Symantec™
A Division of Broadcom

Knowing Me, Knowing You

Leveraging Identities to Empower the Modern Workforce

Shifting to an Anywhere, Any Device Workforce

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

BEFORE COVID-19

31%

working from home on a regular basis[1]

AFTER COVID-19

88%

working from home on a regular basis[1]

This caused strain on many organizations; trying to extend their security beyond its normal limits — but, in a Zero Trust Model, this is the expected norm.

Zero Trust is built to support the anywhere, any device workforce.

[1] Global Work-From-Home Experience Survey, Global Workplace Analytics, May 2020

Zero Trust is a Fundamental Shift in Security Approach

Zero Trust is a data-centric security architecture built upon three basic tenets — organizations must:

1 Verify Every User Requesting Access

2 Validate Every Device Requesting Access

3 Enforce Least Privileged Access

The Zero Trust model is founded on the belief that organizations should not automatically trust anything inside or outside its perimeters and must verify everything trying to connect to its resources before granting access — based on identity, context and trustworthiness.

In the COVID scenario, traditional perimeter defenses, such as firewalls and VPNs, were not scaled to handle the large number of employees suddenly forced to work remotely; however, within the Zero Trust approach, the security is designed to handle any user connecting from any device from any location.

The Importance of Identities in Zero Trust

Leveraging Multifactor Authentication to positively identify users to prevent unauthorized access to corporate apps, systems, and data.

1 Omni-channel Experience

Leveraging Device Fingerprinting and Identification to increase trust for known devices and decrease it for unknown ones.

2 Secure Digital Identity

Leveraging Identity Governance to routinely review and certify access entitlements to ensure least privileged posture is achieved.

3 Trusted App Experience

Authentication is Nice, but is it Enough?

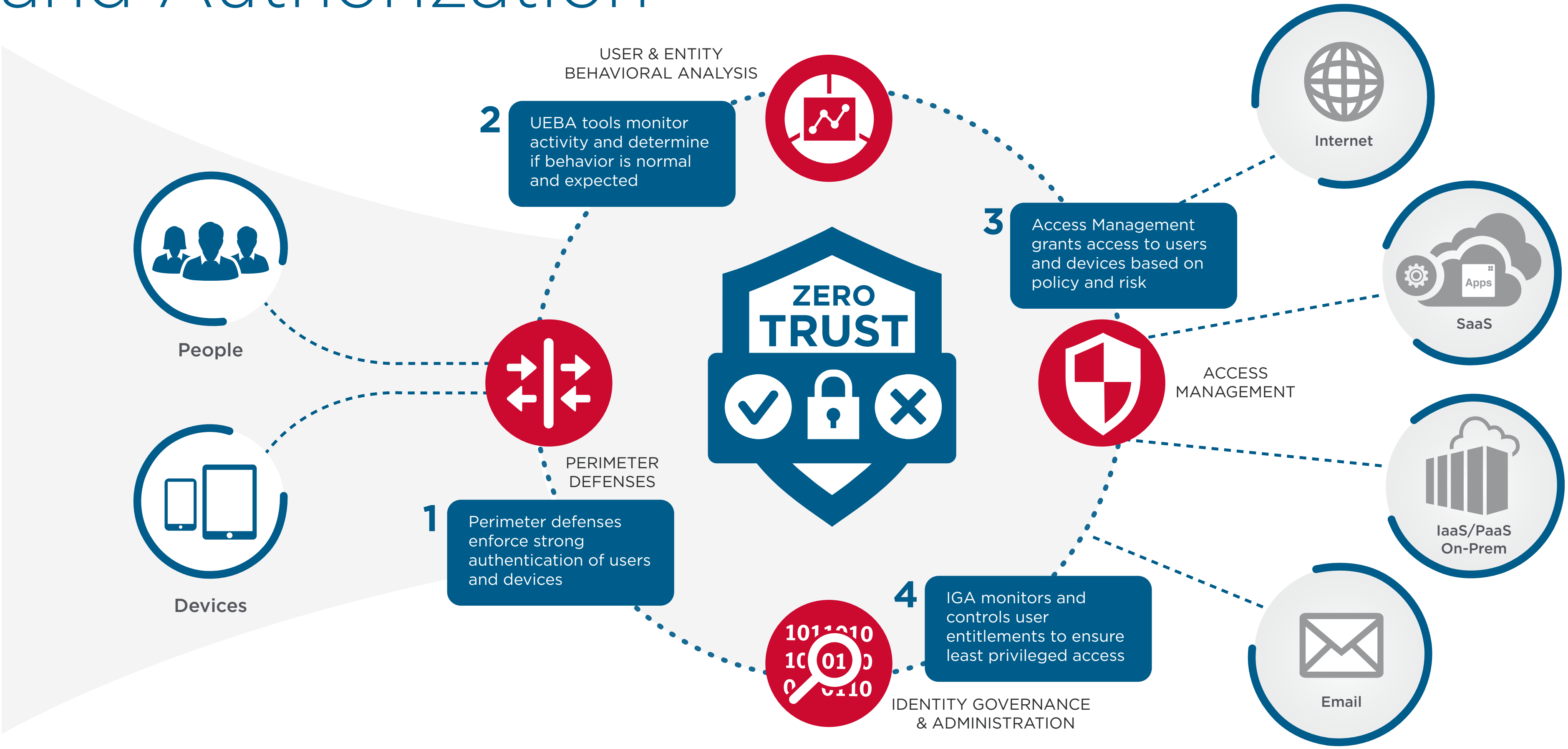
The first basic tenet of Zero Trust is to verify the identity of every user requesting access to an application, data, or system in your environment.

Strong authentication that combines multifactor credentials and contextual risk analysis provides greater confidence that users are whom they claim to be.

The second tenet of Zero Trust is to validate every device that is used to access applications, data, or systems. In many cases, device fingerprinting and identification is a part of many strong authentication processes. Additionally, many organizations have also adopted endpoint security solutions to further protect devices from being compromised.

But is this enough? Does Zero Trust begin and end with just authentication?

Zero Trust Requires Authentication and Authorization



1 Perimeter defenses enforce strong authentication of users and devices

2 UEBA tools monitor activity and determine if behavior is normal and expected

3 Access Management grants access to users and devices based on policy and risk

4 IGA monitors and controls user entitlements to ensure least privileged access

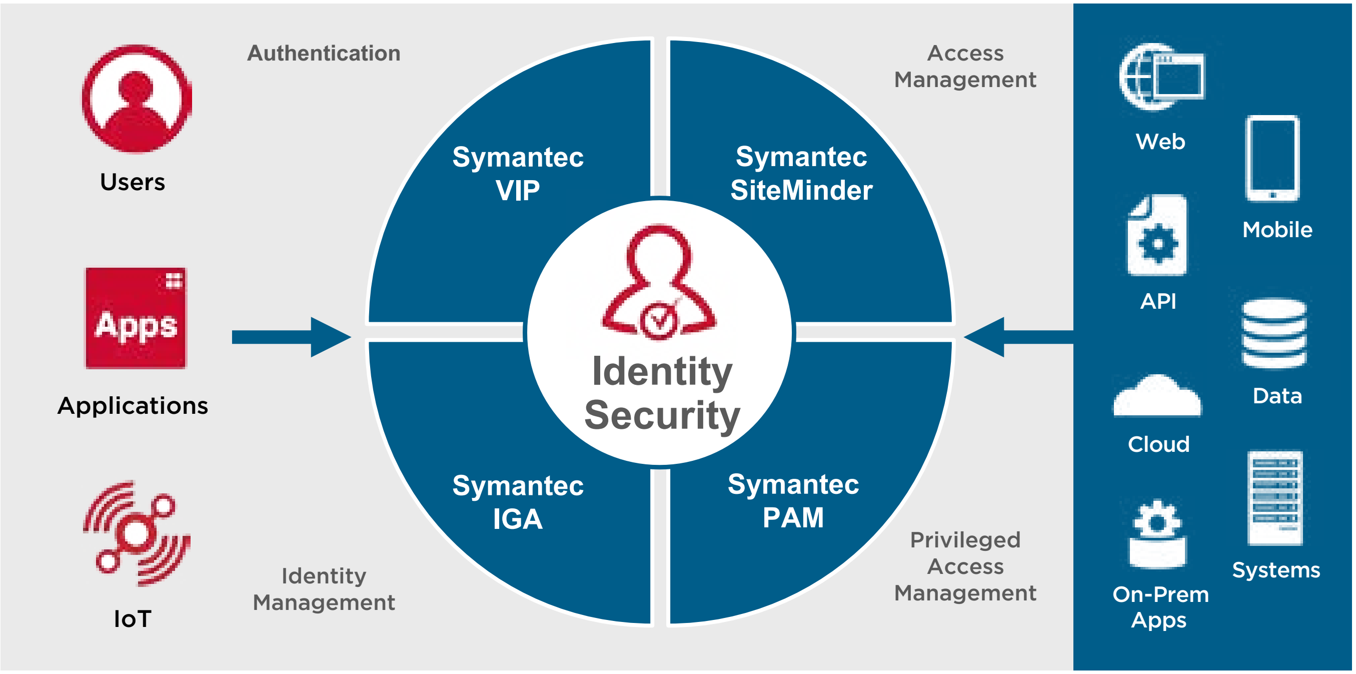
Leveraging Existing IAM Investments & Modernize

Zero Trust is modern. With a Zero Trust architecture, you can support the modern workforce, which means that you can enable secure access to any corporate app, data, or 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. Similarly, your existing IAM platforms can integrate with these newer perimeter tools to continue to perform the verification and validation of users and devices, and grant access to resources.

Symantec Zero Trust combines the best of both worlds – market-leading IAM with modern cloud security to provide a comprehensive platform.

Symantec Identity Security



Endpoint Security

The critical last line of defense in protecting user devices from cyber attacks.

Network Security

Security solutions to protect the essential email and web access with advanced threat protection.

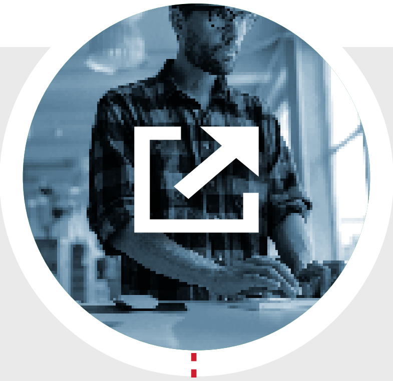
Information Security

Cloud security solutions to help organizations protect their data wherever it resides.

One pillar of the Symantec Zero Trust Platform

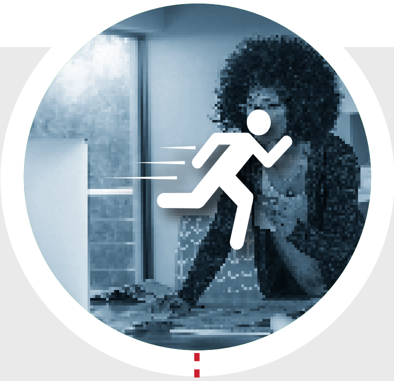
Why Symantec Identity Security

Protecting the World’s Largest Enterprises for over 2 Decades



1. **Distributed** Use Cases

Any vendor can handle the easy use cases, but the modern enterprise must also address the complex use cases.
No one can address these like Symantec.

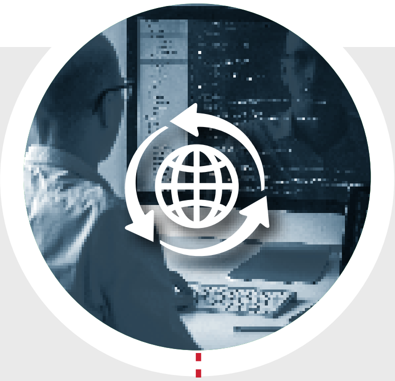


2. Quick **Adaptability**

Helps you launch new applications and increase your capacity no matter how complex your environment so that you can respond to the pressures of your business in real time.

3. Performance & **Scalability**

Built for your demanding workloads whether it’s millions of users, hundreds of applications, or billions of devices or transactions. Our solutions ensures that you maintain performance at scale while minimizing the cost of deployment and operation.



4. **Complete** Platform

Delivers a layered, defense - indepth identity and access management platform that helps you implement a zero trust model while making it easy for your customers to do business with you.

See what's possible when your Zero Trust Platform is built on Identity Security

LEARN MORE TODAY.
BROADCOM.COM/SYMANTEC-IAM

Symantec™
A Division of Broadcom

For product information please visit our website at: broadcom.com

BC-0598EN August 2020