Solution Brief

Symantec
A Division of Broadcom

Five Steps to Zero Trust Network Access

Introduction

The network perimeter is dissolving. Cloud-based data centers have abstracted traditional data centers into dynamic, software-defined entities. The new data center is easy to deploy and destroy and is often managed using APIs and code.

On top of that, a remote workforce is increasingly using their own devices for the sake of productivity, raising questions among security practitioners about the relevance of the castle-and-moat approach for keeping attackers outside the network perimeter.

The attempt to prevent attackers from getting into while allowing users to access remotely, has quickly turned into a lost cause, with red teams (and attackers) easily gaining the initial foothold inside the network, and freely moving laterally across the data center.

The Zero Trust Network Access (ZTNA) approach is becoming more popular across security and operation teams as it can address many of the shortcomings of the traditional castle-and-moat approach. However, the interpretation of Zero Trust can vary between vendors, analysts, and security practitioners.

Figuring out the right way for an organization to implement ZTNA in its environment can be daunting and can prevent the organization from moving toward better security and simpler

In this guide, we will discuss the five steps to achieving a ZTNA model in your the network environment.

Step 1: Figure Out the Right Identity and Access Management for Your Organization

The most basic building block of any modern access approach is the identity; just as the most common attack vector is compromised identity.

When adopting the ZTNA approach, you must be able to trust the user's authentication and, based on that, provide access to the organization's resources.

User authentication must abide by the following critical elements:

- Choose a *single source of truth* for your IAM where all users are authenticated and provided with the correct roles for authorization
- Enable MFA for the sensitive accounts; consider widening this to all accounts
- Have a clear logging and auditing mechanism for user's authentication information
- Have in place a basic identity governance to manage the user's role assignments and onboarding, role transitions, and off-boarding within your IAM solution

Step 2: Differentiate Managed and Unmanaged Devices Used for Access

Once we can trust the user's authentication, we have to make sure that we tie the authentication to the user's device. There's a big difference between a user authenticating from a corporate-managed device, compliant with the organizational policies, versus the same user authenticating from their personal device without any security measures. The ability to differentiate between managed and unmanaged devices is critical when looking into the context of the access request.

In more advanced scenarios, the device's compliance, as well as any risk identified on the device (such as potential malware), can be leveraged to determine the level of access allowed for any given request. User authentication must abide by the following critical elements:

- Have an up-to-date inventory of your managed devices
- Define access scenarios for managed versus unmanaged devices
- Select your endpoint security solution (EDR) to allow dynamic verification of the device compliance and security state

Step 3: Map Your Access Scenarios

Dip your toe in the water first. Migrating the entire organization to a new access paradigm all at once is a task next to impossible. Such a process is likely to raise concerns from the different parties involved. To successfully implement ZTNA, you will have to slowly build the stakeholders' trust in the Zero Trust security model and tackle each concern as it comes. Luckily, the migration process can be easily managed in stages.

Start with an access scenario where ZTNA will generate the biggest value and do this as quickly as possible. Begin with mapping the existing access scenarios. You can do this either by destination or by source: the destination being the resource that's accessed and the source being the user and device accessing said resource. A sample map could be similar to the following:

By Destination (resource)	By Source (user/device)
Cloud-based data centers (as part of a digital transformation project)	Remote and mobile workforce accessing corporate applications
Production IaaS and PaaS workloads across multiple cloud vendors and multiple data centers and regions	Third-party contractors and business partners using their own devices
Services hosting sensitive information, accessed remotely by employees	Engineers who require just-in-time privileged access to production servers

Now that you have a clear view of your organization's different access scenarios, you can prioritize the ones which will benefit the most from the increased security and the reduced operational overhead—the two immediate results that you can expect from migrating to Zero Trust Network Access.

Step 4: Select a ZTNA Solution

Now it's time to evaluate the different Zero Trust Network Access solutions available on the market to see which one provides the best match for your specific requirements. The following is some key criteria to consider:

- **Should the platform be cloud-based or on-premises?** In most cases, a cloud-based solution, delivered as a service, would be the preferred choice due to reduced maintenance requirements as well as a lower TCO.
- **How well does the platform integrate with your existing IAM, Device Management/EDR, SIEM, and UEBA solutions?** Any ZTNA solution requires as much context as possible to provide the right access level at the right moment. The better the chosen platform integrates with your existing infrastructure, the more context it will have to perform the access decisions.
- **Do you need just access, or governance of the user's actions? Do you need a platform that only provides access to cloud-hosted and on-premises corporate resources, or would you want to govern the user's activities when accessing the remote assets?** If you wish to block SSH commands or downloads of sensitive files, or allow access to only a specific set of URIs, you need a ZTNA solution that can provide both the access and the governance.

Step 5: Migrate Network-Level Access Policies to ZTNA Policies

When you have your IAM, EDR, device inventory, and access scenarios all mapped out, and the ZTNA technology selected, you can begin the transition to Zero Trust Network Access with the first scenario identified. As each application, service, and workload becomes accessible via your Zero Trust Network Access solution, you should immediately block all of the network-level access to it. Your resources are then fully cloaked and isolated from both the internet and the user's network and are accessible via the ZTNA only. This access is, of course, based on the user's identity and the device.

Once your applications, servers, or workloads are fully isolated and cloaked, they are completely protected from lateral movement and network-level attacks, both of which are common attack vectors in multiple breaches.

Don't Forget Your Users

Your users, their satisfaction, and cooperation levels are critical to the success of this process. So before you hit the button, make sure the users understand how to access their corporate services, applications, and workloads and how to provide you with immediate feedback. Adding services and applications is easy and quick. Let your users appreciate and benefit from the new speed of your operation.

Validate the successful implementation of the access model via feedback sessions and interviews with your users.

Summary

To conclude, implementing a Zero Trust Network Access solution in your organization doesn't require a complex, multi-year project. In today's agile world, you can start with a simple access scenario built on the basics of identity and device, which most organizations already have.

Solution Brief

Symantec® Secure Access Cloud™

Symantec enables security and IT teams to create Zero Trust Network Access architecture without traditional VPN appliances. Symantec Secure Access Cloud securely connects any user from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate 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 and can be deployed in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. Symantec Secure Access Cloud provides full governance and real- time enforcement of users' actions in each corporate application.

Symantec™
A Division of Broadcom

For more product information: broadcom.com

SYM-ZT-Five-Steps-SB100 November 10, 2021