EBOOK

KNOWING ME, KNOWING YOU

The Importance of Identity Security in Zero Trust

BROADCOM®

The Shift to an Anywhere, Any Device Workforce

During Covid, we witnessed a huge shift in the number of employees working from home.

This caused strain on many organizations as they suddenly needed to extend their security beyond its normal limits—but this was just a temporary imposition, or was it? Turns out employees liked the work-from-home approach and are in no hurry to return to the office.

A recent GitLab study[1] found that:

1 in 3

respondents would quit their job if remote working was no longer an option.

52%

would consider leaving their co-located company for a remote role.

82%

claimed that remote work is the way of the future.

But for organizations grappling with this new reality, there is hope. Zero Trust is built to support the anywhere, any device workforce.

1: GitLab All Remote Work Report 2021

BROADCOM

Employees liked the work-from-home approach

The Importance of Identity Security in Zero Trust

Zero Trust is a data-centric security architecture that is founded on the belief that an organization should not automatically trust anything inside or outside its perimeters, and must verify everything trying to connect to its resources before granting access. This access is based on identity, context, and trustworthiness.

To adopt Zero Trust, many different security tools and technologies are required, each designed to protect a specific area or attack vector. The glue that brings all of these together is identity, as demonstrated in the three basic tenets of Zero Trust:

1 Positively Identify Every User and Device Requesting Access

2 Enforce Least Privileged Access for Authorization Decisions

3 Apply Intelligence to Achieve Continuous Verification Process

BROADCOM

Identity is the glue that brings security silos together to achieve Zero Trust.

Strong authentication provides a greater confidence that users are who they claim to be.

Authentication Is Nice, but Is It Enough?

The first basic tenet of Zero Trust is to verify the identity of every user and device requesting access to an application, data, or system in your environment.

Being able to positively identify legitimate users from fraudulent ones is an important first step to achieving Zero Trust, and it is even more critical when the majority of your users are working remotely. They are coming in from the Internet, and increasingly using unmanaged devices.

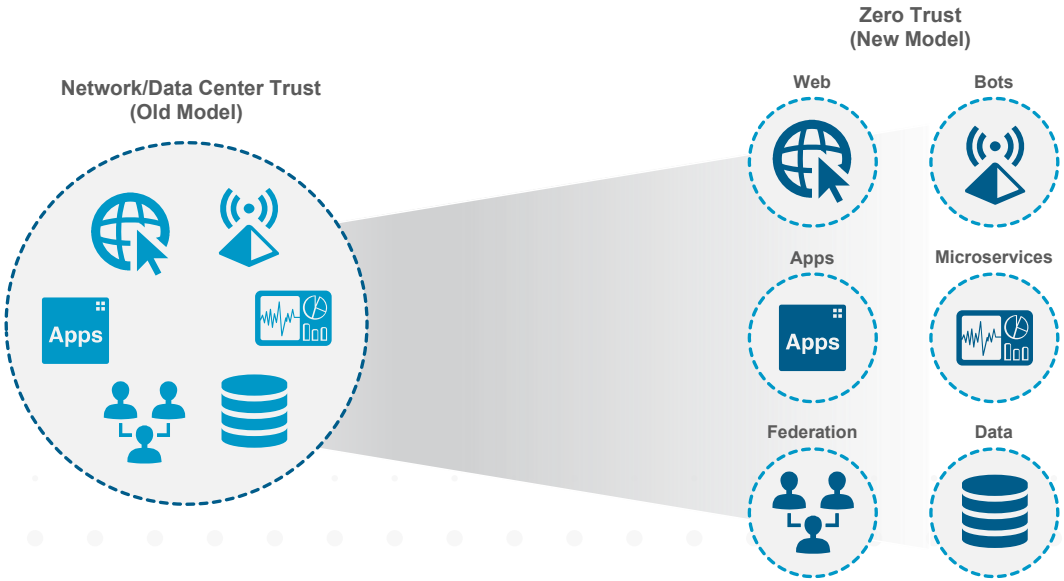
Strong authentication that combines multifactor credentials and contextual risk analysis provides greater confidence that users are who they claim to be. Additionally, device fingerprinting is a part of many authentication processes, as this not only uniquely identifies the device but also associates it with the user. But is this enough? Does Zero Trust begin and end with just authentication?

67% of employees use personal devices at work[1]

1: https://techjury.net/blog/byod-stats/#gref - March 2022

How Many Front Doors Do I Have to Protect?

Historically, the enterprise had one perimeter that protected the data center; enabling remote access to the network and the vast majority of corporate resources was fairly straightforward. Defense tools, such as VPNs and firewalls, combined with multifactor credentials, worked quite well to enable access to a limited number of remote workers. However, these technologies were not designed to handle the significant number of remote workers that we saw during the pandemic, and what is now becoming the new normal.



Modern SaaS, IaaS, and PaaS environments have created virtual relationships, and physical microperimeters, such as security silos, are also challenging traditional perimeter tools, but these can be augmented by new cloud-based, software-defined perimeter technologies. However, with the physical perimeter broken, identity is the only universal perimeter. Therefore, identity must be managed everywhere by default.

BROADCOM

Upgrade perimeter defenses to handle a larger remote workforce and hybrid environment.

Enterprises remain riddled with "Overprivileged" users[1]

Enforcing Least Privileged Access in Two Acts

The second principle of Zero Trust is to ensure least privileged access, and this is primarily done in two phases.

Once remote users are authenticated and granted initial access, they will begin to engage with corporate resources. At this time, various authorization engines will evaluate their request, and will grant or deny access based on policies. Authorizations consider the user's identity, profile attributes, roles, group memberships, and other contextual data. As the user attempts to access increasingly sensitive resources, more scrutiny should be made before access is granted. This is the active, or real-time enforcement of least privileged access to ensure that only authorized users gain access to specific applications and data.

The second, and most critical, place where least privileged access should be implemented is the attestation of user access entitlements. Regardless of how access was given to a user, these entitlements need to be routinely reviewed and certified to confirm that this level of access is still needed. This is the passive enforcement of least privileged access, to ensure that users are assigned only those entitlements they need to perform their job—no more, no less.

Combined, the active and passive enforcement of least privileged access is important, but is simply not enough. In the past year, we have witnessed unparalleled numbers of workers changing jobs. How many of these workers still have access entitlements and orphaned accounts within their old companies?

1: Darkreading.com / Threats / Insider Threats – March 2021

Behavior analytics detect abnormal activity and automatically trigger mitigating actions to minimize risk.

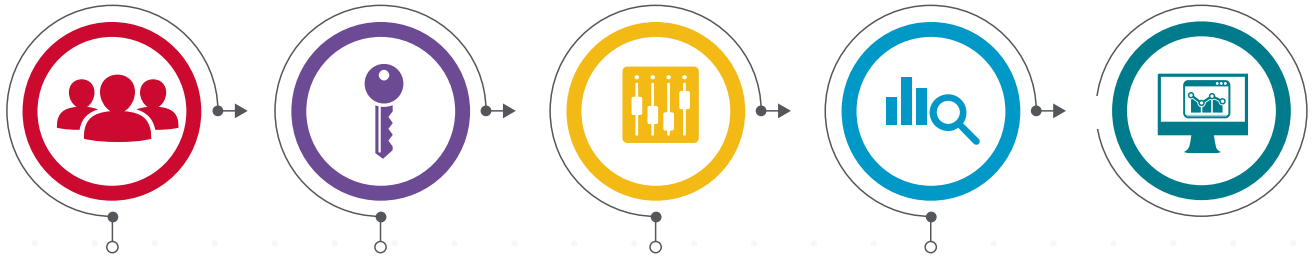
Combating the Insider Threat

External hackers will target internal users, compromising their credentials and taking over their accounts to penetrate perimeter and internal defenses. Additionally, organizations must also fear the insider threat – whether it be initiated maliciously or accidentally. In both cases, authorization engines struggle because the actor is leveraging access privileges that were appropriately assigned to the original user. To detect this threat, intelligence is needed.

User and Entity Behavior Analytics (UEBA) tools enable you to monitor user actions and activities and model normal behavior based on usage patterns. Over time, internal users will exhibit daily patterns that are nearly impossible to mimic by an external hacker. In fact, an external hacker will not even attempt to mimic the user. Additionally, when an internal user turns malicious, they will also begin to exhibit out-of-pattern behavior that can be easily detected. These UEBA tools continuously assess a user's current activities and compare them to their own historical actions, as well as to the behavior of other users, to accurately identify attacks and high–risk activities. With this data, these tools can alert the authorization engines to automatically take steps that mitigate risk. This is especially critical for accounts that have elevated or privileged access.

The Critical Capabilities of an Identity Fabric

In order to align your Identify 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.



1 Positive **AUTHENTICATE** users trying to **access** apps and data

2 Continuously **AUTHORIZE access** based on risk and data sensitivity

3 Automatically **ALLOW, ADJUST, OR BLOCK access** to mitigate attacks

4 **MONITOR access** to recognize risky activity patterns

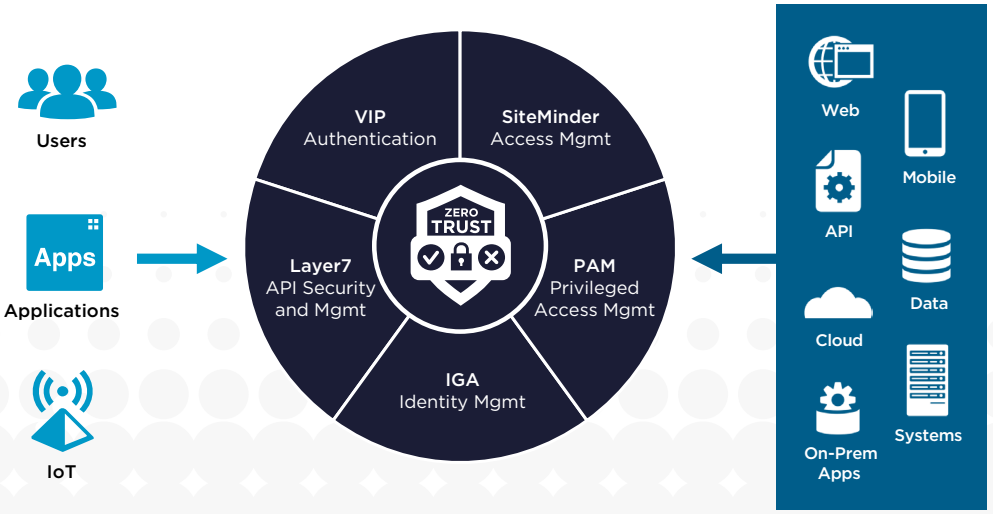
5 Manage and govern **ENTITLEMENTS** to ensure right level of **access**

Risk-Aware, Contextual Access Management to Enable Business Growth while Protecting from Attacks

Most organizations have been deploying IAM technologies for the past twenty years or more, but are now struggling to adapt these platforms to modern applications and environments. But why create a new identity silo when you can build upon what you already have?

A Modern Identity Fabric Portfolio

The Broadcom® Identity Fabric has been protecting organizations for the past 30 years, and is focused around five core technology areas:



Trusted
Exceptional levels of commitment to customer success

Business Critical
Software solutions the scale it the most demanding environments

Industry Leading
Superior technical expertise and solution support for over 30 years

Innovative
Solutions to help organizations build and manage their hybrid cloud infrastructure

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 **Advanced Authentication** with SiteMinder, VIP, and VIP Authentication HUB

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

4 **Intelligence Engine** connected to the Global Intelligence Network from Symantic

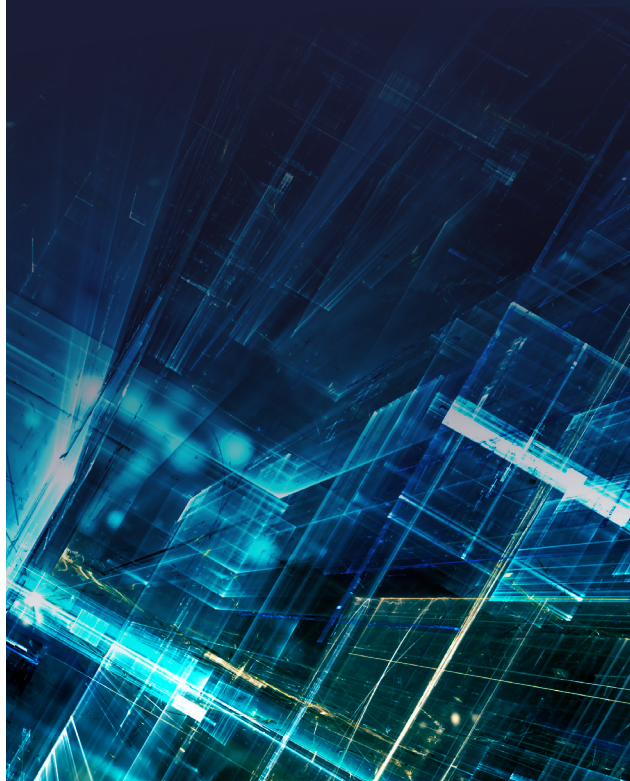
5 **Standards Support** including OIDC, SAML, and OAuth simplifies intergrtion with thrid-party services

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.

BROADCOM

The Security Services Platform delivers new services to our traditional IAM technologies.



Leverage Existing IAM Investments and Modernize

With a Zero Trust architecture and a modern Identity Fabric, you can support the remote workforce. This means that you can securely enable access to any corporate application, sensitive data, and critical system to any user, regardless of where they are located or what device they are using. But does this mean that you need new security tools and technology?

Not necessarily. Some traditional perimeter defense tools, such as VPNs and firewalls, may not be able to deal with modern SaaS, IaaS, and PaaS environments, but these can be augmented by new cloud-based, software-defined perimeter technologies. Your existing IAM platforms should serve as the foundation that glues together your traditional perimeter with the new microperimeters. Additionally, your IAM platforms can be similarly enhanced to adapt to new use cases, standards, and ecosystems.

The Broadcom Zero Trust Architecture combines the best of both worlds: market-leading and proven IAM that is being modernized with our Security Services Platform, combined with the Symantec Cloud Security portfolio to provide a comprehensive platform.

Why Broadcom?

AN **ENGINEERING CULTURE** FIRST AND FOREMOST

80+%
of our workforce is dedicated to R&D and operations

14%
invested in R&D vs. 11% industry standard

3,200+
software-related patents

ENABLING SCALABILITY, AGILITY, AND SECURITY

A **WORLD-CLASS** ENTERPRISE SOFTWARE BUSINESS

$5B+ in annual revenue

96% customer satisfaction rate

LEARN HOW TO PROTECT YOUR REMOTE WORKFORCE WITH OUR IDENTITY FABRIC.

LEARN MORE TODAY.

BROADCOM.COM/SYMANTEC-IAM

BROADCOM®
connecting everything®

About Broadcom

Broadcom Inc. (NASDAQ: AVGO), a Delaware corporation headquartered in San Jose, CA, is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise, mainframe and cybersecurity software focused on automation, monitoring and security, smartphone components, telecoms and factory automation.

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

KnowingMeKnowingYou-eBook-1123 November 16, 2023