ENTERPRISE SECURITY GROUP AT BROADCOM

# Maximizing the potential of a zero trust architecture



Agencies can reap the benefits of zero trust by taking a fresh look at the industry-leading tools they already have

**Stanislav Elenkrich** | Enterprise Security Group at Broadcom

As recently as several years ago, zero trust was not well-defined. Agencies and other organizations understood the need to secure identities, endpoints and data, but the idea that all those elements should come together under a single architecture was something we in industry had to explain.

Now we no longer need to convince government IT leaders that they need zero trust, and most agencies own a significant portion of the components of a zero trust architecture. Today's challenge is to determine whether they're getting the maximum protection from that architecture.

There is a big difference between implementing zero trust simply to meet requirements and truly capitalizing on its potential. Many organizations know their security posture in terms of identities, devices and applications, and they have insights into user behavior and data sensitivity. They imagine different treatments for different levels of risk and have a clear and structured picture in their head of what they want.

They have a lot of good intentions and plenty of tools. But they have different teams that are responsible for different parts of the zero trust architecture. They also have legacy infrastructure, some applications that are hosted in the cloud, and human identities and machine identities, which have different risk models.

## Protecting a rapidly growing attack surface

Even when we add artificial intelligence into the mix, the principles of zero trust are still valid, and the same questions apply: Who can I trust? And who can access or download which resources?

However, AI does change the security paradigm. For one thing, because of AI, the barrier to launching a sophisticated attack against government targets is significantly lower, and adversaries can operate more quickly and effectively. If attackers are moving faster, defenders cannot afford to leave credentials or data exposed because the risk grows exponentially with the size of the attack surface.

Unfortunately, in such a complicated environment, many organizations end up only utilizing a fraction of what a zero trust architecture can deliver. They might be missing the opportunity to create sophisticated rules that distinguish between different levels of users, dynamically change access when necessary or govern any kind of interaction in real time.

For example, a contractor accessing a sensitive dataset from an unmanaged device should trigger a different access decision in real time than a full-time employee on a managed laptop. Most agencies already own the components to make that distinction, but few have configured the rules to act on it.

On our side of the equation, AI is also changing how we defend. We're applying machine learning to classify sensitive data faster in DLP, spot anomalous behavior across human and machine identities, and correlate signals across proxy, endpoint and identity telemetry so agencies can act on risk in real time rather than after the fact.

## A security approach that is hybrid by design

Symantec solutions have been embedded in federal, state and local government systems for over 20 years. When we talk to agencies about topics such as AI, data loss prevention (DLP) and endpoints, we are often talking about tools they have depended on across multiple administrations. That continuity is a huge asset, and it shapes how we at Broadcom approach zero trust.



Rather than telling agencies to deploy new tools from scratch, we help them extract maximum value from what they already have. In addition, our approach is hybrid by design. Symantec's powerful proxy, DLP and endpoint security tools can be deployed in the cloud or on premises. If an agency later decides to move resources between those environments, that shift is supported because the architecture assumes it's a hybrid deployment.

In addition, Symantec Global Intelligence Network is one of the largest civilian networks of threat telemetry in the world, with trillions of events. Government security teams don't have to make decisions based only on their own logs but can benefit from worldwide insights. This advantage compounds as attackers get faster and defenders need to react faster. As AI adoption accelerates, the ability to scale proven security and governance approaches is vital for delivering mission outcomes.

Agencies have invested heavily in security tools, and Broadcom wants to help them make the most of those investments so they can experience the full value of a mature zero trust program.

***Stanislav Elenkrich***
*is director of product management in Broadcom's Enterprise Security Group.*

> **As AI adoption accelerates, the ability to scale proven security and governance approaches is vital for delivering mission outcomes."**

