and customers. While you may only have a few IT admins, they each represent a huge amount of risk. And although your workforce, partners and customers may represent less risk individually, their sheer numbers create exponential risk. And, as you read this sentence, all of them are being attacked through their identities.



SECURE ACCESS EVERYWHERE

It's more than just people's identities; every one of your IT resources has access-related information that needs to be secured: servers, cloud and on-premises apps, VPN, databases, network devices and mobile devices. The key is for identity and access protection to stretch further, but without stretching worker patience by creating friction between people and what they need to get the job done.

Identity breaches need to stop

You need to protect identities as they access applications, endpoints and infrastructure both on premises and in the cloud.

STOP BREACHES THAT ABUSE PRIVILEGED ACCESS TO YOUR INFRASTRUCTURE

- Too many accounts
- Too much privilege
- Heterogeneous infrastructure
- Remote IT admins
- IaaS adoption
- Regulatory compliance

STOP BREACHES THAT TARGET APPLICATIONS

- So many apps
- Too many accounts
- Increasingly in the cloud
- Phishing and other human error
- Time to productivity
- Remote access

STOP BREACHES THAT START ON ENDPOINTS

- BYOD
- Remote workers
- So many apps
- Local administrators
- Weak authentication
- Access context and trust

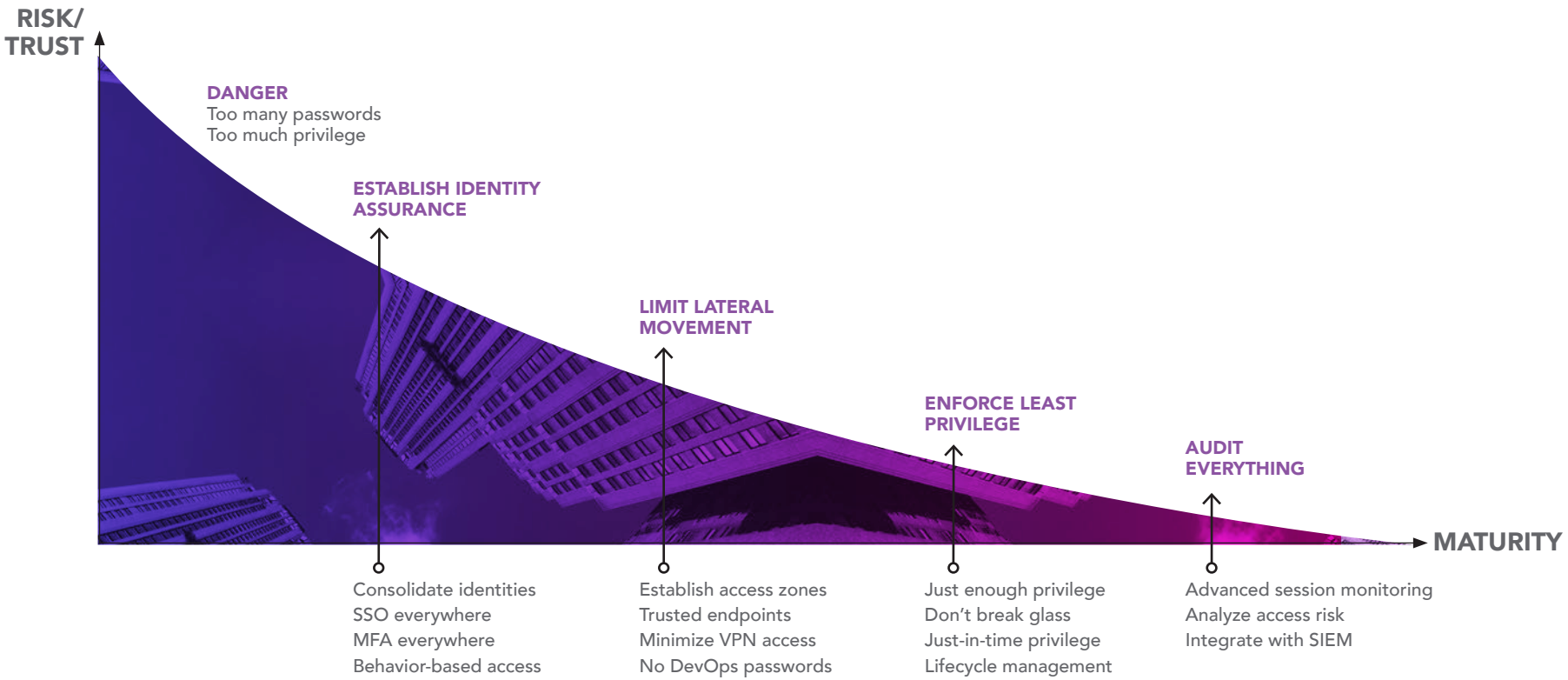
ADAPT

Chapter 3

REDUCE RISK WITH ZERO TRUST SECURITY

Reducing the risk of too many passwords and too much privilege in your organization is a tall order. But according to Forrester research, the solution is to systematically remove trust from the equation, becoming more mature in your Identity and Access Management (IAM).[8]

ZERO TRUST SECURITY REDUCES RISK



FOUR AREAS OF IAM MATURITY

Improving across four maturity areas reduces your likelihood of a data breach while providing the access business needs to thrive.

ESTABLISH IDENTITY ASSURANCE

Never trust, always verify. Identity Assurance is accomplished by consolidating silos of identity, adopting multi-factor authentication (MFA) and single sign on (SSO) everywhere and enforcing behavior-based access control to ensure users are who they say they are, every time.

LIMIT LATERAL MOVEMENT

With a Zero Trust approach, resources should only be accessible from authenticated and trusted endpoints. Then, control people's movement into areas and resources that they shouldn't have access to by establishing access zones, automating account and access provisioning, requiring access approvals and minimizing VPN access.

ENFORCE LEAST PRIVILEGE

Zero Trust involves removing and proactively not granting extra, and often unneeded, privileges. By granting just-in-time privilege and just-enough privilege, you can limit and govern access to only the apps, systems and tasks privileged users immediately need.

AUDIT EVERYTHING

Only when you audit everything can you achieve complete privileged access security. This involves recording and actively monitoring all privileged sessions to get a clear view of all the activity occurring in your organization.

THE BENEFITS OF BEING MATURE

From substantial cost savings to greater productivity, improving your IAM maturity can have a significant impact on your business. Read the **Forrester study results** to learn more.

40%
less on technology costs

$5M
in breach cost savings

2-3x
improved end user productivity [9]

BEST BETS FOR IDENTITY MATURITY

As you consider protecting identity surrounding your company's apps, endpoints and infrastructure, you may wonder where is best to start. While you can make a significant impact quickly beginning anywhere along the maturity continuum, consider the following strategic approaches.

Lowest hanging fruit: SSO and beyond

Given the number of identities across the enterprise — privileged, workforce, partners and customers — the most logical place to start is to improve identity assurance.

Single sign-on (SSO) secures access to thousands of apps by minimizing password risks and lets users access cloud, mobile and on-premises apps from any device. Users can enter a single username and password once, and get secure access to all apps and devices based on policy from IT. SSO needs to support both internal users (employees, contractors) and external users (partners, customers).

Multi-factor authentication (MFA) strengthens security by conditionally requiring that users provide extra information when they access applications, networks and servers. It's one of the best ways to prevent unauthorized users from leveraging compromised credentials to access corporate data — but not if it's only applied for a few apps, some users or a subset of resources. For a Zero Trust approach, it's important to apply MFA across every user and every resource to block cyberattacks at multiple points along the attack chain, mitigating the impact of compromised credentials. Adaptive MFA avoids constant prompting and annoyed users, only challenging when context-based policies aren't met.

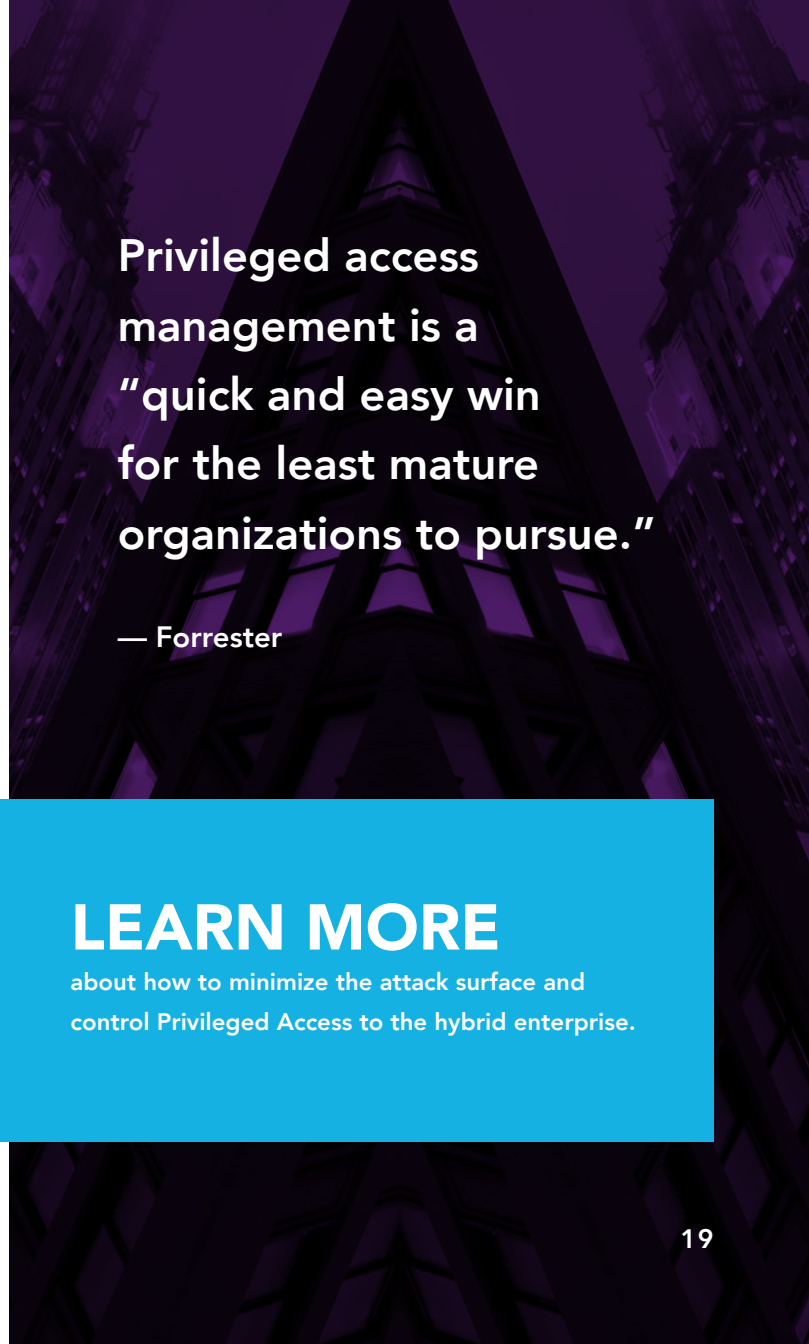
LEARN MORE

Explore SSO and a full range of identity solutions that address your identity needs.

Biggest bang for identity buck: Privilege Access Management

Forrester predicts that 80% of breaches involve privileged credentials.[10] Putting practices into place that put privilege front and center will have an immediate effect on lowering your firm's threat exposure. Privileged Access Management allows you to reduce the risk of security breaches by minimizing your company's attack surface — both on premises and in the cloud. This is accomplished by granting both internal and outsourced IT secure, privileged access to your hybrid infrastructure.

The right privilege solution allows you to consolidate identities, deliver cross-platform, least-privilege access and control shared accounts, while securing remote access and auditing all privileged sessions.



Privileged access management is a "quick and easy win for the least mature organizations to pursue."

— Forrester

LEARN MORE

about how to minimize the attack surface and control Privileged Access to the hybrid enterprise.

STRENGTHEN YOUR IDENTITY

When looking at different solutions to improve your security's identity maturity, consider the following factors when making a decision.

Criteria Checklist

Make sure your solution has these critical capabilities:

- ☐ Does it protect against the leading point of attack used in data breaches — compromised credentials?
- ☐ Does it protect both end users and privileged users by stopping the breach at multiple points in the cyberthreat chain?
- ☐ Does it secure access to both apps and infrastructure across your hybrid enterprise with identity services, both on premises and in the cloud?
- ☐ Is the vendor a trusted leader in security, with 5,000+ customers and greater than a 95% retention rate?
- ☐ Is it recognized by analysts and press as a leader in both PAM and IDaaS sectors?

Chapter 4

APPROACHES TO ACHIEVE ZERO TRUST IDENTITY MATURITY

Improving your Zero Trust maturity can be accomplished in a few different ways, with a variety of consequences. Some choose to piecemeal multiple identity solutions to solve point problems for specific resources. Not only is this expensive, but it can create significant security gaps and increase complexity managing point products. These gaps and inefficiencies pose massive threats, putting companies at risk.

91% of the most mature IAM organizations gravitate toward integrated **IAM PLATFORMS**[11]

CONSIDERATIONS IN PURSUIT OF IDENTITY MATURITY

As you consider how best to improve your company's identity maturity, it's important to keep in mind factors that affect cost, complexity, security gaps and overall risk. The following page breaks out the pros and cons of the three approaches to pursue identity maturity.

Identity status quo

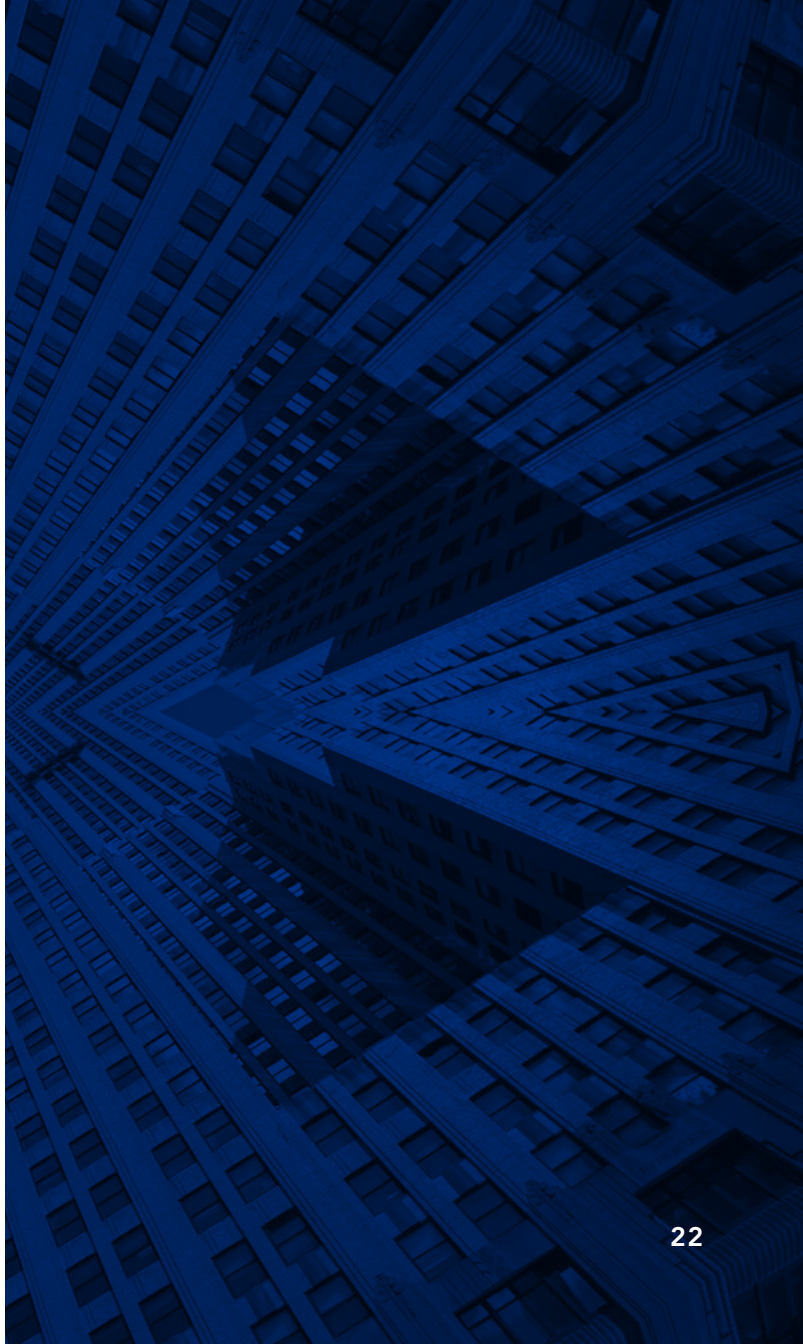
Stay the course with manual processes, or partial, homegrown or legacy solutions.

Best-of-breed identity vendors

Select multiple vendors to address your SSO, MFA and privilege needs.

Comprehensive identity platform

Secure apps, endpoints and infrastructure with a single integrated control plane built on a common platform.



IDENTITY STATUS QUO

Stay the course with manual processes, or partial, homegrown or legacy solutions.

PROS

Partial coverage and benefit from freeware or built-in capabilities improves maturity

Leverages what's already in place with minimal disruption to organization

CONS

Significantly increases your security risk by leaving out entire capabilities required to improve identity maturity

Significantly increases complexity managing multiple homegrown or built-in solutions

Difficult to customize and manage, often requiring expensive skillsets

Lacks breadth of coverage required to mitigate identity-related risks

BEST-OF-BREED IDENTITY VENDORS

Select multiple vendors to address your SSO, MFA and privilege needs.

PROS

Speeds decision-making without coordination among several teams

Reduces some risk by achieving more IAM best practices using state-of-the-art capabilities

CONS

Increases your security risk by leaving gaps in coverage and integration

Increases the number of vendors to manage and receive support from

Cost of integrating silos that only work on one piece of the problem

COMPREHENSIVE IDENTITY PLATFORM

Secure apps, endpoints and infrastructure with a single integrated platform.

PROS

Easier to achieve consistent policy across all your users, so you can see the risk in its totality

Simplifies security management and reduces complexity and integration

Reduces risk by achieving more IAM best practices without sacrificing best-of-breed capabilities

Lowers cost of acquisition and implementation (40% or more on identity technology costs)

Faster time to achieving identity maturity

Better administrative and end user experience

CONS

Requires initial coordination and cooperation across the organization

May require buy-in at a more strategic level in the organization

IAM MATURE FIRMS ACTUALLY SPEND

40%

LESS

on identity technology due to a comprehensive platform approach.[12]

"IT security decision-makers should make best efforts to streamline operations with a single, integrated platform whenever possible to better develop consistent IAM policies and better achieve operational efficiency."[13]

— Gartner

CONCLUSION

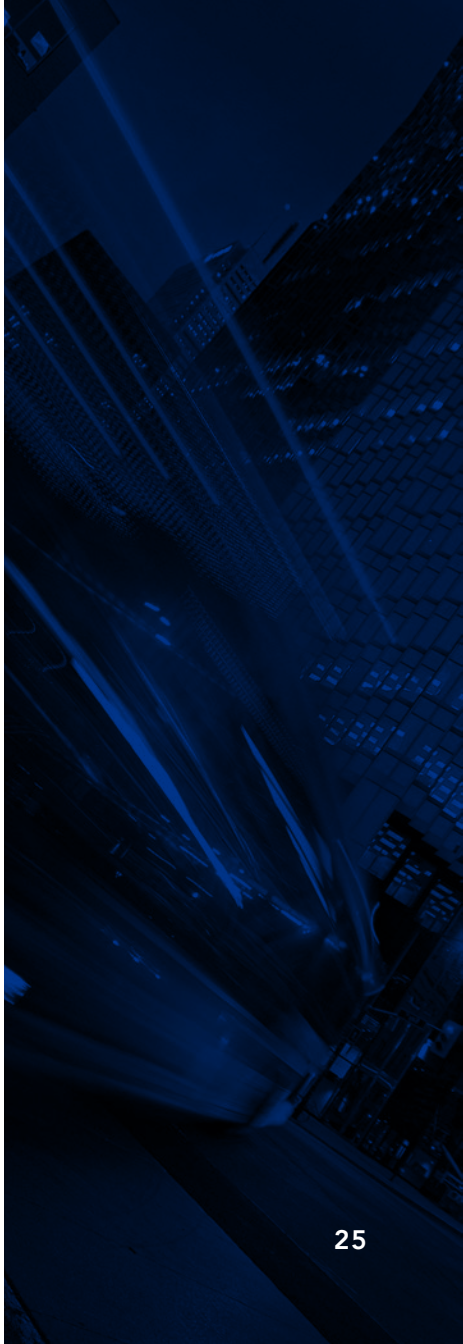
The alarming frequency of breaches in the face of rising security costs requires that companies rethink their security strategy. With compromised credentials as today's #1 threat vector, identity needs to take the security spotlight.

The good news is that you can lower the risk of getting breached by adopting Zero Trust Security and increasing your identity maturity. Zero Trust Security assumes users inside a network are no more trustworthy than those outside the network. As organizations turn increasingly toward a hybrid world of autonomous data management, they need to extend secure access for all identities across the enterprise — from privileged IT admins to business end users to partners to customers. And not just users, but your applications, endpoints and infrastructure — both on-premises and in the cloud. That can only be done by adopting identity best practices to establish identity assurance, limit lateral movement, enforce least privilege and audit everything.

There's more than one way to avoid a security identity crisis. To achieve the full measure of enterprise identity security, both Gartner and Forrester recommend a single, integrated platform approach for greater operational efficiency, better IAM policy consistency and lower technology costs.

There are many factors to consider as you explore your organization's approach to identity, and deciphering various vendors' claims can be challenging. We're passionate about identity's role in securing the enterprise. Let us know how we can help your company's journey.

Secure Your Identity.



1. "Breach Level Index 2017 H1 Report," *Gemalto*. 2017.
2. "Forecast Analysis: Information Security, Worldwide, 1Q16 Update," *Gartner*. June 2016.
3. "The Impact of Data Breaches on Reputation and Share Value," *Ponemon Institute*. May 2017.
4. "IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020," *BusinessWire*. June 2015.
5. "2017 Data Breach Investigations Report, 10th Edition," *Verizon*. 2017.
6. Ibid.
7. "Forecast: Information Security, Worldwide, 2015–2021, 2Q17 Update," *Gartner*. 2017.
8. "Stop the Breach: Reduce the Likelihood of an Attack Through an IAM Maturity Model," *Forrester Consulting*. 2017.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. "Magic Quadrant for Access Management, Worldwide," *Gartner*. June 2017.

Centrify®

ZERO TRUST SECURITY

Centrify is the only end-to-end platform that addresses identity across all your applications, endpoints and infrastructure for all of your users and privileged accounts. Hailed by Forrester, Gartner, PC Magazine and Network World as the only leading provider of both Privileged Identity Management and Identity as a Service (IaaS), we're trusted by over 5,000 customers — more than half of the Fortune 100 — earning a 95% retention rate. They stay because it works. Let us know how we can work for your company.

To learn more visit www.centrify.com.

The Breach Stops Here.