BROADCOM SOFTWARE

# CHECKLISTS
# DELIVERING STRONG USER EXPERIENCES IN THE ZERO TRUST SECURITY FRAMEWORK

## FOUR WAYS TO MITIGATE CYBERSECURITY RISKS WITHOUT COMPROMISING USER EXPERIENCE

As organizations' IT infrastructures become more complex and decentralized—through hybrid or multi-cloud strategies, distributed work, and digital transformation—they are embracing the Zero Trust security framework to govern and protect their business-critical assets.

Zero Trust asserts that organizations must adopt a "Never Trust, Always Verify" approach to cybersecurity by continuously monitoring, authenticating, and securing every resource across applications. But each new security measure an organization introduces has the potential to disrupt users' experiences as they interact with their network.

If your organization does not take an intentional approach to user experience, Zero Trust implementations can create new usability challenges for your employees, contractors, and guest users operating across on-premises and cloud-based environments.

A well-implemented Zero Trust strategy should strengthen your cybersecurity posture and support your end users simultaneously. In a Zero Trust architecture, your organization can use behavior-based, personalized solutions to extend access to trusted users while simultaneously protecting your network from hackers and other cyber threats.

Here are several ways to prioritize user experience as you develop and implement your organization's Zero Trust security strategy:

### 1 ADOPT PERIMETER-LESS SECURITY SOLUTIONS

Your organization may rely primarily on perimeter-based security—like point solutions and VPNs—to protect critical infrastructure in on-premises data centers. However, these solutions simply do not translate to the dispersed, perimeter-less nature of hybrid and multi-cloud infrastructures — including the on-premises data centers.

Point-based security leaves critical gaps in your cybersecurity posture by operating under the assumption that there is a defined perimeter around your network that hackers must breach in order to pose a threat. Attempting to achieve Zero Trust through a multi-point approach only increases integration complexity and leaves your organization exposed to significant risk in the space between point products.

VPNs and similar encryption tools often create challenges for end users, draining battery life on their devices and limiting access to business-critical applications and systems since they do not integrate with identity management solutions.

As you develop a Zero Trust architecture, integrate finite point-based security solutions with network security solutions purpose-built for the complexities of remote work and hybrid cloud operations.

Network security solutions provide unparalleled visibility into how, when, where, and by whom resources are being accessed across your entire organization. Monitor and protect critical assets in the mainframe, in the cloud, and everywhere in between with continuous monitoring, web security, and email security solutions that will not disrupt your users.

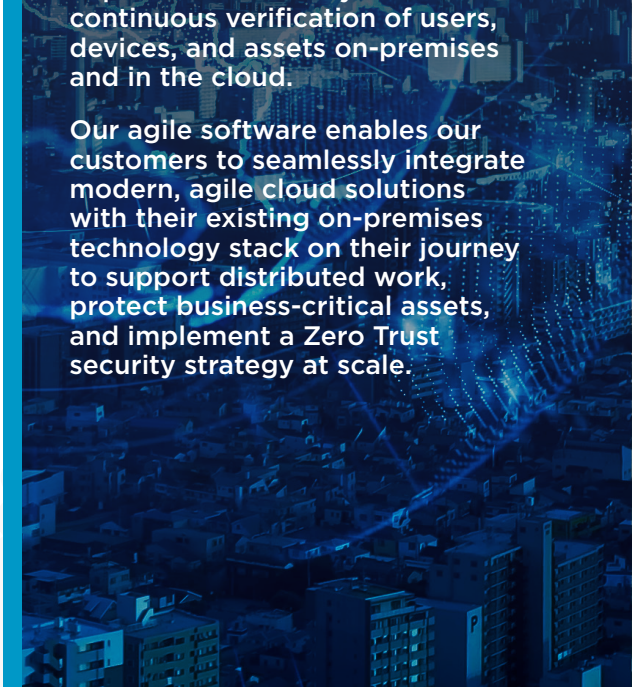
## Advance Your Zero Trust Strategy with a Trusted Software Partner

**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® Software is here to serve as your trusted software 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.**



# CHECKLISTS

## 2 IMPLEMENT IDENTITY-BASED SECURITY MEASURES

Businesses rely on multi-factor authentication (MFA) and single-sign-on (SSO) solutions to authenticate users as they attempt to access applications and data across environments. These solutions are especially applicable in distributed work environments where users may need to access secure networks through a personal device or switch between multiple devices on a routine basis.

However, when applied to a Zero Trust architecture, MFA and SSO solutions create a redundant, disjointed user experience. They require that your users manually confirm their identity each time they move between applications or request access to privileged assets within your network. The result is a frustrating, repetitive process that takes time away from business-critical tasks and disrupts users' daily workflows.

Use identity-based security solutions alongside MFA and SSO to validate users through a single interaction. Then, continuously monitor and authenticate their activities as they move throughout your network.

Identity-based solutions are rooted in identity, credentials, and access management (ICAM), an approach to cybersecurity that focuses on authenticating a user's identity instead of simply verifying their credentials at each point of entry. ICAM facilitates continuous authentication activities and integrates with technologies like MFA and SSO to safely store digital identities and profile data.

These solutions also make authentication significantly less disruptive for your end users. Identity-based authentication technology operates in the background, safeguarding your network and its users from threats without disturbing your employees, contractors, or guest users.

## 3 STAY AHEAD OF NETWORK PERFORMANCE ISSUES

Inconsistent network performance poses multiple risks to your organization, from revenue lost as a result of system downtime to security threats that may go undetected if critical monitoring systems fail. Additionally, performance issues directly impact the users who work within your network every day. They may be unable to complete business-critical tasks, connect with peers, or access data in a timely manner.

Your end users' experiences will suffer not only from the performance issues they encounter but also from the time and effort it takes them to troubleshoot and resolve them. Users may spend hours tracking down the appropriate documentation, reaching out to your help desk, or simply waiting for an update from your IT department—all resulting in lost productivity and poor sentiment.

Do not wait for performance issues to impact your business and its users. Deploy proactive monitoring solutions that leverage artificial intelligence and machine learning to detect and mitigate network performance concerns before they slow down your operations.

AI-powered network performance monitoring software can help you remediate performance issues before they impact your users and your organization's productivity. Instead of spending hours tracking down the cause of slowdowns and other concerns, you will gain the insight you need to identify, isolate, and resolve errors quickly and effectively.

## 4 MAKE SECURITY AN EASY CHOICE FOR USERS

Your cybersecurity team should strike the right balance between easy user access and advanced security controls. A breach may occur if your organization's data, services, and applications are too easily accessible. But if assets are too restricted, users may disregard certain security requirements in order to complete their jobs within your organization.

You might assume that Zero Trust will push your organization too far toward stringent, tough-to-follow security regulations that ask too much of your end users. However, you can bring transparency and convenience to users' cybersecurity experience with the right combination of user-friendly tools and clear, accessible guidance.

Start by increasing communications between your cybersecurity department and the rest of your organization. Then, keep end-users informed on how ongoing changes to your technology stack and Zero Trust implementation strategy will impact their experiences across applications and environments.

### HOW TO START DISSOLVING THE IT-UX BARRIER

- Develop a Privacy and Data Use Policy that is easy to access, navigate, and understand for even the least-technical users working inside of your network.
- Provide clear guidance on password requirements, device usage policies, data sharing restrictions, and other potentially risky business processes—and update these documents regularly.
- Proactively alert users about updates to UI, functionality, and any frontend changes to applications or systems that may affect their experiences.

Helping your end users recognize their role in your organization's Zero Trust strategy empowers them to make intelligent, informed decisions about privacy and security. They will inherently gain a better understanding of what is at risk and how they, their colleagues, and your organization as a whole protect vulnerable information.