SOLUTION BRIEF

ADVANCE YOUR ZERO TRUST STRATEGY WITH A TRUSTED PARTNER

The Zero Trust framework is designed to help organizations transform their entire approach to security, adopting a combination of new processes, technologies, and mindsets to protect their networks and enable continuous monitoring across environments.

Whether your organization is new to the world of Zero Trust or looking to advance its existing strategy, Broadcom is here to serve as your trusted partner.

The Broadcom® software portfolio includes end-to-end Network, Identity, and Information Security software designed to deliver unparalleled visibility and enable continuous verification of users, devices, and assets on-premises and in the cloud.

Our agile software enables our customers to seamlessly integrate modern, agile cloud solutions with their existing on-premises technology stack on their journey to support distributed work, protect business-critical assets, and implement a Zero Trust security strategy at scale.

Continuously Monitor Network Activities in the Zero Trust Security Framework

Four Ways to Implement Continuous Network Monitoring for Your Organization

Overview

Zero Trust methodology asserts that organizations must adopt a "Never Trust, Always Verify" approach to cybersecurity. As technology architecture becomes more complex and cyber threats get smarter, ongoing network monitoring is critical to authenticate users and protect sensitive assets.

To keep up with business operations, IT teams need end-to-end monitoring solutions that provide continuous visibility into users, devices, and activities across environments.

In the Zero Trust model, network administrators need the ability to monitor their networks in real time in order to authorize users, flag suspicious activities, and protect their enterprises from threats. Here are several ways to enable constant network monitoring across your organization's IT infrastructure.

1 Think Outside the Perimeters

What users, devices, and entities are interacting with your environment? Can they be inspected? What exactly are they accessing? Zero Trust urges organizations to prioritize the answers to these questions and ensure they have complete visibility into every user, device, and application interacting with their networks.

In the Zero Trust framework, your organization should prioritize all-around visibility and protection by operating perimeterless. Rather than assuming users will pass in or out of finite barriers, like login pages and other defined access points, implement Network Security software that proactively monitors your entire infrastructure and gives your team unparalleled visibility into ongoing activities.

Network security solutions should include features to protect both on-premises and cloud-based systems:

- Secure web gateways
- Advanced threat protection
- Encrypted traffic management
- Messaging security
- Zero Trust network architecture (ZTNA)
- Cloud access security broker (CASB)

Do not waste another second monitoring perimeters and tracking down access paths. The Zero Trust perimeterless approach to security provides comprehensive visibility and protection, improving IT efficiency and safeguarding critical assets from internal and external threats.

2 Analyze Digital Behavior Patterns

Because Zero Trust provides access by request and enables continuous monitoring, every user action is documented. Over time, your organization can gather behavioral data about privileged users and leverage it to accelerate your automated threat response time.

Examples of data-driven insights include the following metrics:

- Time measurements of user activity
- Which applications are frequently accessed
- How users leverage frequently accessed applications

When current activity conflicts with historical data, your Identity Security software should proactively alert you to suspicious behaviors or changes in routine. Real-time response systems react to this and shut down access before the threat can go any further.

Analyzing digital behavioral patterns and using automated software to flag anomalies is one of the best things your organization can do to stay ahead of cyber threats and maintain trust with privileged users.

3 Conduct Frequent Risk Assessments

Frequent risk assessments are your organization's best chance at catching vulnerabilities or detecting threats before it is too late. The current industry standard is to conduct risk assessments on a rotating schedule (quarterly, annually, etc.) or in response to technology changes. Unfortunately, this process has aged out with the rapid adoption of cloud technologies.

In the Zero Trust framework, you can leverage Network Security software to essentially conduct a risk assessment with each access attempt. Rather than a periodic, sweeping assessment across your entire environment—almost guaranteeing something will be missed—real-time risk assessment covers end-to-end access management.

This continuous assessment process goes deeper than other risk assessment methods. Verified users must navigate robust security measures to access the network—making it nearly impossible for unauthorized users to gain entry. If a threat does somehow get through, their access permissions are still at the lowest level, reducing the impact of the breach. The information they access will be encrypted and indecipherable without the corresponding keys, rendering their attack fruitless.

4 Create a Robust Response Architecture

No matter how sophisticated your protective measures are, there is always a chance that a threat may break through. That is why it is critical to have robust response architecture ready for unforeseen incident responses.

Zero Trust's role in developing a response architecture is the wide variety of data it provides. You won't have to waste time seeking vulnerabilities within the architecture—you will already know.

Follow these response architecture development best practices:

- Enable real-time information collection to ensure threat response is immediate.
- Prioritize which instances trigger an automated threat response.
- Check and ensure all systems are updated to their latest patch.
- Determine if threat response should be content-agnostic or broken down by access permissions.

Think of your response architecture as your first line of defense against threats. By ensuring the upkeep of cyber hygiene as it relates to response architecture, your organization can respond as quickly as possible.

Connect with our sales team to discover how Broadcom can support your Zero Trust strategy with software that modernizes, optimizes, and protects your business from the data center to the edge.

BROADCOM®
connecting everything®

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

ZT-CMNA-SB100 November 8, 2023