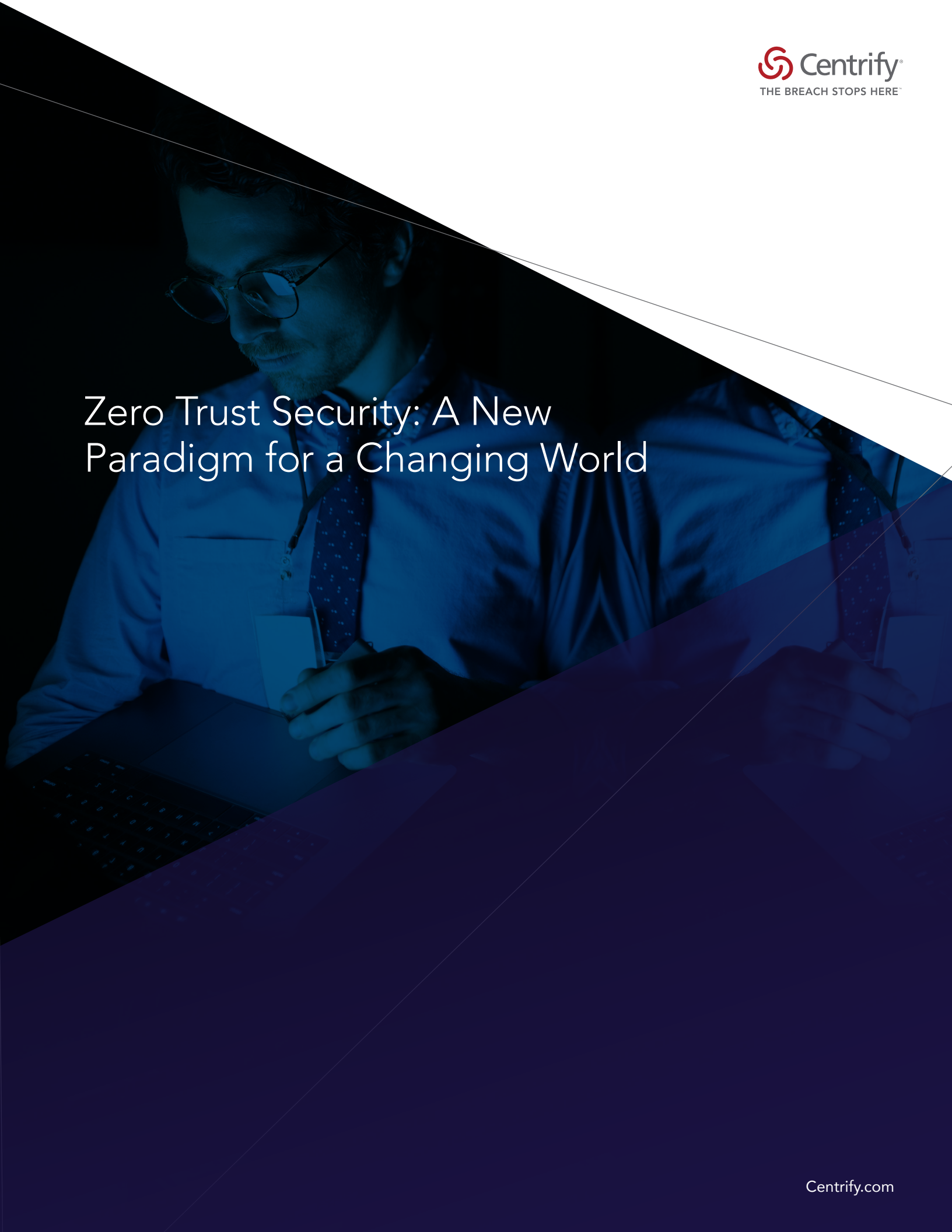
Centrify
THE BREACH STOPS HERE™



Zero Trust Security: A New Paradigm for a Changing World

Centrify.com

Introduction 1

A New Paradigm Driven by Zero Trust Security 2

Zero Trust Security: What the Analysts Say 3

The Google Approach to Zero Trust 3

What is Zero Trust Security 4

Four Core Elements of Zero Trust Security 5

Benefits of Zero Trust Security 7

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 100, 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.

US +1 (669) 444 5200 | EMEA +44 (0) 1344 317950 | Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876 | Latin America +1 305 900 5354 | sales@centrify.com

©2018 Centrify Corporation All Rights Reserved. Centrify is a registered trademark, and The Breach Stops Here and Next Dimension Security are trademarks of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners. ©2018 Centrify Corporation. All Rights Reserved.

Centrify
THE BREACH STOPS HERE

Zero Trust Security: A New Paradigm for a Changing World

A significant paradigm shift occurred in the last few years. Much like other technological shifts of the last decade — when cloud computing changed the way we do business, agile changed the way we develop software and Amazon changed the way we shop — Zero Trust presents us with a new paradigm in how we secure our organizations, our data and our employees.

While difficult to identify the precise tipping point, one thing is certain: what were once extraordinarily high-profile, damaging breaches are no longer extraordinary. In just the last 18 months, Yahoo, Accenture, HBO, Verizon, Uber, Equifax, Deloitte, the U.S. SEC, the RNC, the DNC, the OPM, HP, Oracle and a profusion of attacks aimed at the SMB market have all proven that every organization — public or private — is susceptible.

The epiphany behind the paradigm shift is clear: Widely-accepted security approaches based on bolstering a trusted network do not work. And they never will. Especially when businesses are dealing with skill shortages, overloaded employees and an ever-expanding number of cloud apps and mobile devices that broaden the attack surface with each passing day.

Organizations spent a combined $150 billion on cybersecurity in 2015[1] and 2016[2]. During approximately the same period, 66 percent of organizations surveyed reported five or more data breaches[3]. Money won't solve this problem. An entirely new approach is required. And now it's here.

Commonly-accepted security approaches based on bolstering a trusted network do not work. And they never will.

Organizations spent a combined

$150 billion

on cybersecurity in 2015 and 2016.

During that same period,

66%

of organizations reported five or more data breaches.

1 Gartner Press Release, *"Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015"*, September 23, 2015.

2 Gartner Press Release, *"Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016,"* August 9, 2016.

3 *Stop The Breach: Reduce The Likelihood of An Attack Through An IAM Maturity Model.* (2017). Forrester Research, p.1. Available at: https://www.centrify.com/media/4594046/stop-the-breach.pdf [Accessed 1 Jan. 2018].

©2018 Centrify Corporation All Rights Reserved.

A New Paradigm Driven by Zero Trust Security

Traditional perimeter security depended on firewalls, VPNs and Web gateways to separate trusted from untrusted users. But as mobile employees began accessing the network via their own devices, perimeters blurred. And they virtually disappeared with the rise of cloud computing and IoT devices.

At the time, the benefits of these technologies outweighed the perceived risks. But cybercriminals saw opportunities. In the last few years, businesses were facing the threat of devastating losses, and legacy security providers had no answers. The focus turned to IT security analysts, industry powerhouses and innovative security companies. The conclusion is "Zero Trust Security."

ZERO TRUST MANDATE

Following the highly-publicized breach of the U.S. Office of Personnel Management (OPM), which exposed the personal data of millions of Americans, the U.S. House of Representatives' Committee on Oversight and Government Reform issued a report recommending that federal information security efforts move toward a Zero Trust model. Stating that, "The Zero Trust model centers on the concept that users inside a network are no more trustworthy than users outside a network,[4]" the 2016 report triggered a discussion of Zero Trust across the public and private sectors.

Zero Trust Security: What the Analysts Say

Forrester has long been an advocate of a Zero Trust strategy, stating that "CIOs must move toward a Zero Trust approach to security that is data- and identity-centric — and in our view is the only approach to security that works."[5]

To adhere to Zero Trust, Forrester suggests that organizations should "Never assume trust — even with users: In too many compromises and data breaches, hacked credentials and users' interactions precipitated and even facilitated the attack. Those same users' and admins' credentials and accesses were the avenues through which cybercriminals gained unfettered access to the network."

The research analyst firm adds, "Governing user access is key to success: Just as with network security and Zero Trust, you must identify, segment, and analyze your users to shift power in your favor. Your users have job roles and needs that make your business run; you must analyze those roles and needs and then segment them to enable Zero Trust."

Forrester further suggests that key layers of Zero Trust should include:

Gartner's recommended CARTA methodology, takes a broader approach, but contains many of the core elements of Zero Trust Security.

The Google Approach to Zero Trust

It's not only theory espoused by analysts, Google has put Zero Trust into action with their BeyondCorp project. Recognizing the need for change, the company began altering its own network security policies to reflect a model of "zero trust" back in 2015, essentially handling its internal network as it would the insecure Internet.

Google's BeyondCorp model entirely removes trust from the network, securely identifies the device and the user, and applies dynamic access controls, least privilege and context aware policies. While they have no complete solution for customers, they have provided what many security analysts feel is the most compelling reference architecture to date.

The Google BeyondCorp approach mirrors the Centrify Zero Trust approach. It has always been our goal to provide organizations with the best-of-breed technologies they need to secure their organizations — not through a porous and indefensible perimeter, but through a unified, identity-focused platform that serves all users and their access to all resources, including both apps and infrastructure.

4 Committee on Oversight and Government Reform U.S. House of Representatives, *"The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,"* Hon. Jason Chaffetz, et al. September 7, 2016

5 Forrester Research. "Develop Your Zero Trust Workforce Security Strategy," Cunningham, Chase, 5 Dec. 2017. pp.7-8.

©2018 Centrify Corporation All Rights Reserved.

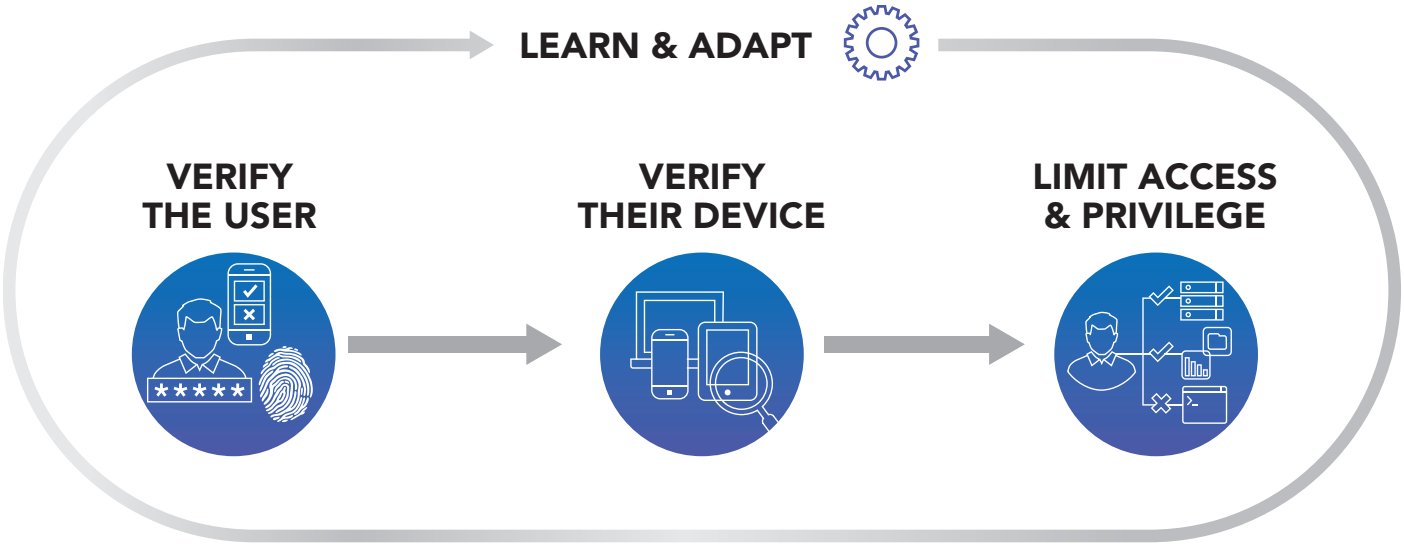
What is Zero Trust Security?

The Centrify Zero Trust Security model assumes that untrusted actors already exist both inside and outside the network. Trust must therefore be entirely removed from the equation. Zero Trust Security requires powerful identity services to secure every user's access to apps and infrastructure. Once identity is authenticated and the integrity of the device is proven, authorization and access to resources is granted — but with the just enough privilege necessary to perform the task at hand.

Instead of the old adage "trust but verify," the new paradigm is "never trust, always verify." Effective Zero Trust Security requires a unified identity platform consisting of four key elements within a single security model. Combined, these elements help to ensure secure access to resources while they significantly reduce the possibility of access by bad actors. To implement Zero Trust Security, organizations must:

1. Verify the user
2. Verify their device
3. Limit access & privilege
4. Learn & adapt

This approach must be implemented across the entire organization. Whether you're giving users access to apps or administrators access to servers, it all comes down to a person, an endpoint and a protected resource. Users include your employees, but also contractors and business partners that have access to your systems. Complicating your environment with different systems for different situations is unnecessary, and disparate tools can introduce gaps in security.



©2018 Centrify Corporation All Rights Reserved.

Four Core Elements of Zero Trust Security

Following are building blocks that when unified, provide a pathway to achieving Zero Trust Security:

1. Verify the User

Today, the most basic way to verify a user is through a username and password. But how can we be certain that the user is who they claim to be and not someone who's guessed or phished the password, or purchased compromised credentials off the Dark Web?

Additional identity assurance is gained by enhancing passwords with multi-factor authentication (MFA), which uses something you have, something you know or something you are. The level of trust gained through additional verification steps partially determines if access is granted and to what specific level.

Zero Trust principles apply regardless of user type (end user, privileged user, outsourced IT, partner or customer) or the resource being accessed (application or infrastructure). Access decisions must be adaptive and dynamic.

Centrify's IDaaS and MFA solutions address Zero Trust Security's Verify-the-User component. Organizations can evaluate attributes and behavior to determine the amount of verification needed to securely authenticate users, and require additional actions (MFA) as needed to ensure authenticity. Once authenticated, users gain access to all pre-approved resources. Additional verification may be required to elevate privilege or to access the most sensitive data.

2. Verify their Device

To achieve Zero Trust Security, identity-centric preventive controls must be extended to the endpoint. As with users, devices cannot be trusted without verification. Verifying a device involves the verified user enrolling their device so that it is recognized.

If the user is requesting access from a registered device they use every day, they have a certain level of trust. If they're trying to access services from a workstation in an Internet café they've never used before, then trust is out the window.

Verifying their device also involves ensuring devices are only allowed access if they meet certain security requirements: Have they been jailbroken? Do the device settings conform to company policies like disk encryption, virus protection and up-to-date patches?

Centrify EMM solution addresses Zero Trust Security's Verify-their-Device component. With Zero Trust, it's essential that information about the user's identity and information about the endpoint come together to assign a risk score. If risk is low, friction decreases. As risk increases, the appropriate controls kick in, requiring additional factors of authentication or more restricted access.

©2018 Centrify Corporation All Rights Reserved.

3. Limit Access & Privilege

User privileges must be tightly managed. Malicious parties frequently target personnel with administrative privilege to gain control over business systems. First, with Zero Trust Security, it's important to limit lateral movement within all resources such as servers and workstations by limiting users to only the access they need to perform their jobs.

Second is authorization into business applications. Because these applications often contain large amounts of critical data and because they're typically accessed by more users within the organization, they can be easier targets for attackers. It's therefore equally important to provide just enough access inside each application for users to do their jobs.

Suppose an attacker logs into a database using stolen credentials. Because the user's privileges are limited to the bare minimum, the attacker will be limited to what they can access as well. The more critical the data, the less privilege--and the increased use of MFA to ensure identity.

Centrify's host-enforced Privileged Access Management (PAM) restricts access to just the systems and resources associated with a user's specific job. By granting just enough privilege and easing the process for privilege elevation, risk is reduced and security increased. If user credentials are compromised, the amount of damage that can be done is limited.

4. Learn & Adapt

Much like Gartner has suggested with their CARTA approach, Zero Trust Security must continuously improve by learning and adapting. Information about the user, endpoint, application or server, policies, and all activities related to them can be collected and fed into a data pool that fuels machine learning.

The system can then automatically recognize out-of-the-ordinary behaviors–such as a user trying to access resources from an unusual location — which immediately raises a red flag that may require a second form of authentication, depending on policies.

Behavior analytics are used to ascertain the risk level of individual transactions and decide in real-time whether or not to allow them. This also provides identity services with key insights that can tell administrators when policies need to be changed.

Centrify Analytics Service leverages behavioral data to stop compromised credential-based attacks. Through machine learning, Centrify Analytics Service assesses risk based on constantly-evolving user behavior patterns. It assigns a risk score and enforces an appropriate access decision, all while simplifying risk monitoring and analysis.

©2018 Centrify Corporation All Rights Reserved.

Benefits of Zero Trust Security

The Zero Trust paradigm moves from network-based to identity and application-based security, dynamically balancing user experience with risk and allowing companies to embrace a perimeter-free infrastructure.

This approach to security minimizes exposure and increases compliance by securing access to applications and infrastructure for all users. In addition, Zero Trust Security:

- Leaves no gaps by covering the broadest range of attack surfaces, ranging from users to endpoints, networks and resources.
- Enables organizations to increase business agility through the secure adoption of cloud and mobile solutions.
- Provides a framework to properly manage the risk of exposing sensitive apps and infrastructure to business partners.
- Ensures IT visibility into risk in their access controls, and can automatically identify the "needle in the haystack" of potential risk through abnormal behavior which would never be detected through manual forensics.
- Creates satisfied, productive users by ensuring the proper controls are in place to address appropriate levels of risk without requiring a heavy-handed, maximum-control approach.
- Requires less management, skillset and costs less than a patchwork defense focused on silos or resources.

It Takes Centrify. Never Trusting. Always Verifying.

It takes zero trust to trust. Zero Trust Security reduces the risk of breaches and enables business agility by dynamically controlling access based on what is known about a user and their device. The Zero Trust approach secures access to enterprise resources through verifying the user, verifying their device, limiting access & privilege and learning & adapting.

Centrify's Zero Trust Security empowers your business and protects your customers in ways that go far beyond typical security concerns, addressing challenges such as digital transformation, intersilo finger-pointing and increasing data awareness and insight.

Through a unified, integrated solutions offering, Centrify provides identity services across applications, endpoints and infrastructure for all users, without sacrificing best-of-breed features. Organizations may consider approaching Zero Trust by implementing IDaaS, MFA, EMM, PAM and User Behavior Analytics (UBA) technologies from separate vendors, but disparate solutions leave gaps and are expensive to implement and maintain.

Centrify's Identity Services provide all elements of Zero Trust Security and Centrify is the only vendor with leading solutions recognized in:

- The Forrester Wave™: Identity-as-a-Service, Q4 2017 (IDaaS)
- The Forrester Wave™: Enterprise Mobility Management, Q4 2017 (EMM)
- The Forrester Wave™: Privileged Identity Management, Q3 2016 (PAM)

For more information on how you can implement Zero Trust Security across your organization with Centrify, visit www.centrify.com/solutions/zero-trust-security-model.

©2018 Centrify Corporation All Rights Reserved.