BROADCOM SOFTWARE

WHITE PAPER

THE ROLE OF ICAM IN THE ZERO TRUST SECURITY FRAMEWORK

Enabling Continuous Identity Verification in Hybrid and Multi-Cloud Infrastructures

WHITE PAPER

The Role of ICAM in the Zero Trust Security Framework

BROADCOM SOFTWARE

TABLE OF CONTENTS

Enabling Continuous Identity Verification in Hybrid and Multi-Cloud Infrastructures

Enterprise-wide identity verification has always been complex. To protect their network from threats, IT teams must verify a continuous stream of users—each with varying access permissions—as they navigate multiple devices, systems, applications, and environments.

The disjointed nature of cloud-based software and an accompanying shift to remote work adds a new layer of complexity to identity and access management. This is especially true in hybrid and multi-cloud ecosystems.

As businesses embrace hybrid cloud strategies and Zero Trust security, advanced identity verification and authentication solutions are integral to protecting their most critical assets.

Zero Trust methodology asserts that organizations must adopt a “Never Trust, Always Verify” approach to cybersecurity. This includes continuous authentication of every user, device, and application that interacts with their networks.

Navigate the Complexities of Distributed Identity Management

As an organization expands beyond the perimeter base, disjointed identity management solutions can create critical gaps across its network. Hybrid and multi-cloud architectures, combined with distributed workforce operations, create a perfect storm of identity verification challenges that put sensitive data at risk and create frustrating user experiences.

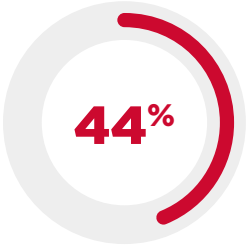
End users and IT professionals alike struggle to reconcile identities across systems. Employees, contractors, and other users must manage a unique set of credentials for each application they access.

CYBERSECURITY TEAMS CANNOT EFFECTIVELY DETECT AND MITIGATE THREATS WITHOUT A COMPREHENSIVE VIEW OF USERS' VARIOUS IDENTITIES.

At the same time, security teams must track users' paths of action between platforms to confirm their identities and monitor their activities. This approach is not just difficult to maintain; it also opens the door for bad actors, making it easier for them to exploit compromised account credentials and covertly conduct malicious activities.

Potentially serious red flags, such as one user attempting to access the network from two different countries simultaneously, may go unnoticed or unresolved since IT teams cannot correlate these events to one another in real time.

The likelihood of a cyber attack or data breach exponentially increases when employees leave the organization and are not de-provisioned correctly. Former employees may exploit their lingering credentials, or cyber criminals may discover and take over the still-active accounts.



In their 2022 Cost of Insider Threats Global Report, the Ponemon Institute found that

Insider threat incidents rose 44%

between 2020 and 2022, with annualized costs averaging $15.38 million.

Once these intruders make their way into the network they often move laterally, gaining access to other systems and evading SIEM solutions by appearing to be legitimate users.

Rather than combining application-level solutions to protect their networks, organizations should leverage identity verification solutions that unify user identities across devices, applications, and environments.

Create a Single Source of Identity With ICAM

Organizations should take a unified approach to identity management to support Zero Trust and enable continuous identity verification. They can do this by investing in solutions that verify users' true identities rather than simply verifying their credentials for an individual point of entry into the network.

A CENTRALIZED YET MULTI-FACETED VIEW OF EACH IDENTITY GIVES SECURITY TEAMS VALUABLE INSIGHT INTO THEIR TRUSTED USERS—AND THE CONTEXT THEY NEED TO SPOT UNUSUAL ACTIVITIES.

A comprehensive identity, credential, and access management (ICAM) policy emphasizes the value of a cohesive Identity Fabric and a single, unified identity for every user that spans on-premises and cloud applications.

These continually verified identities go far deeper than login credentials, accounting for users' locations, job titles, behavior patterns, trusted devices, and more. A centralized yet multi-faceted view of each identity gives security teams valuable insight into their trusted users—and the context they need to spot unusual activities.

An organization's Identity Fabric should be equal parts scalable and flexible. It should be supported by identity and access management software that allows them to expand unified identity verification quickly, matching the pace of innovation without compromising security.

As this Identity Fabric grows, security teams will gain extensive visibility into each user's true level of access across all systems, even if the systems themselves are not fully integrated.

Implement ICAM in the Zero Trust Security Framework

ICAM supports a Zero Trust architecture by giving the network administrator insight into every user or device attempting to access the network—including what level of access that resource needs or should be granted.

The right software is critical for verifying users' identities. Still, an effective ICAM policy also requires that security teams and end users rethink their approach to identity verification.

Reduce Reliance on Passwords

Excessive password usage can open the door to account breaches and unauthorized use of privileged credentials. The goal should be not to eliminate the existence of passwords entirely but to reduce the number of times users are required to enter their passwords when moving between multiple systems. Organizations can deploy single sign-on (SSO) solutions in tandem with identity-based security software to simplify verification and limit password entries across systems.

Instill Least-Privilege Access Controls

The more assets a user can access, the greater risk their identity poses if it falls into the wrong hands. In a least-privilege access model, user identities begin with no access to any systems in the network. Access is granted as needed, based on what that specific resource needs to complete their work. This ensures the appropriate level of access for privileged users and devices while limiting opportunities for bad actors to access critical assets by stealing a user's identity.

Use Risk Scoring to Assess Potential Threats

Risk assessments leverage the User Entity Behavior Analysis (UEBA) methodology to calculate each user's potential risk to an organization based on their behaviors and deviations from security standards. Risk scores range from zero to 100, with 100 representing maximum risk. Once a user's score reaches a threatening level, IT professionals can use behavioral data to further investigate their activities and mitigate risk by revoking or demoting their access to certain applications or systems.

Make Strategic Product Decisions

Software is central to any ICAM policy and larger Zero Trust architecture. Organizations should be intentional and strategic in implementing solutions that support unified access management, empowering security teams, and making security as seamless as possible for end users. ICAM software platforms with multi-factor authentication, identity federation, and end-to-end monitoring capabilities are integral in enhancing verification processes and protecting business-critical systems.

Enhance Identity Verification With a Trusted Software Partner

Zero Trust requires that businesses transform their entire approach to security by adopting a combination of new processes, technologies, and mindsets to secure resources and users across complex 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 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.

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-ICAM-WP100 September 15, 2022 2:37 PM