

EBOOK

WEAVING YOUR ZERO TRUST IDENTITY FABRIC

How to spin your existing IAM
silos into gold

Identity is More Critical Than Ever

The past year was challenging on so many levels—social, physical, emotional, and financial. This was especially true for most business and government agencies who were forced to accelerate their digital transformations to adapt to the new landscape. But while the bulk of us suffered and struggled to find our feet, one group was thriving—hackers. The 2021 IBM Cost of a Data Breach found that:

While the bulk of us suffered and struggled to find our feet, one group was thriving—hackers.

There was a

10%

increase in the average total cost of a data breach from 2020 to 2021.

There was a

\$1.1M

cost difference where remote work was a factor in the breach.

20%

of breaches caused by compromised credentials; the most common attack vector.



Is Zero Trust the Answer?

As traditional IT defenses were strained during the pandemic, one potential architecture framework emerged as a potential savior to address these business challenges: Zero Trust. But, is this an effective solution?


The data speaks for itself...

\$1.8M

cost difference where
mature zero trust was
deployed vs. no zero trust.

So, if Zero Trust is the answer, then where
do you begin your journey?





Zero Trust states that you must verify everything trying to connect to your resources before granting access.

The Security Maturity Model and Zero Trust

To adopt Zero Trust, many different security tools and technologies are required; each to protect a specific area or attack vector. But the glue that brings all of these together is Identity. To understand why Identity is the foundation of Zero Trust, we need to examine the security maturity model journey.

Organizations start their security at the perimeter, securing access to the data center. The data center is then segregated into forests and virtual private clouds to further isolate sensitive resources. Access controls are implemented within applications and data stores, and communication channels are encrypted and protected. Finally, privileged access controls are implemented to push security down to the individual servers and containers.

Zero Trust states that you must verify everything trying to connect to your resources before granting access, which means that security must be built from the kernel to the perimeter (and beyond to the emerging cloud environments).

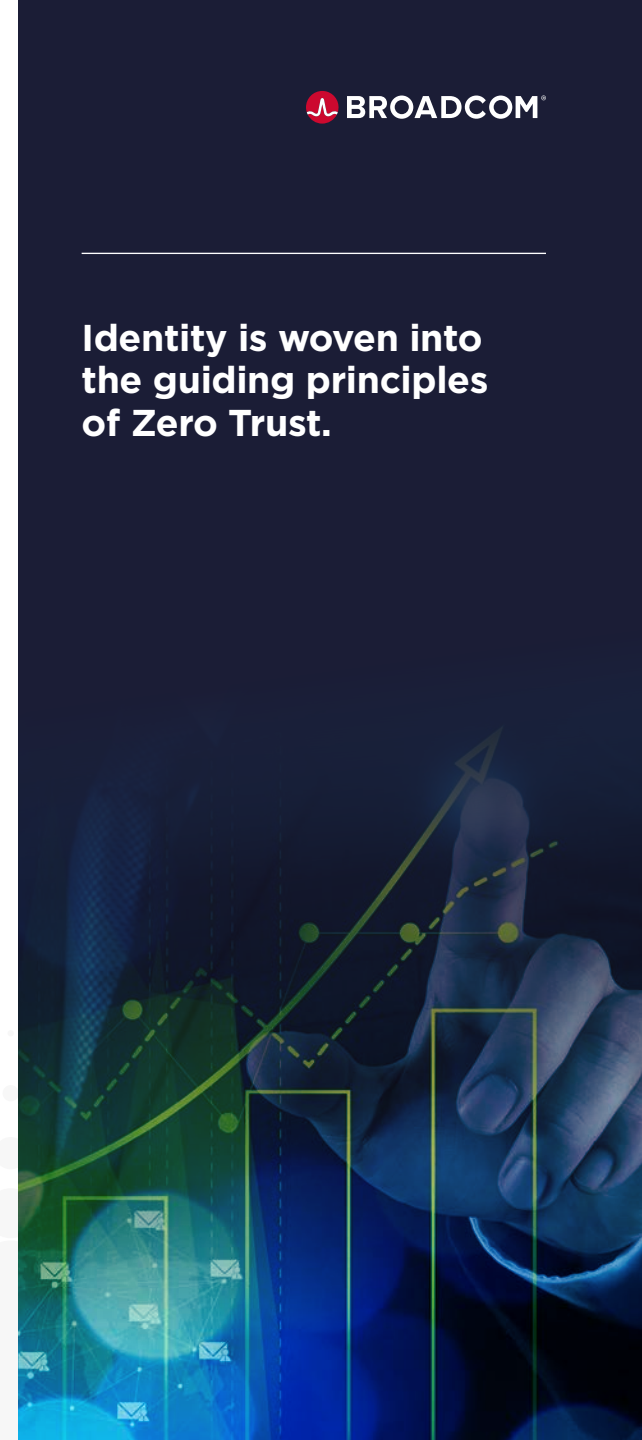
The Authorization Dilemma of Zero Trust

The difficulty with extending Zero Trust down to the kernel is based on the granularity of access required because the deeper you move into your environment, the finer the granularity is required to make authorization decisions, and this significantly increases the operation burden to manage these policies and entitlements.

This is why Identity is woven into the guiding principles of Zero Trust:

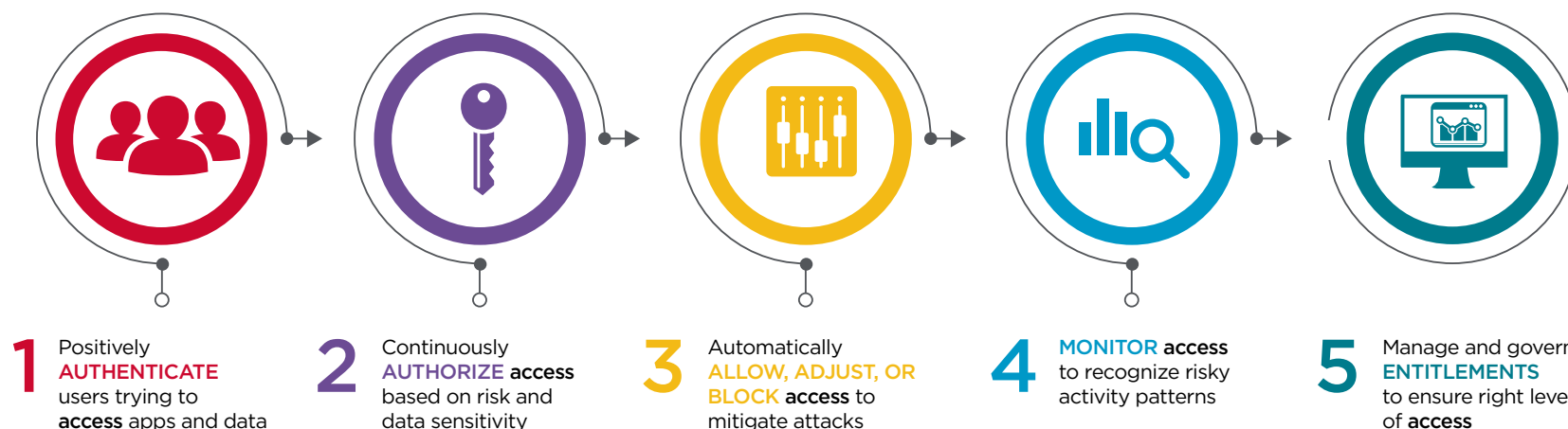
- Positively Identity Every User and Device Requesting Access;
- Enforce Least Privileged Access for Authorization Decisions; and
- Apply Intelligence to Achieve Continuous Verification Process.

Identity is woven into the guiding principles of Zero Trust.



The Critical Capabilities of an Identity Fabric

In order to align your Identity Fabric with the principles of Zero Trust, you must ensure that Identity and Access Management (IAM) technologies can do the following for any user connecting through any device to any application.

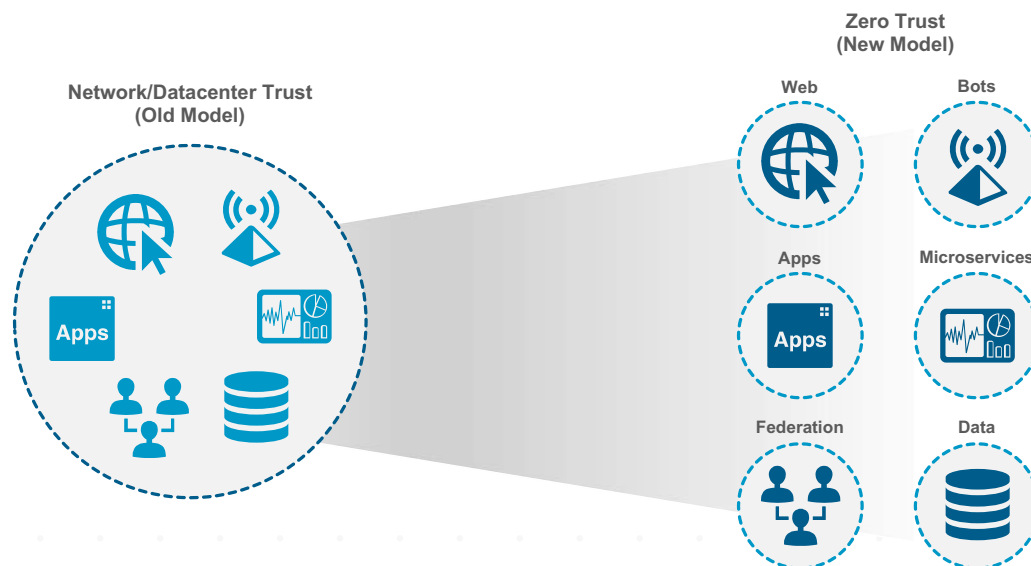


But we are already doing this, or are we? Most organizations have been deploying IAM technologies for the past twenty years or more. So why are we hearing so much about building an Identity Fabric now? What has changed?

We need to bridge today's "as-is" environments and tomorrow's "to-be" environments, securely.

Digital Transformation is Driving IAM Architecture 3.0

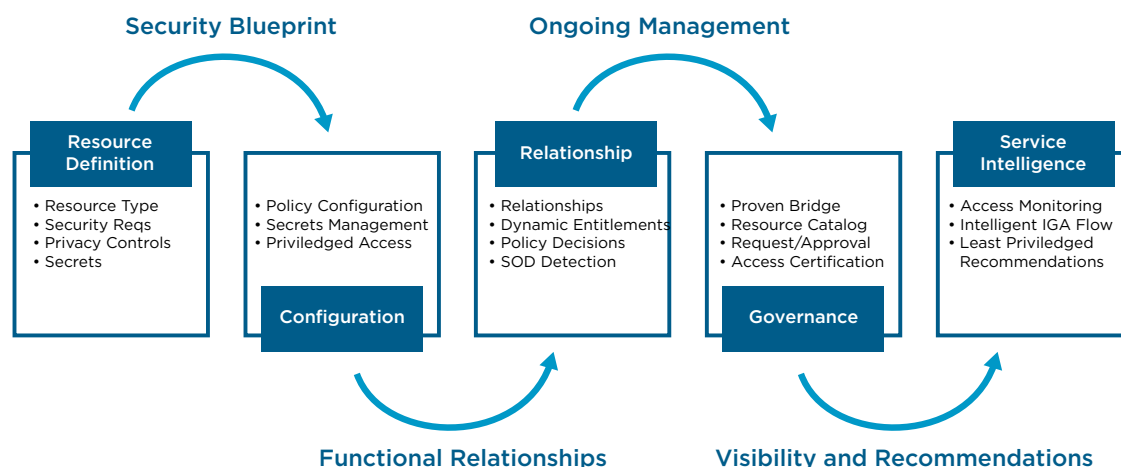
The physical perimeter no longer exists; Identity is the only universal perimeter. Therefore, identity and security must be everywhere by default.



Virtual relationships and physical micro perimeters (security silos) are the new reality, so you must be able to create and tear down relationships with consumers, partners, and employees dynamically, and to do this, we need to bridge today's "as-is" environments and tomorrow's "to-be" environments, securely.

Building Your Identity Fabric for the DevOps World

In addition to the micro perimeters, the modern applications are built in a continuous development and continuous innovation manner, and the dynamic nature of this approach is that your traditional IAM technologies must be able to integrate and support the new DevOps ecosystem. The IAM services needed to support identity interoperability and session management must be automated and consumable as microservices.

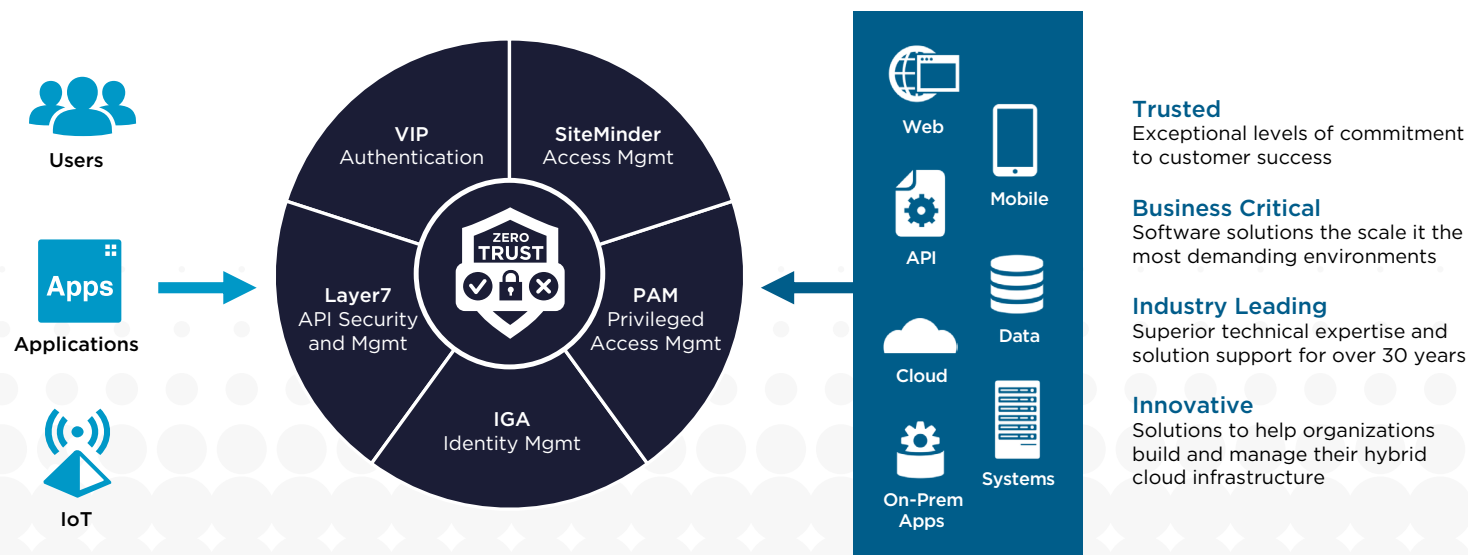


This requires a fundamental shift in your security architecture as your identity fabric must bridge both the modern and traditional applications and environments, and herein introduces the dilemma: Do I create a new identity silo or enhance my legacy IAM to handle my new challenges, or can I do both?

Do I create a new identity silo or enhance my legacy IAM to handle my new challenges, or can I do both?

The Next Evolution of our Identity Fabric Portfolio.

The Identity Fabric by Broadcom has been protecting organizations for the past thirty years, and is focused around five core technology areas.



Broadcom has created the Security Services Platform, which delivers both new business and shared services to our traditional IAM technologies.

The Next Evolution of our Identity Fabric Portfolio

To extend the capabilities and adapt to the requirements of the modern applications and environments, Broadcom has created the Security Services Platform, which delivers both new business and shared services to our traditional IAM technologies. The initial focus of this platform is the Symantec® VIP Authentication Hub.



1 Risk-based authentication with support for various factors including Mobile OTP/Push, SMS and FIDO



2 Native integration with SiteMinder®, VIP, and Advance Authentication



3 API-driven, enabling total control and customization of the end-user experience



4 Intelligence Engine connected to the Global Intelligence Network from Symantic



5 Standards Support including OIDC, SAML, and OAuth simplifies intergrtion with thrid-party services



6 Cloud-native architecture deploys in minutes, scales as needed, and updates with zero downtime



7 DevOps and Operations friendly K8S, Helm Charts, Kafka Grafana, etc.

LEARN WHAT'S POSSIBLE WHEN YOU MODERNIZE YOUR IDENTITY FABRIC.

LEARN MORE TODAY.

[BROADCOM.COM/SYMANTEC-IAM](https://Broadcom.com/Symantec-IAM)



About Broadcom

Broadcom is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, please visit our website at: www.broadcom.com

Copyright © 2023 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

November 2, 2023