CASE STUDY

Broadcom Achieves Application-Aware Workload Protection

The Customer

Broadcom Inc. is a global infrastructure technology leader built on 50 years of innovation, collaboration, and engineering excellence. With roots based on the rich technical heritage of AT&T/Bell Labs, Lucent, and Hewlett-Packard/ Agilent, Broadcom focuses on technologies that connect the world. Through the combination of industry leaders Broadcom, LSI, Broadcom Corp., Brocade, CA Technologies, and Symantec, the company has the size, scope, and engineering talent to lead the industry into the future.

The Challenge

Continuous Attacks

Global technology leaders like Broadcom are major targets for malicious exploits and attacks that are increasing in both frequency and ingenuity. These evasive attacks are bypassing traditional perimeter and threat hunting tools and executing at the memory layer during runtime.

Critical Security Gaps

Broadcom wanted to stay proactive with its cybersecurity efforts, and initially, the company needed to focus on identifying potential security gaps in its customer portal, which provides critical product information and support services for thousands of customers worldwide. At the same time, stakeholders wanted to limit valuable time and resources spent tuning and policy adjusting to stay abreast with new vulnerabilities.

Conventional Security Tools Were Not Enough

Broadcom already relied on a full range of conventional security technologies, including endpoint protection, WAF and EDR products. But even with these multiple layers, the security leadership team worried about critical gaps in their strategy that could open doors to exposing sensitive customer information and corporate data.

VIRSEC

"When we deployed the Virsec platform, we experienced an immediate ROI, and a clear view into our entire application attack surface. Now, we have visibility and control over how our application code executes during runtime and identifies malicious behavior. This awareness is especially true for zero-day attacks, which Virsec can detect without any prior knowledge."

Sid Phadnis
Principal for Cybersecurity
Broadcom

The Solution

Evaluating a Next-Generation Security Solution

Broadcom's decision to identify a new solution provider to enhance its cyber defense strategy required a careful and thorough evaluation of potential vendors and security platforms. They had to take into consideration a highly complex infrastructure, available resources, and ongoing management of vulnerabilities and configurations. Virsec was selected for a detailed POC because of its depth of protection, automation, and lack of false positives.

Protecting the Full Application Stack

The Virsec Security Platform (VSP) protects the full application stack for the customer portal, including Java, Node.js, and Nginx web servers. The solution was tested for efficacy, performance, and usability while protecting web, memory, and host layers against advanced attacks.

Detecting and Stopping Evasive Attacks in Runtime

Broadcom found that the Virsec solution was able to detect and stop the broadest range of attacks, especially those that bypassed their existing WAF, endpoint, and EDR solutions, a significant differentiator compared to other solutions. Stakeholders also found the Virsec solution was significantly easier to manage by using automated, out-of-the-box detection that requires no signatures, learning, tuning, or policy updates.

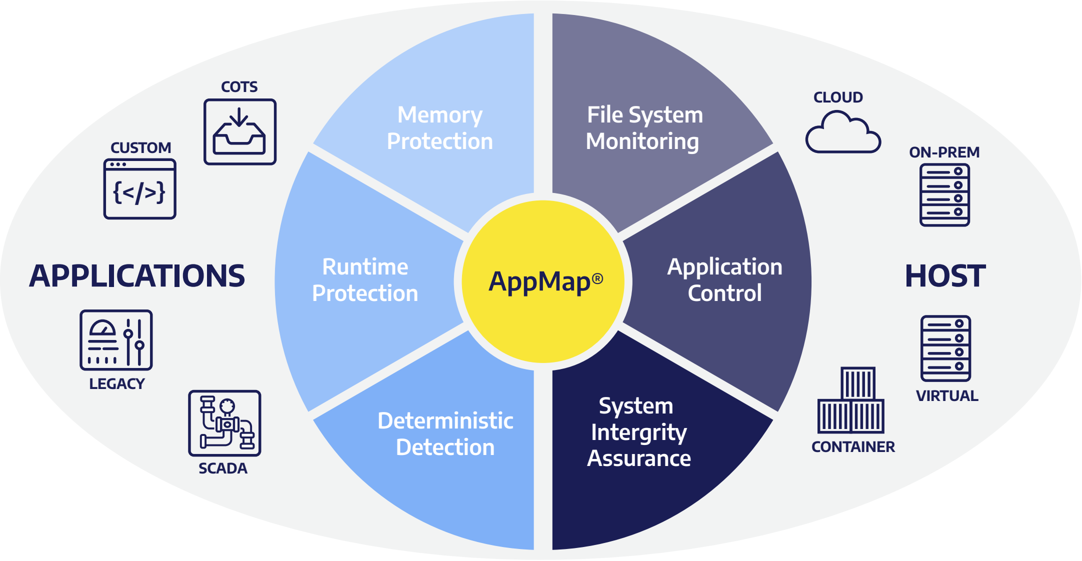
Detecting Zero-Day Attacks with No Prior Knowledge

Because Virsec can detect zero-day attacks with no prior knowledge, Broadcom found that the solution was ideal for ensuring compensating controls like vulnerability shielding, against unknown vulnerabilities and those yet to be patched.

Protecting Mission-Critical Application Workloads

With tangible and quantifiable results from the POC, Broadcom quickly decided to deploy Virsec to protect 100+ application instances across Broadcom's full application stack, including web applications, web servers, third-party tools, and host systems.

> **The program was so effective that Broadcom has now implemented the Virsec solution across their entire network to protect their mission-critical application workloads.**



The Results

Achieving Application-Aware Workload Protection

Broadcom's mission-critical applications and data are now protected against evasive runtime exploits at the process memory level, achieving true zero-trust runtime protection. Broadcom's proactive decision to implement system integrity assurance, application control and memory protection within a single solution ensures that their application workloads are now protected across web, memory, and host layers, during runtime.

Ensuring Good by Mapping the Application Stack

All of Broadcom's legitimate applications, file libraries, operating systems, processes, and memory are now mapped with Virsec's patented AppMap® technology. The technology continuously scrutinizes application processes across the full stack and ensures that critical applications only behave as intended and aren't corrupted by advanced exploits.

All of Broadcom's legitimate applications, file libraries, operating systems, processes, and memory are now mapped with Virsec's patented AppMap® technology. The technology continuously scrutinizes application processes across the full stack and ensures that critical applications only behave as intended and aren't corrupted by advanced exploits. Instead, this zero-trust model of "ensuring good" defines that any deviation from the norm is instantly detected, treated as a threat and stopped.

A Proactive Security Stance

Broadcom's bold security initiative to protect their business-critical applications and data and achieve true runtime protection across their entire infrastructure puts them at the forefront of the industry. They realized conventional security tools were not enough to provide full protection and have adopted a next-generation security solution to protect against next-generation cyber threats and attacks. Broadcom now has full visibility into their entire application attack surface and can rely on full runtime protection.

VIRSEC

"Today's hackers are more advanced than ever before, and overall, we need to be more proactive with our security stance. Conventional tools will not help us protect what matters most to our business – our business-critical applications and data.
To do that, we start with runtime protection from the inside, and that's why we have selected Virsec. They are truly leading the way to more advanced cyber protection."

Andy Nallappan
Chief Technology Officer and Head of Software Business Operations
Broadcom

Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Recognition

Cyber Catalyst	CRN	Cyber Defense Magazine Global Awards 2019 Winner	Gartner
Cyber Security Excellence Awards Winner 2020	MITRE	Info Security Products Guide 2020 Global Excellence Gold	Ovum

Partners & Customers

Tech Mahindra	NCUA	Raytheon Technologies	godrej
Schneider Electric	YOTTA	du	AVEVA
BROADCOM	inspirage	etisalat	GDIT

VIRSEC

Server & Application Workload Protection

Application-Aware Mapping Technology

No Signatures, No Tuning, No Noise

Zero Dwell Time

Full-Stack Runtime Protection