TRENDS REPORT

Advance Enterprise Security Beyond the Perimeter

BROADCOM SOFTWARE

TABLE OF CONTENTS

Trends and Opportunities Inform How Organizations Authorize Users and Devices in the Zero Trust Framework

Across industries, enterprises are accelerating Zero Trust implementation to strengthen their cybersecurity posture, adapt to evolving business landscapes, and support the modern workforce.

Zero Trust's central message, "Never Trust, Always Verify," requires that these organizations take a proactive, least-privilege approach to user access and authentication across applications and internal systems. However, factors like remote work and hybrid, multi-cloud environments introduce new challenges for IT and security professionals looking to verify users' identities and authorize devices on a continuous basis.

Security teams must monitor multiple credentials, applications, environments, devices, and work locations, all of which open the door to unique threats and vulnerabilities like phishing and other data breach practices.

Trends Shape the Role of Device and Access Management in Zero Trust

As organizations develop Zero Trust implementation strategies and identify their most critical security needs, several trends and opportunities influence their decisions:

Distributed Work is Increasing Security Risks

Upwork's 2019 Future Workforce Study found that **seventy-three percent of all departments will include remote employees by 2028.** This shift offers new opportunities for agility and business growth. Unfortunately, it also poses significant cyber risks as users operate on multiple devices and networks simultaneously, leaving a much larger attack surface for cyber criminals to prey upon.

Cloud is Pacing Innovation and Complexity

According to the Flexera 2022 State of the Cloud Report, **eighty-seven percent of enterprises** have already adopted hybrid cloud strategies to enable rapid innovation and scalability. However, hybrid and multi-cloud infrastructures are complex to protect and maintain. The IT teams that manage them must secure assets on-premises and in the cloud without disrupting operations or hindering end users' experiences.

Identity-Based Cyber Attacks are on the Rise

The Identity Defined Security Alliance's (IDSA) 2022 Trends in Securing Digital Identities white paper reports that **eighty-four percent of organizations experienced an identity-related attack in 2021.** Experts theorize this uptick in attacks will persist as employees are asked to manage upwards of 30 identities—or sets of login credentials—across applications and cyber criminals hone in on high-value credentials of privileged users.

Improve Device Management Across Environments

Develop Detailed Access and Device Use Policies

To accompany their rapid shifts to remote or hybrid work, organizations must develop clear, security-focused device management policies to protect their employees, customers, and IT infrastructure from potential breaches.

Bring-your-own-device (BYOD) and use-your-own-device (UYOD) models are popular but require specific security controls to ensure security teams can identify, monitor, and secure devices remotely. Even if employees use company-issued devices, enterprises need to invest in remote access and security solutions to ensure IT teams can detect and resolve issues from anywhere, at any time.

INVEST IN REMOTE ACCESS AND SECURITY SOLUTIONS TO ENSURE IT TEAMS CAN DETECT AND RESOLVE ISSUES FROM ANYWHERE, AT ANY TIME.

Collaborative IT teams and operations stakeholders align on an enterprise-wide device-use policy and supporting software. Then, they must develop accessible documentation to ensure end users know how to manage their devices, whether they are working remotely or on-site.

Effective training enables even the least-technical team members to follow pre-defined security policies and help them understand their role in securing company assets.

Reinforce Endpoint Security Measures

Organizations can easily establish standard operating environments when teams primarily worked in finite physical office spaces. However, distributed work—whether across global offices or employees' preferred work-from-home locations—has exponentially increased the scope and complexity of IT infrastructures and associated enterprise security concerns.

Remote work and flexible device-use policies have made endpoint security more critical, and complicated, than ever. IT professionals need endpoint security software that closely monitors activities across all devices interacting with the network, including laptops, desktops, mobile devices, servers, applications, storage devices, and anywhere else data might reside.

IT teams benefit when endpoint security solutions provide comprehensive, real-time visibility into device activities, from users' login attempts across applications to the data being stored or transmitted to and from each device. These solutions must also give teams the ability to track security threats to their source and mitigate them efficiently through detailed activity reports.

Extend Monitoring Efforts Beyond the Data Center

Perimeter-less security is a central tenet of the Zero Trust framework. It urges organizations to evolve the perimeter-based approaches they use in the data center into strategies that account for the infinite nature of cloud-based applications.

Industry leaders in the IT and software spaces are establishing a new, less rigid perimeter: the software-defined perimeter (SDP). SDP technology goes beyond the data center, accounting for applications and workloads in the cloud as well as mainframes and other on-premises locations.

SDP solutions allow organizations to establish consistent security controls and accompanying policies across their entire infrastructure without compromising user experience or leaving gaps between the seams of point-based solutions.

THE ZERO TRUST FRAMEWORK URGES ORGANIZATIONS TO EVOLVE THE PERIMETER-BASED APPROACH TO ACCOUNT FOR THE INFINITE NATURE OF CLOUD-BASED APPLICATIONS.

A Zero Trust security model calls for organizations to employ end-to-end network monitoring software alongside point-based solutions to ensure seamless monitoring and protection across their hybrid cloud infrastructures.

Support Dynamic Authorization Through ICAM

A user's identity within an organization goes far beyond the login credentials they use to access an application, system, or trove of sensitive data. Even so, many employers ask their staff to manage an array of login credentials and multi-factor authentication (MFA) methods across systems to prevent data from falling into the wrong hands.

MFA and single-sign-on (SSO) solutions can help reduce the frequency of unauthorized network access. Still, most do not account for the multiple layers of each user's identity, like their geographic location, job title, typical behavior pattern, or list of trusted devices.

This Identity Fabric is critical in validating a user's identity and detecting unlawful attempts to use that identity as a means of skirting access controls.

As organizations secure endpoints and enhance monitoring efforts, they also need to implement an identity, credential, and access management (ICAM) policy that accounts for the complexities of each user's true identity.

Advance Your Zero Trust Security Strategy With a Trusted Software Partner

Device management is just one element of an effective Zero Trust security strategy. Successfully securing resources and users across complex environments can help organizations reduce cyber threats, simplify network monitoring, and better support their trusted users.

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 Endpoint, Network, Identity, and Information Security software designed to streamline access controls and enhance monitoring across on-premises and cloud applications.

Our agile software enables our customers to seamlessly integrate hybrid, 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.

Connect with our sales team today to discover how we can support your Zero Trust strategy with software that will modernize, optimize, and protect your business from the data center to the edge.

BROADCOM® SOFTWARE

About Broadcom Software

Broadcom Software 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 Software 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, visit our website at: software.broadcom.com

BSG-ZT-Network-Access-WP100 September 15, 2022 11:09 AM