Centrify®

LEVEL UP YOUR SECURITY

Leveraging Multi-factor Authentication to Power Protection

THE QUEST FOR
BETTER SECURITY

IT seems like we are constantly being bombarded with new headlines about high profile organizations falling victim to massive data breaches. Over the last several years, some of the most well-known companies on the planet were rocked by a series of cyber attacks.

Consider some of the most well-publicized recent data breaches:

CASE 01

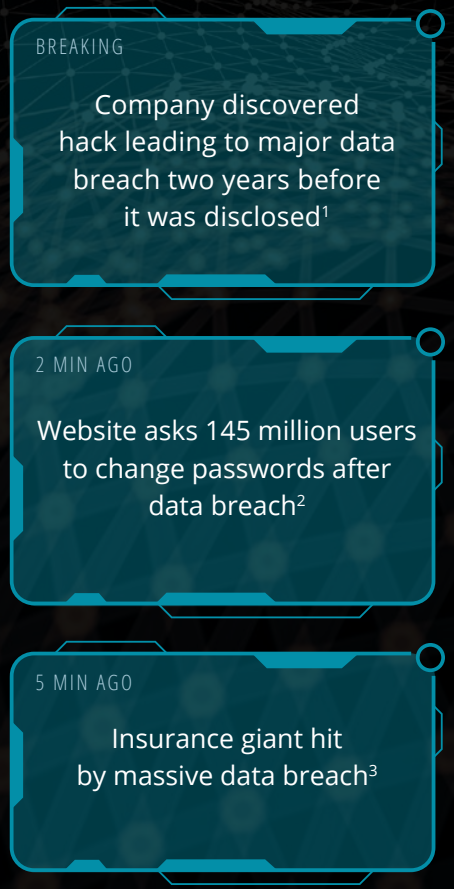
In September 2014, hackers used malware to infiltrate a home improvement retailer's network and steal the credit and debit card information of approximately 56 million customers in the United States and Canada.[4]

CASE 02

In February 2015, a major health insurance plan provider fell victim to a data breach that compromised roughly 80 million patient and employee records.[5]

CASE 03

In May 2016, a data breach of a payroll giant exposed the sensitive financial information—including tax and benefits data—of roughly 640,000 companies.[6]



THE QUEST FOR BETTER SECURITY

From 2014 to 2015, we witnessed a **38%** rise in detected security incidents and a saw whole new wave of organizations fall victim to data breaches—including a global credit reporting company, a healthcare provider, and even an office of the United States Government.[7] According to the Breach Level Index, the first half of 2016 marked an additional **31%** increase in data breaches—as over **554 million** data records were stolen or lost during this period.[8] But that isn't because enterprises are neglecting cyber security. As enterprise networks expand to include more devices, applications (on-premises and in the cloud), and individuals, they create more opportunities for savvy hackers to gain entry and inflict damage. Many cyber attacks occur because the sophistication level of modern cyberthreats surpasses the capabilities of traditional cyber security measures.

In order to protect this larger attack surface against advanced cyberthreats, modern enterprises must level up their security strategies. Implementing more stringent identity-based security company-wide can help prevent sensitive assets from falling into the wrong hands. **Multi-factor Authentication (MFA)** can stop unauthorized access immediately.

In this eBook, enterprises will discover how adding additional layers of authentication can level up their cyber defense and learn how properly deploying Multi-factor Authentication (MFA) can safeguard against modern cyberthreats.

554
MILLION

LOST OR STOLEN DATA RECORDS IN 2016

TABLE OF **CONTENTS**

IT'S GAME OVER FOR PASSWORDS

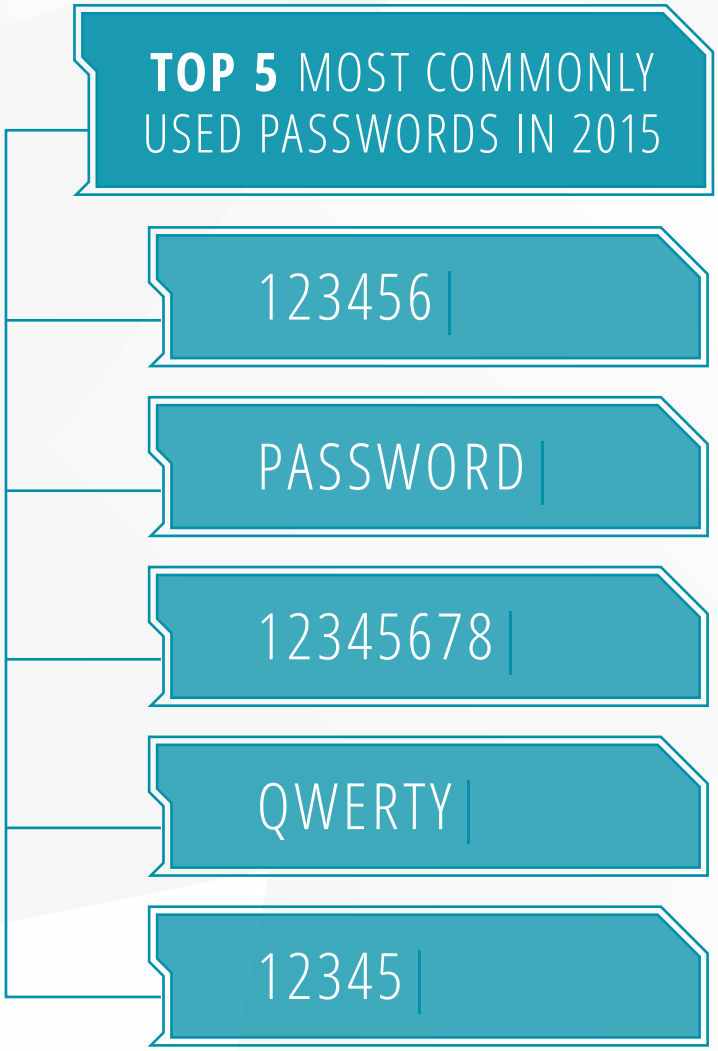
LEVEL 01

IT'S GAME OVER FOR PASSWORDS

IF you would, please join us in a moment of silence for passwords. Individuals and enterprises have long turned to passwords to help keep sensitive assets from falling into the wrong hands, but it's time to call it a mutual split with security's weakest link.

Relying on a single level of username and password-based authentication alone is no longer acceptable in today's cyber security landscape for a number of reasons. For starters, we are collectively very poor at password management. Did you know that **nearly half** (47%) of people use passwords that are at least five years old and **54%** of people use five or fewer passwords across their entire online life?[9]

What makes this even more alarming is how unbelievably simple a lot of our passwords are. According to SplashData, the top five most commonly used passwords in 2015 were: 123456, password, 12345678, qwerty, and 12345.[10] With so much on our minds, it's understandable to want to pick a password that can be easily recalled—but if we can recall our passwords so easily, savvy hackers can too.

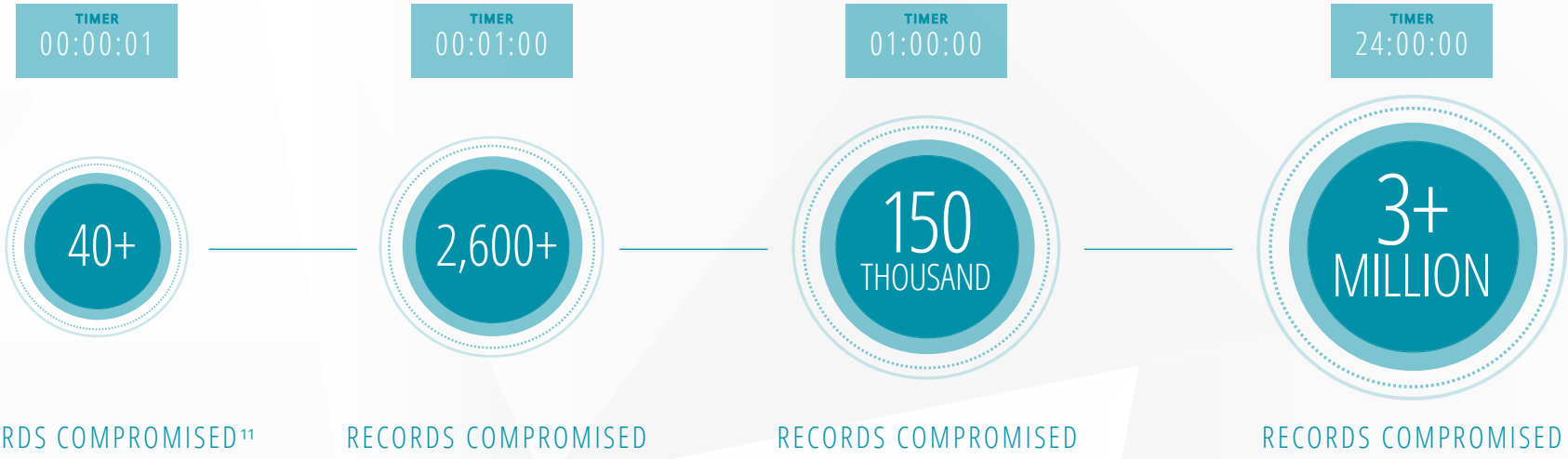


LEVEL 01

IT'S GAME OVER FOR PASSWORDS

Sure, many companies have special criteria in place to keep the family dog ("Spot") or your only child ("Joshua") from being the only line of defense between hackers and sensitive corporate assets. But even when we do come up with a 16-character password complete with numbers and exclamation points, we can't remember them, which is why we keep them written on sticky notes hanging from our monitors, add them to spreadsheets on our desktop, and reuse them across sites and services—all prime examples of poor password management that can leave us just as vulnerable to cyber attacks as simple passwords.

Additional factors leading to the downfall of passwords are the increase in sophistication and frequency of modern cyberthreats. Today, user passwords are subject to a wide range of threats, including social engineering, phishing, brute force attacks, and malware—all at historically high rates. If we break down 2016's 554 million data breaches to date even further, we can truly see how frequently records are compromised or stolen.



IN ORDER TO SAFEGUARD AGAINST THIS ADVANCED ONSLAUGHT OF ATTACKS, MORE ENTERPRISES ARE LOOKING FOR ADDITIONAL LEVELS OF SECURITY THAT CAN AUGMENT—AND ULTIMATELY REPLACE—PASSWORDS.


LEVEL
02
2FA
ACHIEVEMENT
UNLOCKED

LEVEL 02

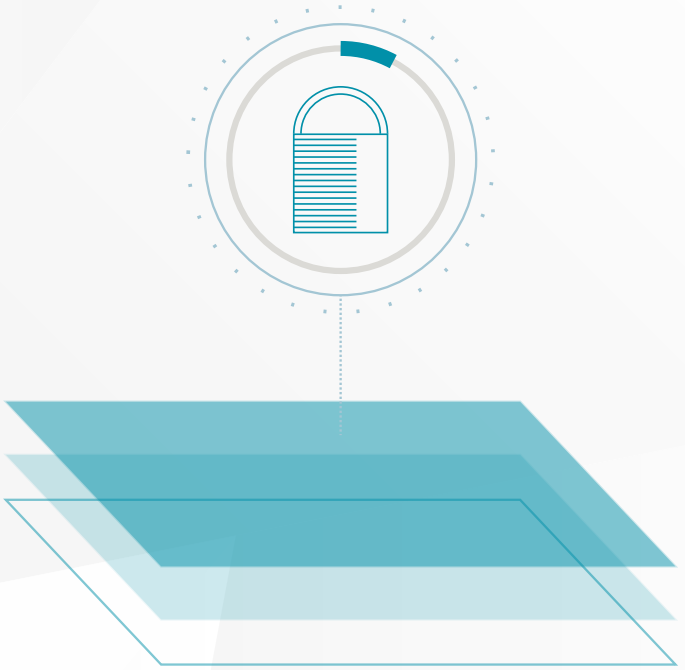
2FA ACHIEVEMENT UNLOCKED

The year was 1968 and Three Dog Night's chart-topping hit "One" cautioned us about the loneliness associated with flying solo. While we're fairly certain Danny Hutton and Co. weren't talking about levels of cyber security, their sentiments ring true in our industry to this day.

Only **10%** of cyber security professionals believe that a single level of username and password authentication provides adequate protection given the current state of cyber security[12], which is why many organizations are looking to level up their security by adding an additional layer of authentication.

Two-factor Authentication, often called *2FA*, is the next logical step for many modern enterprises looking to bolster their cyber security strategies and it does succeed in adding an additional layer to basic account logins. In other words, 2FA combines something you know (like a username and password) with something you have (like a one-time passcode that is sent to your smartphone). Depositing or withdrawing money at an ATM machine with your debit card (something you have) and your PIN (something you know) may be the most common example of 2FA in action.[13]

ONLY **10%** OF CYBER SECURITY PROFESSIONALS BELIEVE THAT A SINGLE LEVEL OF AUTHENTICATION IS ADEQUATE.



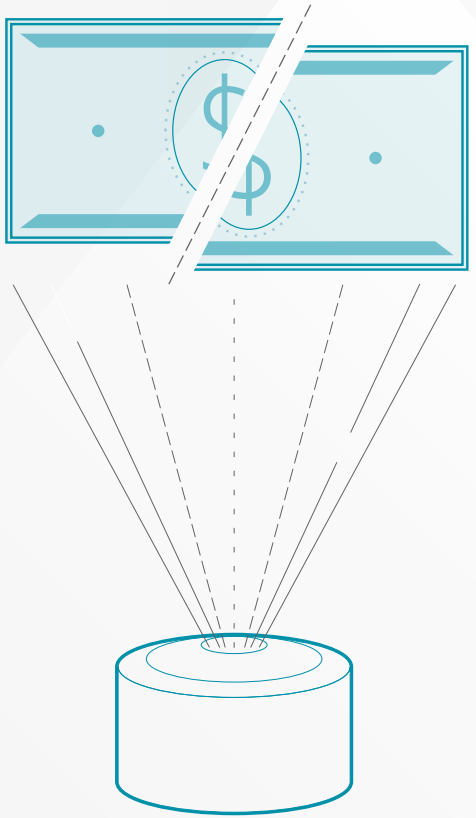
LEVEL 02

2FA ACHIEVEMENT UNLOCKED

Any time your enterprise can add an additional level of security, it makes it more difficult for hackers to break in to accounts and compromise credentials. While 2FA is an important security step to take, legacy solutions are not without their flaws. To put it in gaming terms, legacy 2FA is like a clunky armor upgrade that ultimately bogs down users too much to be effective.

2FA isn't a new idea, but organizations looking to add a second factor of authentication typically had to implement a dedicated on-premises solution that assigned costly hardware tokens to every user. Traditional 2FA solutions either caused too much user friction to be widely adopted, or only worked with certain endpoints and applications—or both. The cumbersome and costly nature of legacy 2FA gave it a bad reputation with both IT professionals and end users.

Although 2FA is improving and represents a step in the right direction, in order to more thoroughly augment passwords today and lay a secure foundation that can help safeguard against future cyberthreats, enterprises need to continue to level up their cyber defense.



A RECENT STUDY CONDUCTED BY ENCAP® SECURITY SAYS COMPANIES CAN CUT AUTHENTICATION COSTS IN HALF BY GETTING RID OF HARDWARE TOKENS.[14]

LEVEL
03

MFA
RESPAWNED

LEVEL 03

MFA RESPAWNED

According to Verizon's 2016 *Data Breach Investigations* Report, **63%** of confirmed data breaches last year involved weak, default or stolen passwords.[15]

If user credentials are the keys to the digital kingdom[16], it makes sense to secure them with as many layers of security as technologically possible. Modern hackers are constantly trying to thwart network defenses, and leveling up your cyber defense with an additional layer of security that is truly unique to each user, makes it infinitely harder for hackers to compromise credentials. But simply adding additional factors of authentication everywhere—every time users need access—will lead to user revolt, which means game over for IT.

Many modern enterprises know that Multi-factor Authentication (MFA) can augment passwords and upgrade security, but legacy MFA generally involves an on-premises deployment that is costly to manage in terms of IT resources and manpower. Creating and distributing physical hardware tokens requires a significant amount of overhead, and many traditional MFA solutions only protect certain assets and end users. Organizations looking to truly level up their security measures across all enterprise identities and resources, will want to look past legacy MFA in favor of an innovative and adaptive cloud-based solution.

LEVEL 03

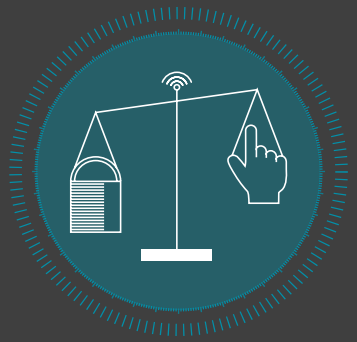
MFA RESPAWNED

Still, many organizations are not experiencing all that MFA has to offer. Maybe they have deployed legacy MFA solutions in a limited capacity. Or maybe they have been reluctant to adopt MFA because they know traditional MFA solutions are costly to deploy and manage—plus the constant prompting is cumbersome for users.

This is why it's time to level up to adaptive Multi-factor Authentication (MFA). By using context-based clues, adaptive MFA can turn what has historically been the weakest security link into a multi-layered nightmare for modern hackers without creating unnecessary hassle for end users. For example, if an employee attempts to log in to an approved cloud app from their work computer during normal business hours, adaptive MFA may not require the employee to provide any additional factors of authentication.

However, if that same employee tries to access the same cloud app from a remote location or a personal mobile device, adaptive MFA will intervene and ask for proof of identity. Implementing flexible authentication methods goes above and beyond traditional perimeter protection to deliver strong and convenient security for modern organizations.

The key to adequately protecting the keys to the digital kingdom is knowing how to properly deploy MFA across your organization so that it not only levels up security, but also improves the user experience.



INDUSTRY-LEADING MFA SOLUTIONS ARE ABLE TO BALANCE STRINGENT SECURITY AND REWARDING USER EXPERIENCES, MAKING STRONG AUTHENTICATION SEAMLESS AND CONVENIENT.[17]

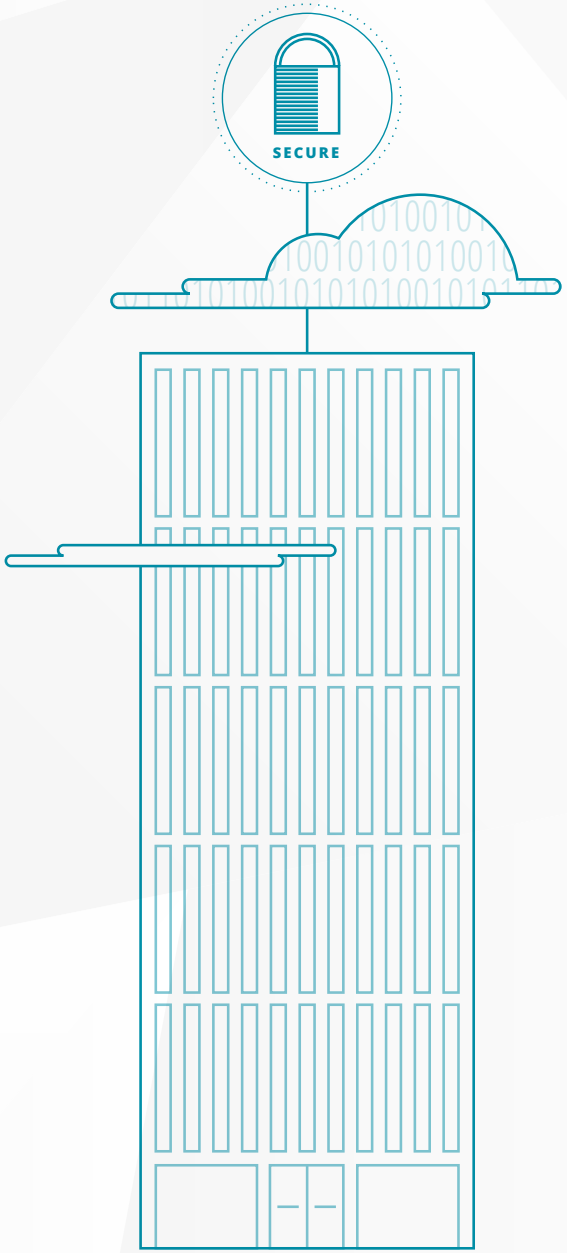
MFA EVERYWHERE
FOR THE WIN

LEVEL 04

MFA EVERYWHERE FOR THE WIN

There's a right way and a wrong way to deploy MFA. At this point in the game, the benefits of MFA are widely understood.[18] Most modern enterprises know that deploying MFA can bolster security for *every* enterprise user, including end and privileged users inside and outside of the organization. They also know that MFA is designed to protect a broad range of enterprise resources, both on-site and in the cloud, including laptops, desktops, servers, applications, VPNs, and even privilege elevation for IT. Most importantly, modern enterprises know MFA can reduce complexity and eliminate glaring security gaps with multiple layers of authentication criteria.

Because security is only as strong as its weakest link, the best way to get the most out of MFA is to adopt an *MFA everywhere* approach.[19] Deploying MFA in silos—across only certain applications, resources, and users—leaves organizations vulnerable to cyber attacks. As more data and workloads are being moved to the cloud, deploying MFA throughout your hybrid IT infrastructure enables companies to more thoroughly protect all potential access points hackers will be looking to exploit.



LEVEL 04

MFA EVERYWHERE FOR THE WIN

When deployed company-wide, adaptive MFA can help ensure your organization's most valuable environments are protected, including[20]:

CLOUD APPS

MFA everywhere boosts the security of applications by requiring that users provide extra information or factors when they try to access applications. Rather than require specific integrations with dedicated apps, today's cloud-based MFA solutions work "in front" of any app, regardless of whether it has a sophisticated security policy or it's a simple homegrown app.

SERVERS

Servers are frequent attack points for hackers looking to access sensitive resources. *MFA everywhere* protects on-premises and cloud servers by requiring users to provide multiple factors before gaining access, checking out super user passwords, or elevating privilege to run specific commands.

VPNS

According to the International Data Corporation (IDC), the number of mobile workers in the United States is expected to reach **105.4 million** by 2020.[21] As more people work from remote locations, *MFA everywhere* can help companies provide users with secure remote access to any IT components they need.

ENDPOINTS

Users can be prompted for additional factors right at login, or before gaining access to application or resource portals—whether from laptops or mobile devices.

INDIVIDUAL USERS

With *MFA everywhere,* all end user and privileged accounts can be secured to block cyberthreats at multiple points in the attack chain.

LEVEL
04

MFA EVERYWHERE FOR THE WIN

Also critical to the success of any MFA solution is the user experience. Traditional MFA solutions are either on or off, meaning they will constantly prompt users to provide additional factors of authentication. Adaptive MFA solutions, on the other hand, are able to make authentication decisions based on context that keep data protected and users from becoming annoyed.[22]

LEVEL
05

CHOOSING THE RIGHT
PLAYER TWO

LEVEL 05

CHOOSING THE RIGHT PLAYER TWO

Already, we've come a long way since the single layer of username/password-based protection of Level One.

You now know that two authentication layers are better than one, and an adaptive policy is best of all. You also know that deploying MFA consistently across all users and resources levels up your cyber defense even more. The final—and maybe most critical—way your organization can level up its security measures is by partnering with the right MFA provider.

In order to help your organization choose the right MFA provider, here's a quick list of features and capabilities to look for in potential solutions[23]:

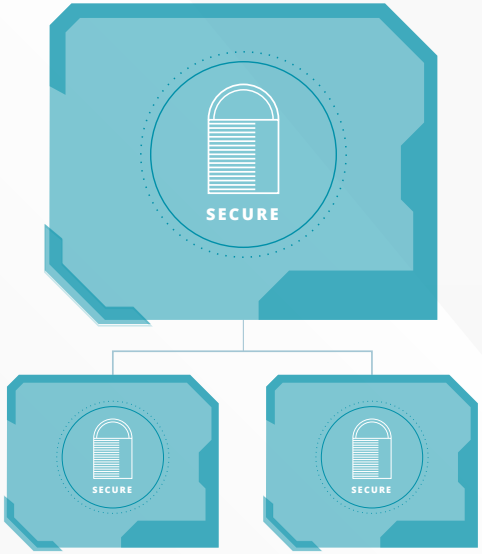
01. The solution being offered should be a comprehensive, centrally-managed platform that enables companies to manage access holistically.

02. It must be able to support an *MFA everywhere* strategy. It should work across all enterprise identities, including end user and privileged user systems, cloud and on-premises applications and servers, VPNs, laptops, and mobile devices.

03. It must be flexible enough to support a range of authentication factors that empower a rewarding user experience and work for tech-averse users. **These factors should include:**

- Push notifications to mobile device and smart watches
- One-time passcodes (OTP)
- SMS/text messages, email or third-party OATH-compliant tokens
- Interactive phone calls
- Smart Cards and derived credentials
- USB PKI tokens
- Endpoint biometrics

04. It should be smart and simple. Companies today need security that is smart and agile enough to adapt as cyberthreats evolve. MFA should be able to challenge for additional factors of authentication based on context. It should also be customizable with flexible authentication profiles and context-based policies.



CENTRIFY'S MFA SOLUTION STRENGTHENS SECURITY ACROSS ENTERPRISE IDENTITIES AND RESOURCES, ALLOWING ORGANIZATIONS TO PROTECT AGAINST THE LEADING CAUSE OF DATA BREACHES.

CONCLUSION
THE CYBER SECURITY ENDGAME

Remember that scene in every sci-fi movie ever made where the protagonist accesses a computer and/or bank vault via retina scan? That's a prime example of biometric security, or authentication based on the characteristics that make each individual unique, and it is quickly becoming more of a reality than a fantasy.

We can already access our smartphones via fingerprint analysis, and many experts believe that biometrics are an advanced way to prove the true identity of end users.[24] We can also take advantage of user behavior and heuristics to make better decisions, further capitalizing on the "something you are" part of MFA. If you walk a certain way, type a certain way, or usually do specific activities at given times from known places—solutions can better assure that you're really you.

CONCLUSION
THE CYBER SECURITY ENDGAME

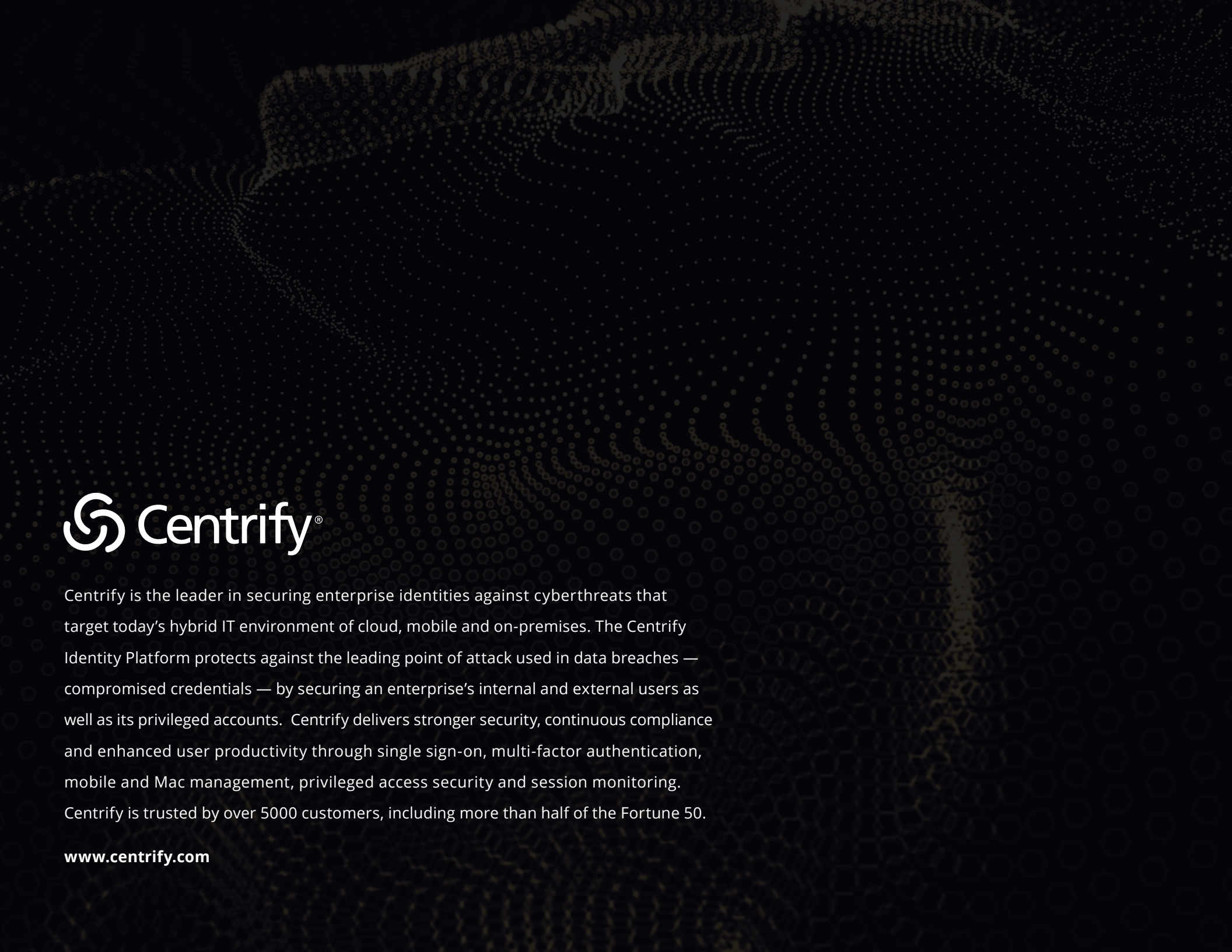
How large of a part biometrics will play in corporate security programs remains to be seen, but one thing is for sure: the cyber security landscape will continue to evolve, which means enterprises must continue to adapt their defense strategies accordingly. In order to protect against the next generation of cyberthreats, organizations need an adaptive identity enterprise platform designed to protect all users and resources across the enterprise. Fortunately, Centrify's suite of MFA solutions are built specifically to level up your security measures company-wide.

Centrify offers flexible authentication methods that make MFA as seamless as possible for all users. Customers can choose from a wide range of methods that include push notifications to smartphones and smart watches, security questions, and Smart Cards. With Centrify's MFA solutions, employees can enjoy secure access to on-premises and cloud applications in the office and on the go. Remote workers can access the IT resources they need to be productive without worrying about being susceptible to cyber attacks, and IT administrators and other privileged users can rest easy knowing multiple authentication factors are preventing unauthorized access to critical resources.

WHEN IT COMES TO LEVELING UP YOUR CYBER SECURITY WITH MFA, CENTRIFY IS THE CLEAR WINNER. **CONTACT US TODAY** TO LEARN MORE ABOUT HOW CENTRIFY PROVIDES MFA EVERYWHERE YOU NEED IT.

SOURCES

1. https://www.washingtonpost.com/news/the-switch/wp/2016/11/10/yahoo-discovered-hack-leading-to-major-data-breach-two-years-before-it-was-disclosed
2. https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach
3. http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/
4. http://www.huffingtonpost.com/2014/09/18/home-depot-hack_n_5845378.html
5. http://www.forbes.com/sites/quora/2015/12/31/the-top-10-security-breaches-of-2015/9/#7453bb505b55
6. http://www.crn.com/slide-shows/security/300081491/the-10-biggest-data-breaches-of-2016-so-far.htm/pgno/0/2
7. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
8. http://www.breachlevelindex.com
9. https://www.entrepreneur.com/article/246902
10. https://www.teamsid.com/worst-passwords-2015
11. http://www.breachlevelindex.com
12. *ESG Infographic IAM Cybersecurity Feb 2016*
13. http://blog.centrify.com/2fa-mfa-difference
14. https://www.encapsecurity.com/study-companies-can-halve-authentication-costs-by-ditching-hardware-tokens
15. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
16. https://msisac.cisecurity.org/whitepaper/documents/1.pdf
17. https://www.centrify.com/media/2275583/centrify-app-security-mfa.pdf
18. https://www.centrify.com/media/3134248/sb-identity-services-for-mfa.pdf
19. https://www.centrify.com/media/3403844/bpb-best-practices-for-multi-factor-authentication.pdf
20. https://www.flipsnack.com/centrify/think-about-mfa-guide-flip.html
21. https://www.idc.com/getdoc.jsp?containerId=prUS25705415
22. https://www.centrify.com/media/3134248/sb-identity-services-for-mfa.pdf
23. https://www.flipsnack.com/centrify/think-about-mfa-guide-flip.html
24. http://www.csoonline.com/article/2891475/identity-access/biometric-security-is-on-the-rise.html



Centrify®

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.

www.centrify.com