Solution Brief

Symantec
A Division of Broadcom

Symantec® Zero Trust Framework

Challenge

Traditional perimeter defenses have been disappearing as organizations shift applications and workloads from on-premise data centers to cloud infrastructure. These technologies were never meant to scale to handle the large numbers of remote workers. A Zero Trust architecture is designed to address these challenges; however, organizations are struggling to integrate the different pillars of Zero Trust into a consolidated platform.

Opportunity

Zero Trust offers a comprehensive framework that secures legacy and future applications across the hybrid environment. In many cases, organizations already have many of the building blocks necessary to achieve Zero Trust, but these security tools and technologies exist within their own silos. The Symantec Integrated Cyber Defense approach brings these disparate systems together. Not only do we provide all of the components necessary to deliver Zero Trust, but we also can integrate with your existing solutions to protect those investments.

Benefits

A comprehensive security approach, embracing the principles of both Zero Trust and Secure Access Service Edge (SASE) models, will protect data regardless of where it is used or stored: on the mainframe, on-premises, or in the cloud. It also protects users and their devices, which are capable of accessing this data from anywhere. Zero Trust leverages security data across different security tools to build intelligent and comprehensive usage patterns that improve threat detection.

The Zero Trust model is founded on the belief that organizations should not automatically trust anything inside or outside its perimeters and must verify everything trying to connect to its resources before granting access—based on identity, context, and trustworthiness. To accomplish this goal, you must build an integrated platform that shares information across different security technologies.

Introduction

The concepts of Zero Trust are not new; they have been around for years. However, three recent developments are making Zero Trust more relevant and its adoption more important than ever:

- **Cloud Migration:** The spread of cloud technologies is changing every facet of modern IT, including reshaping the way we develop and use applications. Organizations embracing the cloud are enjoying a range of business gains, but cloud adoption also introduces new security challenges. Traditional security tools were not designed to adapt to the dynamic nature of these cloud environments.
- **Secure DevOps:** At its most fundamental level, DevOps seeks to engage Agile methodologies to increase the speed and quality at which innovation can be introduced into applications. One of the key facets of DevOps is automation; however, traditional security processes and tools are still heavily dependent on human configuration and effort to implement. As a result, security is often being ignored because it impacts the delivery of apps to the market.
- **Remote Workforce:** The modern enterprise was already facing an issue with "Bring Your Own Device" movements within the workforce, but this issue was compounded by the COVID-19 shutdown. Traditional perimeter defenses, such as firewalls and VPNs, were not scaled to handle the large number of employees suddenly forced to work remotely, many of whom may have been forced to access corporate resources with personal devices.

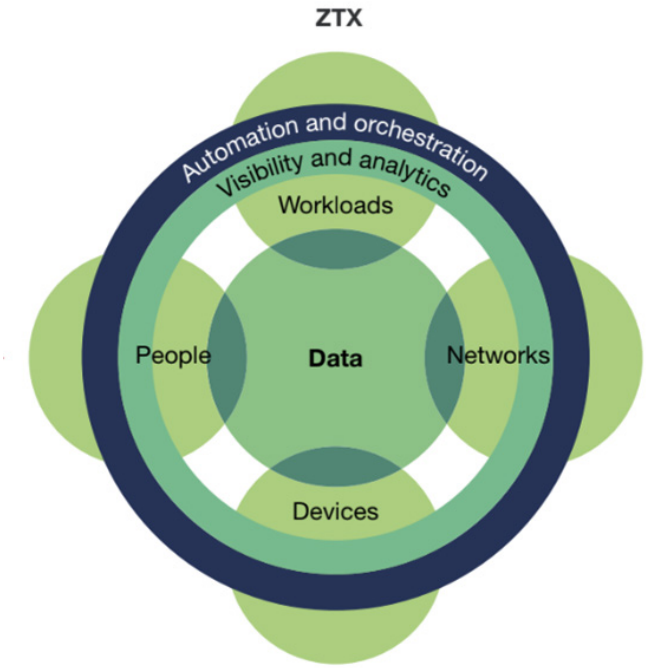
Although each of these challenges may look unique and different, and they may not seem related, the reality is that a Zero Trust approach addresses them all. But before we discuss the elements of the Symantec Zero Trust solution, let's look at the key pillars of Zero Trust.

The Pillars of Zero Trust

In 2009, Forrester developed a new information security model called the Zero Trust Model which has since gained widespread acceptance and adoption (although the term *zero trust* was actually coined by Stephen Paul March in 1994). Since its creation, Forrester has continued to evolve the model to its most current state.

The Forrester model includes seven pillars. Data sits at the center of the Forrester model because this is what you are trying to protect. People, devices, and workloads surround data because these are three primary "actors" trying to access and use the data. Networks are the primary means to connect the actors to the data. The final two pillars represent automation and orchestration (the ability to make all of the pillars work together to seamlessly enable secure access to the data) and visibility and analytics (the ability to know who is accessing the data for governance and the ability to detect and prevent unauthorized access).

Figure 1: Forrester Seven Pillars of Zero Trust Architecture



Achieving Zero Trust with Symantec Integrated Cyber Defense

The following sections describe the Symantec solutions that address each Zero Trust Model pillar.

Securing Devices

Devices are a primary target for cyber attackers. With today's global threats adept at entering at the endpoint, it can take less than 7 minutes for an attacker to compromise an entire enterprise. The impacts on businesses can be staggering. Properly protecting endpoint devices in today's environment requires addressing threats and attacks across the entire attack chain via attack surface reduction, attack prevention, breach prevention, and detection and response.

Symantec Endpoint Security (SES) Complete delivers a comprehensive and highly integrated endpoint security approach, protecting all traditional and mobile endpoints while providing interlocking defenses at the device, application, and network level and using artificial intelligence (AI) 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 (EDR) technologies with Symantec security operations center (SOC) analyst expertise to precisely detect advanced attacks, provide real-time analytics, and enable active threat hunting for investigations and remediation.

SES Complete works alongside other Symantec security solutions and integrates with third-party vendors via the Symantec Integrated Cyber Defense Exchange (ICDx) strategy. With these SES Complete integrations, IT security teams can detect threats anywhere in their networks and address threats with an orchestrated response.

Additionally, another point of attack is the communications between devices and corporate applications and resources, which are predominantly done using APIs. Symantec addresses this threat vector with its Layer7® API Management solution, which is lightweight, low-latency mobile gateway with integrated security and management controls designed

to help enterprises safely and reliably expose internal assets to developers and remote apps as mobile APIs. Deployable in the cloud, on-premises, or in a hybrid configuration, the gateway solves critical, mobile-specific challenges around identity, security, adaptation, optimization, and integration. Layer7 has Common Criteria Certification in two profiles, addressing the needs of regulated industries, as well as public sector requirements. In addition, it is FIPS 140-2 out of the box, and can be configured for both FIPS 140-3 and PCI-DSS compliance. Layer7 includes both OAuth and OpenID Connect (certified in four profiles), and includes over 100 built-in policies to protect against DoS and API attacks.

Layer7 also includes a mobile SDK to integrate with enterprise IAM systems such as SiteMinder, as well as social login, to maintain a seamless end-user experience. The SDK also supports multi-factor auth and biometric authentication on devices that support this. Finally, Layer7 tracks the relationship between the user, the app, and the device, and can trigger further authentication when an action deviates from the established pattern (meaning, when a user looks at his bank account and makes mobile deposits regularly, a transfer request for a large amount can trigger a biometric authentication requirement in order to continue).

Securing People

Extending Zero Trust to people begins with authentication—positively identifying legitimate users from fraudulent ones is a critical and foundational step as you cannot effectively enforce access controls if you do not really know who is requesting the access. Symantec VIP addresses this challenge by providing multifactor credentials and contextual risk analysis from the cloud so that stronger authentication can be applied where it is needed.

Once authenticated, you must ensure that only authorized users gain access to sensitive resources. For over 20 years, Symantec SiteMinder has been helping organizations by providing seamless Single Sign-On (SSO) access to on-premise and cloud-based applications. Furthermore, SiteMinder can also be enhanced through integration and implementation of Symantec Secure Access Cloud. Cloud-delivered Secure Access Cloud manages granular access to enterprise applications in IaaS/PaaS environments or on-premises data centers.

Privileged accounts are often an organization's most valuable asset—and the most likely to be exploited by external hackers or insider threats. One compromised privileged account can cause irreparable damage to infrastructure, intellectual property and brand. Symantec Privileged Access Manager (PAM) is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies, and monitoring and recording privileged user activity across virtual, cloud, and physical environments.

Finally, you must address least privileged access. Certainly the aforementioned access management tools can grant or deny access to your resources, but they do not ask the question, *should* the user have this access at all. Symantec Identity Governance and Administration (IGA) addresses this challenge by streamlining and automating the processes associated with reviewing and certifying user access—and this access governance ensures that users are only granted the level of access that they absolutely need.

Securing Network

The traditional approach to securing the network perimeter has been rendered obsolete by a perfect storm of mobile users, remote offices and home working, cloud apps, compliance obligations, and evolving security threats. Network and security teams need solutions that protect a remote workforce that needs to be connected around the clock and from any location. At the same time, they need a seamless and secure solution that improves the user experience.

Secure Access Cloud provides highly secure granular access management for enterprise applications deployed in IaaS clouds or on-premises data center environments. This SaaS platform eliminates the inbound connections to your network and creates a software-defined perimeter between users and corporate application and establishes application-level access. This zero-trust access service avoids the management complexity and security limitations of traditional remote access tools, ensuring that all corporate applications and services are completely cloaked—invisible to attackers targeting applications, firewalls, and VPNs.

Another aspect of protecting the network is providing secure access to the web, and this connectivity often requires traffic to be backhauled to an enterprise data center so that security and policies can be enforced; however, this approach is no longer effective. Symantec Web Security Service (WSS) provides superior security for data, apps, and users through a comprehensive cloud-delivered Secure Web Gateway. Built upon an advanced proxy architecture, Symantec WSS offers protection from advanced threats, protection of sensitive information, and compliant cloud application use—all delivered with scale upon a resilient, high-performance network backbone.

To protect against advanced email attacks which are delivered via SMTP (a different channel from most Internet activity), dedicated email threat and data protection capabilities are required. Email threats have evolved; no longer is traditional spam and anti-malware detection effective. With the rise of ransomware, phishing, and business email compromise fraud, sophisticated detection, prevention, and risk avoidance methods are needed. Symantec Email Security protects against advanced threats, risky URLs, and impersonated email. Web Isolation technology allows uncategorized or risky webpages to be opened in a secure, disposable container, stopping web-delivered malware or phishing sites from impacting users. In addition, email encryption that integrates with Symantec DLP extends an organization's data protection policies to the email channel.

Securing Workloads

As organizations have shifted their applications to cloud environments, security concerns have been raised. And although most cloud infrastructure puts strong safeguards in place to help protect customer privacy, there is often a lack of visibility into who is using the cloud and how they are using it, especially when it comes to large workloads of sensitive data that may be stored and/or processed in the cloud.

Symantec CloudSOC CASB empowers organizations to confidently enable cloud applications and services while helping them stay safe, secure and, compliant. CloudSOC enables rapid detection and response to security issues for cloud apps and infrastructure all in one platform. CloudSOC can protect sanctioned and unsanctioned use of the cloud platform within your organization with the following initiatives:

- Monitoring, logging and analyzing user and admin activity
- Enforcing access controls to prevent misconfigurations
- Detecting and remediating risky exposures in different cloud instances
- Defending cloud storage from advanced malware and APTs
- Detecting compromised accounts with user behavior analytics
- Detecting and restricting misuse and *shadow* cloud instances

Symantec Cloud Workload Protection automates security for cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and administrative burdens.

Rapid discovery, visibility, and elastic protection of cloud workloads enable automated security policy enforcement to help protect applications from unknown exploits.

In addition, with potentially thousands of cloud resources deployed across multiple regions and multiple clouds, Symantec Cloud Workload Assurance provides visibility into cloud environments, assessment of cloud security posture, and enforcement of security and compliance policies. Organizations can also have visibility and control of the cloud management plane, which is used to manage and configure cloud resources such as launching virtual instances or configuring virtual networks. The solution continuously monitors a cloud environment for resource misconfigurations that can expose data to the public internet. It extends the ability to resolve issues quickly with easy-to-follow, guided remediation steps developed by security analysts and compliance experts.

Symantec solutions for securing the cloud infrastructure provide organizations with a comprehensive view into who is using the cloud and how they are using it. By deploying Symantec CloudSOC CASB, Symantec Cloud Workload Protection, and Symantec Cloud Workload Assurance, organizations can help protect their cloud environments from misconfigurations, misuse, attacks, threats, and data loss.

Securing Data

Symantec Information Security secures data stored on-premises and in the cloud. It provides total visibility and control of data flowing in, out, and across your organization's extended perimeter. Our leading DLP solution integrates with CASB, web, and email gateway technologies to find data stored on endpoints, servers, file shares, databases, SharePoint, and more. Underpinning the integration is a single data protection policy giving you consistent and up-to-the-minute protection, avoiding the hassle of policy duplication. The Symantec integrated solution delivers Zero Trust controls, today. Consider a remote user on an unmanaged device looking to access SaaS applications. With our innovative Mirror Gateway, part of an integrated SASE solution, they get a high-quality security and end-user experience without the need for a reverse proxy or agent installed on the device.

Analytics and Automation

Efficient investigation and remediation processes are critical to any Zero Trust approach. Symantec solutions provide the telemetry that feeds our targeted attack detections, the deep forensic records that speed investigations, and powerful tools to quickly remediate breaches. Built on strong preventative protections in

endpoint, network, email, and cloud infrastructure, we integrate data-driven analytics and reporting across all control points and create a way to capture telemetry from other solutions within the security stack through our Integrated Cyber Defense Exchange (ICDx) technology. ICDx collects data, normalizes, and then correlates it, analyzing events across a wide range of control points, including third-party solutions, to deliver rich threat intelligence to analysts.

The Symantec Global Intelligence Network (GIN) is one of the largest civilian security threat intelligence networks in the world. It applies artificial intelligence to analyze over 9 petabytes of security threat data. It offers the broadest and deepest set of threat intelligence in the industry—the biggest global footprint of threat intelligence. We have spent more than two decades collecting data, applying advanced analytics and machine learning, and using our own threat experts to review and interpret the results. The GIN supplies threat intelligence to all our cyber security solutions. It is the fuel that makes our industry-leading technologies protect businesses more completely.

Symantec Security Analytics delivers enriched, full-packet capture for full network security visibility, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic. Armed with this detailed record, you can conduct forensic investigations, respond quickly to incidents, and resolve breaches in a fraction of the time you would spend with conventional processes.

Symantec Information Centric Analytics (ICA) is a User and Entity Behavior Analytics (UEBA) technology and a core component of our Symantec Data Loss Prevention (DLP) solution. It enables rapid identification of insider threats and cyber breaches. Through centralized analytics, extensive dashboards, and in-depth metrics, ICA escalates those issues that might otherwise go unnoticed or demand complex analysis. With automated remediation recommendations, ICA provides organizations with the visibility and workflows necessary to directly reduce exposure to sophisticated threats, greatly reducing manual effort.

Summary

Achieving Zero Trust is a journey and requires the integration of many types of security tools that have traditionally operated in their own silos. Many of these tools may already exist within your enterprise, some delivering value but likely with the potential to deliver even more. Customers need a partner to weave all of these disparate systems together—a partner who can also help fill in the gaps where they exist. Broadcom is that strategic partner. Our Symantec security portfolio delivers endpoint, network, information, and identity security across on-premises and cloud infrastructures, to provide the most complete and effective Zero Trust solution in the industry. Our Integrated Cyber Defense technology can weave these products and your existing security solutions into a platform that can secure your workforce, your data, and your workloads to deliver superior visibility and control.

To learn more visit symantec.broadcom.com/zero-trust.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

Zero-Trust-FW-SB100 May 7, 2021