ENTERPRISE SECURITY GROUP AT BROADCOM

# Identity, endpoints and the new security perimeter



Continuous visibility into users and endpoints remains foundational in an increasingly distributed and AI-powered environment

**Manoj Sharma** | Enterprise Security Group at Broadcom

The hardened network edge, what is typically called the perimeter, dissolved years ago with the adoption of cloud and remote work. Users and data have left the building, which raises the question of how effective a perimeter is when the most critical assets are no longer inside it.

Now most data lives in the workloads, and those workloads are in the public cloud, edge locations and on-premises data centers. When users work from home, they are authenticating from anywhere and on any device. It becomes even more complicated when artificial intelligence has been enabled in software and the name. technology is making autonomous decisions and API calls in the user's name. In many cases, the human is not in the loop for every decision.

Agencies are no longer just securing the people who are accessing data. They also need to secure AI agents. The perimeter has essentially moved to wherever identity, data and workloads come together. In an ideal scenario, the perimeter travels with every user, device, application and agent rather than sitting in a fixed boundary. It means the old model of defend the edge and trust the inside needs to be reevaluated.



decisions and API calls in the user's

## Catching anomalous behavior in real time

Investigations into the most recent major breaches have revealed that attackers did not hack in. They literally logged in using a compromised identity or an unmanaged, unmonitored endpoint. That's why a zero trust approach to security is so important. It assumes that any identity, whether human or machine, could be compromised, and every request should be verified in context and continuously. However, identity by itself means very little by itself. An attacker's intent becomes an action when identity and an endpoint come together.

Defenders need continuous, real-time visibility into what's happening for a variety of reasons. First, if the IT team is only reviewing static events, such as employees' use of passwords and multifactor authentication, once a week or once a month, it won't know that compromised credentials were used to allow an attacker to come inside and move laterally until long after the intrusion happened.

Second, because the perimeter has evaporated, there is no longer a single checkpoint to monitor. Instead, identity and endpoint telemetry often forms the only common thread between activities happening in the cloud, on premises and through remote access. Teams have to continuously monitor all these events to

make sense of them and recognize when an incident is occurring.

Third, AI-driven attacks are coming faster and faster. If defenders are not continuously monitoring what is happening and how people are getting in, they have no chance of securing their resources. Continuous, automated correlation is the only way to catch anomalous behavior in time to stop an attack.

## Unmatched experience and a proven platform

Broadcom brings together security solutions for identities, endpoints, networks and data through a portfolio that includes CA Technologies, Symantec, Carbon Black and VMware. Our solutions are decades in the making, and they continue to mature with deployment in the most demanding environments. The experience we bring to the table is unmatched, and our software has been proven at scale in the most complex, highlyregulated industries worldwide.

When agencies work with Broadcom, they are investing in a mature, well-adapted, hardened platform that will deliver the outcomes they need. Furthermore, when agencies combine our tools with a zero trust architecture, they have continuous, coordinated visibility across identity, endpoint, data and network telemetry. With Broadcom, zero trust principles are enforced consistently no matter where a user is, and whether that user is a human or an AI agent.

***Manoj Sharma** is chief security strategist in Broadcom's Enterprise Security Group.*

> "In an ideal scenario, the perimeter travels with every user, device, application and agent rather than sitting in a fixed boundary."

