THINKING OUTSIDE THE PERIMETER

Zero Trust and Digital Transformation

WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Modern enterprise security is a complex task of managing constantly changing risks from multiple, varied locations. Perimeter-based approaches have always been a critical part of enterprise network security, but they are no longer relevant to modern applications. Legacy architectures were designed to stop people from getting into a protected network. In modern enterprises, the larger threat isn't people getting in, it's large amounts of data getting out. Traditional networks were also created when most people in a company worked directly for that company and did most of their work in a finite number of physical offices. Anyone who has interacted with a modern enterprise knows that hasn't been the case for decades. In addition, many applications themselves operate outside the traditional firewalls, for example, in public clouds. Smart companies embrace better options for controlling access to applications and data.

Today's risk management forerunners are using authentication and authorization schemes to keep out attackers and protect against data exfiltration. When someone or something wants to access data, a smart risk-management system weighs the value of data against the assurance of three things: that the person is really there, that they are using secure tools, and that they are authorized to access the data. It turns out that whether that person is inside or outside the corporate network is not a reliable indicator of any of those three assurances. Customers, employees and partners are increasingly mobile, and consume your apps and other resources from every network, not just your own.

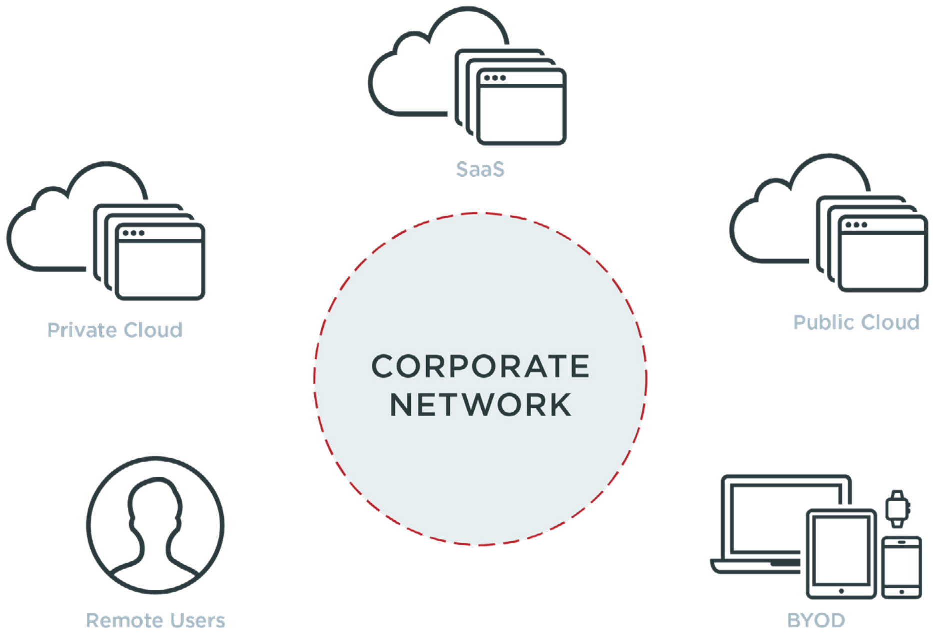

Figure 1: Today's users, devices and resources often interact entirely outside the corporate perimeter

Zero Trust is the security paradigm for the modern digital enterprise. In this white paper, you will learn about its philosophical components, how adopting this model can lead to increased security, agility and productivity across your organization, and how to best make the transition to the Zero Trust architecture to achieve your digital transformation goals.

THE ZERO TRUST PHILOSOPHY

The philosophy of Zero Trust networks comes from an unconventional idea: that the network a request originates from is a weak indicator of whether that requestor should be allowed to do restricted things. The idea is that an enterprise should have zero trust in the user's network as an indicator of security; in fact, it can give a false sense of security that can cause your Security Operations Center to trust traffic that would normally raise a red flag, just because the user is behind a firewall. Whether the identity entering any domain is a customer, a partner, an employee or other, it must be verifiable beyond the edge and into the backend components such as microservices and/or serverless functions.

There are five building blocks to this philosophy:

1. Validating the Network is No Longer Enough

Customers access your applications from public wi-fi in coffee shops and airports on a regular basis. Your employees and partners must also be able to do the same, using the public and private networks available wherever they might be. Digital transformation also requires applications and services in a variety of public and private clouds to interact with your business applications. Consequently, network validation can no longer exist to validate insider vs. outsider access. Every user, device and application is subject to the same rules, regardless of network locality. This means that even critical high-risk applications have to be exposed to the open Internet. After all, today's corporate network IS the Internet.

2. Authenticate the User

Intelligent authentication is the backbone of a Zero Trust security architecture. This means the user should have multiple "factors" that prove their identity. There are three possible factor categories: something the user knows (like a password), something the user has (like a phone), and something the user is (like a fingerprint). Different user activities should require different levels of authentication. Reading email might only require a password. Issuing a paycheck might require a password and proof of ownership of a private key stored on a hardware device.

3. Authenticate and Validate the Device

Sometimes valid users can be tricked into doing work on compromised devices. If the computer or phone that the user is working on is compromised, critical enterprise data and passwords will be compromised, even if the user has been strongly authenticated. Device identification and certificate issuance can be leveraged to check whether the user is working on validated hardware that hasn't been tampered with.

4. Authenticate the Application

Even if we have a valid user on a registered, validated device, they still might be missing a critical security patch. They might have been conned into installing a malicious browser plugin. They might be using an imposter application. Any of these cases could allow an attacker into a critical system. Methods of application validation vary widely. Some things, like OS version, can be accomplished through device management. Others, like validity of an OAuth client registration, require newer and tougher security standards like Proof Key for Code Exchange and Token Binding.

5. Authorize the Transaction

Finally, the transaction itself must be authorized. A central authorization engine must judge whether this user is allowed to perform this transaction. The default answer should always be “no,” unless there is enough information to make a decision. This may involve static rules like “only employees can send corporate email” and a heuristic rule like “only users with a risk score below 65 can view the corporate directory.” A risk-scoring system employs a number of weighted variables like behavioral biometrics, continuous authentication, location, time and comparison against patterns of past attackers to determine how likely it is that the current transaction is malicious.

MAKING THE TRANSITION

No enterprise is ready to put 100 percent of their applications on the open Internet today. Fortunately, it's easy to get started. Customer-facing and some partner-facing apps are already publicly accessible. For their internal apps, enterprises are organically and gradually adopting the Zero Trust methodology as they onboard new services that run outside their domain (e.g., cloud services) and as they build new applications or re-build legacy applications using modern architectures.

Transitioning an existing application to be Internet facing is less risky than you might expect. One of the largest risks is that current employees will be locked out of doing their work due to the new, more stringent, authentication and authorization policies. Fortunately, traffic can be monitored before the transition to see how many people would be able to accomplish their daily tasks under the proposed architecture. Problems can be rectified before the transition is made to ensure that no one is locked out. Many enterprises also dip a toe in the water by building one new non-critical application outside their firewall and seeing how it goes.

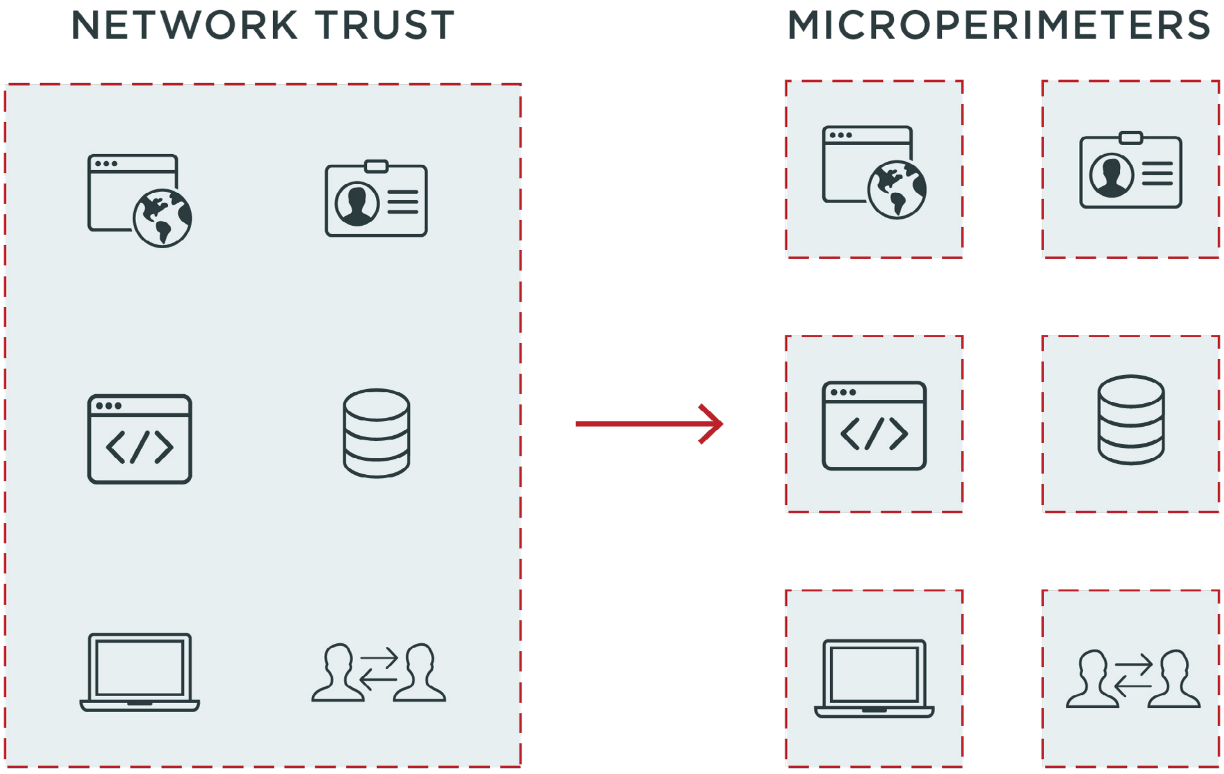

Figure 2: Transitioning from network trust requires enhanced security at each point of access

BENEFITS OF SWITCHING

Zero Trust architectures provide organization-wide benefits ranging from improved security, agility and productivity to reduced costs and efforts for security teams. Above all, however, is a defined path forward for business leaders to proceed with digital transformation without fear of compromise or frustration from burdensome security controls. Zero Trust provides the means for security no matter where resources are deployed or which types of users require access on what devices. In a business context, Zero Trust becomes a framework to expose sensitive data, applications and infrastructure to business partners without friction. The granular controls available under Zero Trust also support improved compliance with regulations such as PCI and HIPAA. Collectively, the business case for Zero Trust is defined in its enablement of digital transformation.

Benefits to Productivity

Many professionals already know something that can come as a surprise to security teams: Firewalls are a pain point, and they reduce productivity. Traditional firewall security does not lend itself to the methodology of dynamic access control required by Zero Trust, nor the self-service capabilities needed for seamless access. VPN connectivity can be easy with the right tools and configuration, but without them, employees are often locked out of the tools they need to get work done for hours while help desk tickets are resolved. Putting applications on the open Internet makes it easier and faster for employees to sign into their applications and start working from anywhere. It also enables security teams to provide the right balance between security and productivity, increasing security for resources with higher-risk profiles and reducing friction for low-risk resources.

Benefits to Security

Many enterprises also benefit from an improved security posture after implementation of Zero Trust architectures. By intelligently verifying users and devices, limiting lateral movement and enforcing least privilege at each point of access, the impact of insider attacks as well as those executed with compromised credentials can be minimized. As bad actors search for the easiest (least expensive) ways to profit from malicious activities, a Zero Trust architecture makes attacks more expensive by reducing the value of each stolen credential and reducing the efficacy of phishing attacks as second factors must also be compromised for those attacks to succeed.

These rigorous authentication and authorization policies required to execute Zero Trust should exist in every enterprise. In addition to supporting access policy enforcement with increased granularity, log data produced at each point of access can help to shorten SOC response times to ultimately minimize the impact of a breach. They also prevent a facade of security from taking hold in an organization, with the false comfort of having a firewall in place causing a lack of proper security investment and rigor. For example, many API development teams don’t test the security of APIs that can be accessed only from inside a firewall.

Benefits to the Bottom Line

By reducing friction, Zero Trust lets organizations more easily take advantage of new business opportunities, multiply revenue streams and drive profits. In addition to top-line growth, Zero Trust architectures reduce bottom-line costs. By leveraging intelligent identity solutions to automate adaptive access, organizations reduce the need for writing complex policies for each and every scenario in which access might be granted or denied. As all access under Zero Trust is authenticated and authorized, access management for third-party vendors, partners, customers and other user populations becomes streamlined and easily governed.

Further cost-saving opportunities exist around exploring VPN, Privileged Access Management and Network Access Control usage within an organization. A Zero Trust approach can streamline your use of these perimeter-centric security tools, resulting in cost savings both from a licensing perspective and operationally reducing the need to manage multiple sets of tools.

CONCLUSION

Zero Trust architectures have been successfully deployed at many large enterprises, and more companies are adopting the philosophy every day. Firewalls are a weak indicator of whether network traffic has the potential to be malicious. Indicators like authentication, authorization and device management can do that job much more effectively. The cost of firewalls in terms of financial expenses, productivity drops and usability headaches is driving more and more companies to the realization that the benefits don’t pencil out—and that investment is better spent executing on Zero Trust architectures.

To learn more, visit pingidentity.com/en/initiatives/zero-trust.html