WHITE PAPER

A Zero Trust Approach from Broadcom® Software

Zero Trust Technology Solutions

November 11, 2022
ZER-TRU-WP100

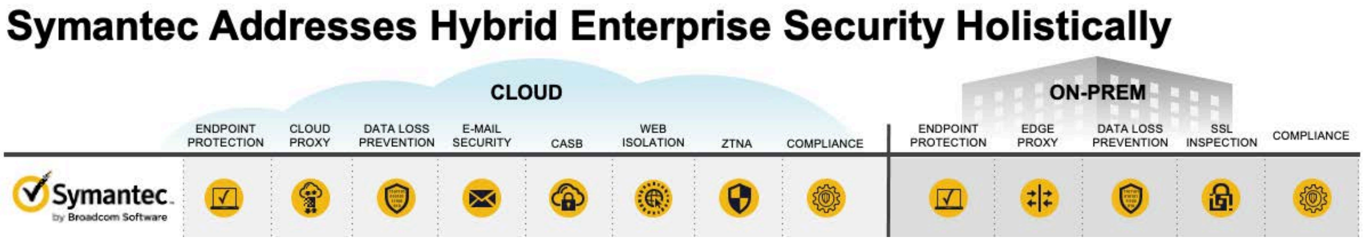
Overview

Broadcom® Software understands that zero trust is founded on the principle that organizations should not automatically trust anything and must verify everyone and everything trying to connect to its resources before granting access based on identity, context, and trustworthiness. To accomplish this goal, organizations must select and integrate technologies that can provide controls through policies to achieve the organization's goals across a continuously evolving enterprise.

While many vendors advocate a single leap to zero trust based on a Secure Access Service Edge (SASE) solution, Broadcom Software believes it is more of a journey from current state to desired state that will require most enterprises to operate existing on-premises solutions while evaluating, testing, acquiring, designing, selecting, integrating, and configuring cloud-based solutions.

Because we believe zero trust is a journey, we have a very practical approach to zero trust. Given the breadth and depth of our portfolio, we offer a unique migration path because many of our solutions are available both on-premises and in the cloud as shown in Figure 1.

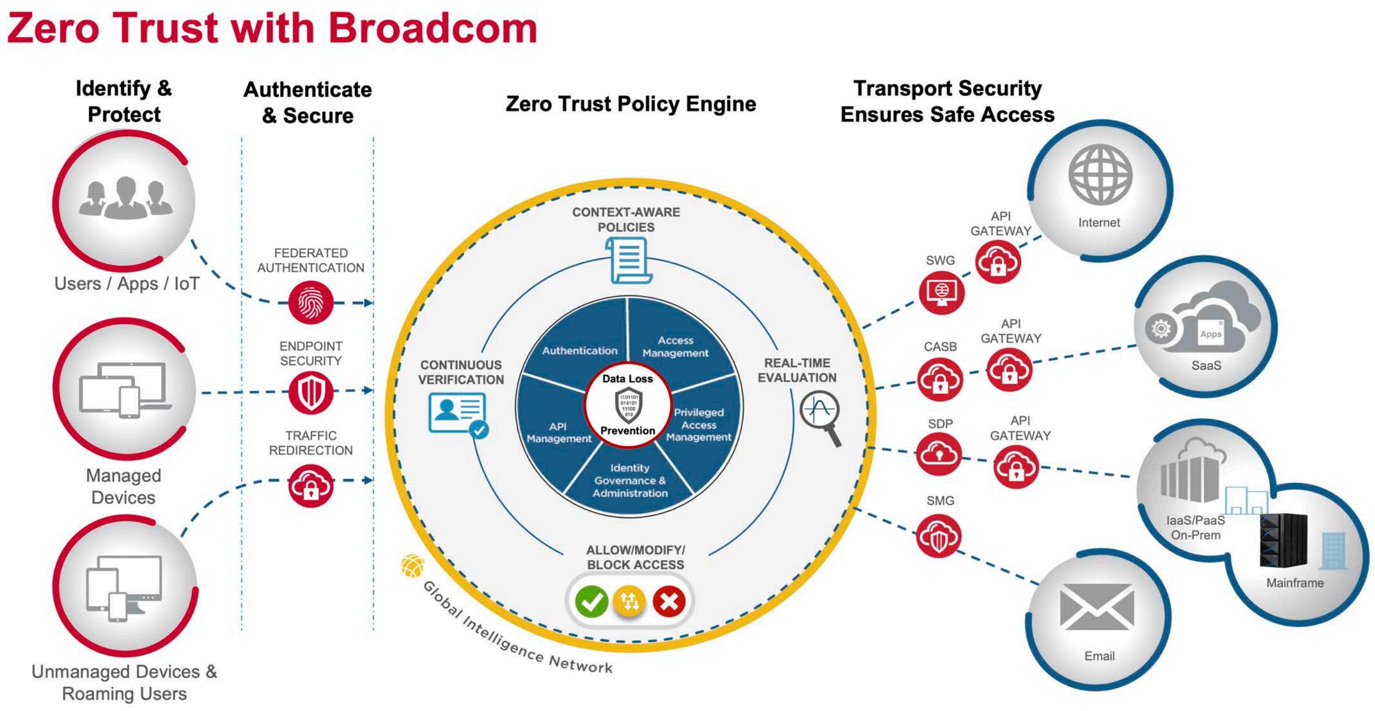
Figure 1: Broadcom Software Hybrid Enterprise Portfolio



With our breath and depth of on-premises and cloud-based cybersecurity, identity and access management, API security and orchestration, network performance monitoring, and end user experience monitoring capabilities, Broadcom Software provides many controls organizations leverage to execute their zero trust strategy.

While Broadcom Software offers standalone cloud-based solutions for organizations that are looking for point product solutions, many of our zero trust components are also integrated into a comprehensive SASE offering. Our SASE architecture is an all-inclusive convergence of services including software defined perimeter, secure web gateway, cloud access security broker (CASB), secure messaging gateway, browser isolation, TLS/SSL inspection, and data loss prevention.

Figure 2: Zero Trust with Broadcom Software



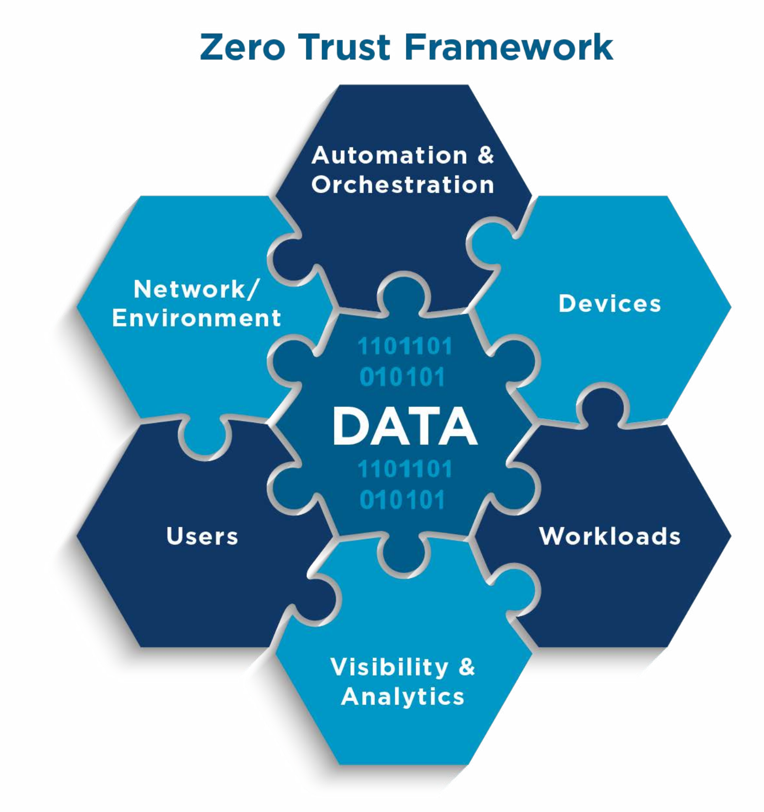
The remainder of this document highlights capabilities from the Broadcom Software portfolio that support an organization's zero trust strategy and controls.

Broadcom Software Zero Trust Technology Solutions

Symantec® Data Loss Prevention

As organizations adopt zero trust, they expend significant time and resources designing, acquiring, integrating, and configuring an array of technologies to ensure that only properly verified people and systems can access data, because data is the center of zero trust as shown in Figure 3.

Figure 3: Zero Trust Reference Architecture



Therefore, once access to data has been granted, it is paramount that organizations take steps to prevent accidental or malicious disclosure by those who have been successfully vetted by zero trust controls. Preventing disclosure is the exact role of data loss prevention (DLP) solutions.

As a DLP industry leader, our solution provides visibility and control for sensitive information wherever it lives and travels across devices and on-premises environments so you can prevent accidental sharing of data, stop insider risks, and enforce compliance requirements.

Symantec DLP discovers, monitors, and protects sensitive data with a single policy across multiple channels: endpoint, storage, network, email, and cloud. Symantec DLP delivers a single console for policy management and administration. It allows operators to write policies once and apply them across web, email, endpoints, storage, and cloud instead of having to write specific policies for each channel, avoiding the hassle of policy duplication.

Symantec DLP integrates with end user devices, servers, databases, web gateways, cloud access security brokers, network devices, and email gateways to reduce the chance of a data breach. The following sections highlight Symantec DLP control capabilities.

DLP for Endpoints

The following products provide DLP solutions for endpoints:

- **Symantec DLP Endpoint Discover** scans local hard drives and gives you visibility into any sensitive data stored by users on laptops and desktops and establishes a baseline inventory. It provides a number of responses including quarantining files, flagging files for Symantec Endpoint Protection, in addition to custom response actions such as encryption, DRM, or redacting confidential information enabled by the Endpoint FlexResponse API.
- **Symantec DLP Endpoint Prevent** monitors users' activities and enables fine-grained control over a wide range of applications, devices, and platforms. It provides a wide range of responses including identity-based encryption and DRM for files transferred to USB. With Endpoint Prevent, administrators can alert users to incidents using on-screen pop-ups or email notifications. Users can also override policies by providing a business justification or cancelling the action (in the case of a false positive).

DLP for Storage

The following products provide DLP solutions for storage systems:

- **Symantec DLP Network Discover** finds confidential data by scanning network file shares, databases, and other enterprise data repositories. This scan includes local file systems on Windows, Linux, AIX, and Solaris servers; SQL databases; and Microsoft Exchange and SharePoint servers. It provides high-speed scanning for large, distributed environments, and optimizes performance by scanning only new or modified files.
- **Symantec DLP Network Protect** adds robust file protection capabilities on top of Network Discover. Network Protect automatically cleans up and secures all of the exposed files Network Discover detects, and it offers a broad range of remediation options, including quarantining or moving files, copying files to a quarantine area, or applying policy identity-based encryption and DRM to specific files. Network Protect even educates business users about policy violations by leaving a marker text file in the file's original location to explain why it was quarantined.

DLP for Network

The following products provide DLP solutions for networks:

- **Symantec DLP Network Monitor** captures and analyzes outbound traffic on your corporate network, and detects sensitive content and metadata over standard, non-standard and proprietary protocols. It is deployed at network egress points and integrates with your network tap or Switched Port Analyzer.
- **Symantec DLP Network Prevent for Web** protects sensitive data from being leaked to the web. It monitors and analyzes all corporate web traffic, and optionally removes sensitive HTML content or blocks requests. Network Prevent for Web is deployed at network egress points and integrates with your HTTP, HTTPS or FTP proxy server using ICAP.
- **Symantec DLP Network Prevent for Email** protects sensitive messages from being leaked or stolen by employees, contractors, and partners. It monitors and analyzes all corporate email traffic, and optionally modifies, redirects, or blocks messages based on sensitive content or other message attributes. Network Prevent for Email is deployed at network egress points and integrates with mail transfer agents and cloud based email including Microsoft Office 365 Exchange.

DLP for Cloud

The following products provide DLP solutions for cloud services:

- **Symantec DLP Cloud Detection Service** inspects content extracted from cloud app and web traffic and automatically enforces sensitive data policies. Cloud to cloud integration with Symantec CloudSOC® protects data in motion and at rest across more than 100 unsanctioned and sanctioned cloud apps, including Office 365, Google Workspace (G Suite), Box, Dropbox, and Salesforce. The integration allows extension of existing policies and robust detection to cloud applications, and incident management directly from the DLP console.
- **Symantec DLP Cloud Service for Email** continuously monitors corporate email traffic, using built in intelligence and advanced detection to minimize false positives. It protects against data leaks in real time with automated message modification or locking to enforce downstream encryption or quarantine. For data shared with third parties, it can automatically enable identity based encryption and digital rights for email bodies and attachments.
- **DLP Cloud Detection Service for Web Security Services** integrates with Symantec Web Security Service to monitor even encrypted web traffic for protection of roaming and mobile users.

User and Entity Behavior Analytics

Symantec Information Centric Analytics is a user and entity behavior analytics platform that provides an integrated, contextually enriched view of cyber risks in your enterprise. It collects, correlates, and analyzes large amounts of security event data from across diverse sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Backed by patented machine learning, Symantec Information Centric Analytics delivers rapid identification and prioritization of user and entity-based risks.

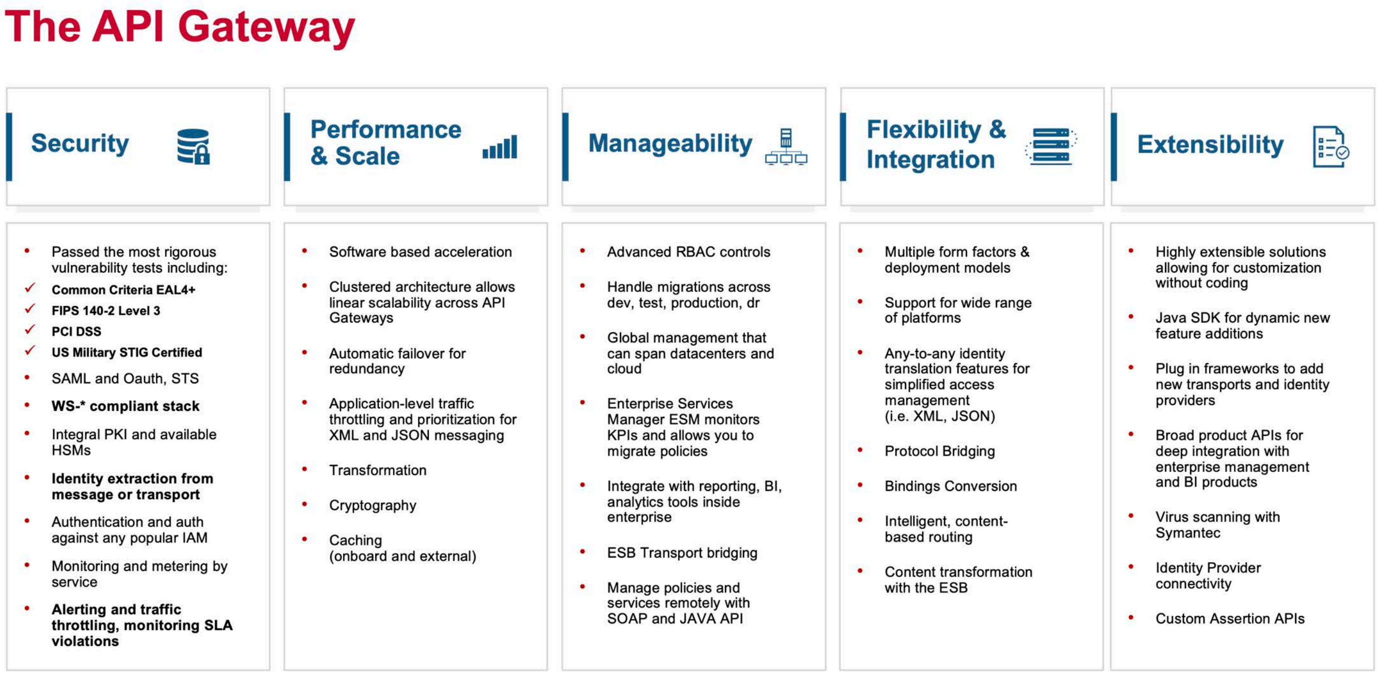
Broadcom Software Layer7™ API Gateway

The ability to leverage existing Identity, Credential, and Access Management (ICAM) solutions and other target solutions with the objective of achieving zero trust can only be accomplished with a well thought out phased product selection and implementation plan. A key component of this plan should be the understanding of how all of these different product solutions integrate together to address the specific enterprise or organizational goals.

The best approach to accomplishing this is with a strong security focused gateway, designed and built to leverage industry standards using and securing APIs that are offered today by most vendor-based solutions.

The Layer7™ API Gateway is common criteria for Enterprise Service Management (Access Control and Policy management), STIG, and FIPS 140-2 compliant. It is hardened, tuned, and offered as a special purposed appliance or virtual image. The Layer7 API gateway can run on-premise or in a hybrid cloud-based environment. It provides leading edge support for industry and vendor security standards and solutions and includes significant auditing and logging capabilities which can be used to provide non-repudiation information to fully verify activity.

Figure 4: Layer7 API Gateway



The API Gateway

Security

- Passed the most rigorous vulnerability tests including:
- ✓ **Common Criteria EAL4+**
- ✓ **FIPS 140-2 Level 3**
- ✓ **PCI DSS**
- ✓ **US Military STIG Certified**
- SAML and Oauth, STS
- **WS-* compliant stack**
- Integral PKI and available HSMs
- **Identity extraction from message or transport**
- Authentication and auth against any popular IAM
- Monitoring and metering by service
- **Alerting and traffic throttling, monitoring SLA violations**

Performance & Scale

- Software based acceleration
- Clustered architecture allows linear scalability across API Gateways
- Automatic failover for redundancy
- Application-level traffic throttling and prioritization for XML and JSON messaging
- Transformation
- Cryptography
- Caching (onboard and external)

Manageability

- Advanced RBAC controls
- Handle migrations across dev, test, production, dr
- Global management that can span datacenters and cloud
- Enterprise Services Manager ESM monitors KPIs and allows you to migrate policies
- Integrate with reporting, BI, analytics tools inside enterprise
- ESB Transport bridging
- Manage policies and services remotely with SOAP and JAVA API

Flexibility & Integration

- Multiple form factors & deployment models
- Support for wide range of platforms
- Any-to-any identity translation features for simplified access management (i.e. XML, JSON)
- Protocol Bridging
- Bindings Conversion
- Intelligent, content-based routing
- Content transformation with the ESB

Extensibility

- Highly extensible solutions allowing for customization without coding
- Java SDK for dynamic new feature additions
- Plug in frameworks to add new transports and identity providers
- Broad product APIs for deep integration with enterprise management and BI products
- Virus scanning with Symantec
- Identity Provider connectivity
- Custom Assertion APIs

As shown in Figure 4, part of the Layer7 API Gateway feature set provides for an orchestration capability to support integration and transformation of information from multiple subsystems to other subsystems that require multiple transformed pieces of information to arrive at an appropriate zero trust based access grant.

Essentially, the Layer7 API Gateway provides the *glue* between multiple vendor solutions including those offered from the Broadcom Software stack that are reviewed below.

Symantec Web Protection

Secure web gateways, formerly known as BlueCoat Web Proxies, once used for network optimization is now one of the most important cyber security orchestration devices on the network. Secure web gateways enable organizations to control user access to websites and apply authentication to web resources.

Secure web gateways are an important zero trust control because they are the only devices on the network that proxy a connection between the client and the external web. While vulnerabilities and malicious contents can get through next-generation firewalls, they will not be able to bypass secure web gateways because secure web gateways deny all traffic unless the entire payload has been fully assembled, inspected, and authenticated.

On-premises secure web gateways often serve as an integral network security orchestration point in many data center security stacks while cloud-based secure web gateways serve as the foundational technology in many SASE architectures. Broadcom Software secure web gateway is powered by one of the world's largest global intelligence networks. As a result, we provide the most comprehensive and accurate web URL categorization in the industry. Symantec offers both on-premises and cloud-based secure web gateway in a single solution known as Symantec Web Protection. Symantec Web Protection increases mission agility by supporting any mix of centrally-managed cloud and on-premises user populations, including all cloud deployments, enhancing the ROI of existing investments, policies, and expertise. It allows existing on-premises Secure Web Gateway (SWG) customers to efficiently support their remote workforce without the need to backhaul traffic or completely overhaul their security stack.

Symantec Web Protection gives organizations an advanced cloud-delivered SWG and leading on premises SWG deployment-both of which can operate seamlessly together with a unified management, reporting, and policy control interface. It also includes a cloud firewall service, threat intelligence, SSL inspection, content analysis, deep file inspection, isolation, reverse proxy, and more.

Symantec Web Protection allows customers to move 100% to the cloud right now. However, Web Protection is also designed for organizations who are not ready for full-cloud SWG adoption, yet want the flexibility to begin this journey now or any time in the future. It also serves as an entry-level SASE foundation, enabling secure and fast web access for any user, from any device, located anywhere-protecting users, devices, and data from known and unknown threats across all locations (remote, branch, and HQ).

Symantec CloudSOC

Symantec CloudSOC is a CASB solution that enables zero trust by providing agencies with the ability to control the use of cloud applications and services.

By leveraging both gateway and API technologies, CloudSOC provides flexible options to protect against a broad range of cloud application use cases to cover sanctioned and unsanctioned cloud app usage, and managed and unmanaged device coverage. CloudSOC enforces granular access controls, applies data loss protection, detects malware, and generally keeps a security eye on users to identify compromised accounts or other high-risk activity.

Symantec CloudSOC offers unique value through industry-leading CASB capabilities and is a core capability included in our SASE service. It consists of three modules that are managed through a common management console:

CASB Gateway

Symantec CloudSOC CASB Gateway continuously monitors and controls the use of cloud apps to enforce policies, identifies malicious or inappropriate data sharing, signals malware threats, responds to security incidents, and automates escalations. It offers deep visibility into user activity across thousands of cloud apps and services, and both tracks and governs activity of sanctioned and unsanctioned cloud apps.

CASB for SaaS and CASB for IaaS

CloudSOC CASB for SaaS and CloudSOC CASB for IaaS are cloud based services that provide visibility and control over user activities in cloud applications. They monitor and protect stored, transferred, and shared data. A complete list of supported cloud applications can be found in the CloudSOC online store; it includes Microsoft Office365, Google Workspace (G Suite), Box, Salesforce, and ServiceNow.

CASB Audit

Symantec CloudSOC CASB Audit discovers and monitors every cloud app used across your organization, identifies their users, and highlights any risks and compliance issues they may pose. It provides visibility into Shadow IT, and blocks access to unapproved cloud services.

Symantec Secure Access Cloud

Secure Access Cloud (SAC) is a software defined perimeter solution that enables zero trust by eliminating inbound connections to agency networks and creating a software defined perimeter between users and agency application and establishing application level access.

SAC can be configured to completely cloak all agency applications and services so that a user requesting access to a specific application needs first to be authenticated and authorized. Only then will SAC create the secured granular applicative connection between the user and the requested application. This connection is ephemeral and automatically terminates once the user completes her task on the specific application.

SAC securely connects any user (be they employees, contractors, partners or customers) from any device, anywhere in the world to agency on-premises and cloud-hosted applications while all other agency resources are cloaked. No network access is ever granted to prevent any lateral movements to other network resources while eliminating the risk of network-based attacks.

The platform is agentless. It can be deployed without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. SAC provides full governance and real-time enforcement of users' actions in each agency application.

With SAC, users gain access only to the specific applications and resources for which they are authorized. The solution takes the zero-trust access approach further by providing full visibility, governance and contextual enforcement for user actions, monitoring and logging every operation for simplified auditing and reporting.

Symantec Messaging Gateway

Given the pervasiveness of email based attacks in today's threat landscape, an email security solution is required and often included in a SASE architecture, as is the case with our SASE solution.

The Symantec on-premises email security solution, known as Messaging Gateway, provides essential inbound and outbound messaging security including, powerful protection against the latest messaging threats including ransomware, spear phishing, and business email compromise. A zero-trust proprietary technology *Disarm* removes all active content from office and PDF attachments that could potentially contain malicious content. Symantec Messaging Gateway catches more than 99 percent of spam with a less than 1 in 1 million false positives, and effectively responds to new messaging threats with real-time automatic anti-spam and anti-malware updates.

Symantec Endpoint Security Complete

Symantec Endpoint Security (SES) Complete delivers a comprehensive and highly integrated endpoint security approach, protecting all traditional and mobile endpoints. It provides interlocking defenses at the device, application and network level and, it uses artificial intelligence to optimize security decisions.

Symantec defends endpoints proactively to reduce the attack surface with advanced policy controls and technologies that scan for vulnerabilities and misconfigurations across applications, Active Directory, and devices connecting to the endpoint. It proceeds with hardening the system and locking down processes and behaviors to render many attacker tactics and techniques ineffective.

Symantec also stops breaches and prevents attackers from persisting or dwelling on the network. Pairing network firewall and intrusion prevention capabilities with deception and Active Directory security to stop lateral movement, Symantec prevents credential theft and blocks reconnaissance efforts.

To help quickly close out endpoint incidents and minimize attack impact, SES Complete combines endpoint detection and response technologies with Symantec security operations center analyst expertise to precisely detect advanced attacks, provide real-time analytics, and enable active threat hunting for investigations and remediation.

Symantec Data Center Security

Symantec Data Center Security is our strongest zero trust endpoint security product that goes beyond traditional anti-malware and application allow lists to provide total system lockdown for virtually every Windows and UNIX operating systems. It is also known as the un-hackable technology as it has protected the Symantec flag from being captured at Black Hat for 10+ years. It has successfully defended against *every* zero-day vulnerabilities and IAVAs to date.

Data Center Security is commonly used to protect organizations' most critical assets and to secure any end-of-life operating systems. Since it is extremely lightweight, it is also used to defend many operational technologies, SCADA systems, and IoT environments.

Broadcom Software Network and End User Experience Visibility

As agencies embark on their zero trust journey, they will have to deal with a seismic shift in thinking about how users access data and the adoption new technologies such as Software Defined-Wide Area Networking (SD-WAN) and SASE as parts of their zero trust architecture. While on the journey to zero trust, federal agencies continue to contend with the fluid landscape of employees working from anywhere (WFA).

Unfortunately, one of the most likely challenges agencies will face as a result of zero trust architecture and WFA is the likelihood that the user experience has been and will continue to be impacted. As policies are put in place to granularly control and intentionally limit user access to data and applications, IT teams likely will increasingly face scenarios where users cannot access the data and applications as they have in the past. IT Admins will have to determine if this is by design or if it is the result of a network or application performance issue.

Broadcom Software DX NetOps

Broadcom Software NetOps has provided enhanced network performance monitoring to federal agencies for years. With our recent acquisition of AppNeta®, federal agencies can now just as effectively monitor the user experience in SD-WAN/SASE environments and WFA scenarios.

A combination of real-time monitoring and machine-learning driven analytics for SD-WANs, DX NetOps comprehensively simplifies today's network complexity through high scale, unified monitoring enabling full-stack analytics for assuring traditional, SDN, and cloud architectures. DX NetOps converts inventory, topology, metrics, faults, flow, and packet analysis into actionable intelligence for network teams. The platform is complemented by our solution that enables teams to establish proactive, autonomous remediation capabilities across applications, infrastructure, and networks that fuel superior user experiences.

Broadcom Software DX NetOps is a solution that combines fault management, performance analysis, and flow diagnostics to deliver an operational observability of classical networks as well as software-defined networks and SD-WAN. We have the largest SD-WAN vendor support in the market covering Viptela/Cisco, 128T/Juniper, Versa, Nuage, SilverPeak, and many more to come.

Broadcom Software AppNeta

AppNeta helps IT proactively track, manage, and optimize performance, no matter what apps or networks are being used. AppNeta combines active synthetic network and application monitoring with passive packet visibility. This unique blend of active and passive monitoring offers comprehensive visibility of business-critical apps and networks from the end user perspective.

AppNeta enables IT operations teams to fully understand how performance is affected by common issues such as application outages, route changes, connectivity drops, and ISP peering changes. With AppNeta, teams can monitor the end-to-end application delivery path, regardless of which cloud, office, home, or data center is used. By helping isolate where issues stem from, the solution enables IT teams to reduce mean time to innocence for issues that are outside their sphere of responsibility.

Broadcom Software Identity and Access Management

We have a complete solution with which enterprises are often able to achieve their end-to-end IAM goals. Our solution spans from identity management and provisioning, credential enrollment, authentication and authorization and privileged access management. Our ICAM portfolio consists of the following components:

- **Identity Governance and Administration:** IGA delivers comprehensive access management and governance capabilities through an easy-to-use, intuitive interface.
- **Authentication and Authorization:** SiteMinder™ is a unified access management platform that applies appropriate authentication and authorization with single sign-on, identity federation, and granular security policies, while monitoring and managing the entire user session.
- **Privileged Access Management:** Privileged Access Management securely vaults and manages privileged credentials, seamlessly brokering connections to endpoints without users/applications seeing or knowing credentials, while providing full auditing and recording of those sessions.
- **Directory Service:** Directory Service is a proven next-generation directory server that provides standards-based distribution and replication models with higher performance than the competition. Highly scalable to support large, complex and problematic environments.
- **Advanced Authentication:** VIP Authentication Hub enables rapid integration of applications using a completely open and standards-based solution, while extending the value proposition of the existing solutions you already have in place.

About Broadcom Software

Broadcom Software is a global technology leader that designs, develops, and supplies a broad range of infrastructure software solutions that are available on most Government IDIQ/GWAC contract vehicles. Our category-leading product portfolio serves critical markets including data center, networking, enterprise software, and storage.

Broadcom Software, with $5+ Billion in revenues, has a major presence in numerous markets. We are engineering-focused and for decades have always operated with that model at our core. We have one of the industry's largest IP portfolios with over 3,200 software patents. Everything we do is framed around technological leadership.

Additionally, we continue to acquire and invest the most strategic and business critical technologies for our customer base. We lead the industry in investing 14% of profits back into software research and development and will always continue to invest in and fund that innovation. Our aim is to lead in each of our target technology segments and our software portfolio is a great example of this strategy.

Broadcom Software is part of Broadcom, Inc. Broadcom is a U.S.-based company that is incorporated in Delaware and headquartered in California.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

BROADCOM®
SOFTWARE