ZERO TRUST AND BEYOND

A Journey For Everyone

censornet.

ZERO TRUST... MAXIMUM SECURITY_

Zero Trust and ZTNA (Zero Trust Network Access) are two of the most important concepts in enterprise security. But your business can benefit from them too.

This guide will help you understand Zero Trust, discover how it can benefit your organisation and assist you with taking those crucial first steps towards the future of your own cloud security.

A BRIEF HISTORY OF ZERO TRUST:

2007_

The Defence Industry Security Association (DISA) introduced Black Cloud, a forebear of Zero Trust. It removed visible DNS information from application infrastructure so it could not be detected. This made applications impervious to many forms of network-based attack, including scans, vulnerability exploits, Dos and DDoS attacks.

2010_

John Kindervag, principal analyst with Forrester, coins the term Zero Trust.

2011_

The Cloud Security Alliance unveils Software Defined Perimeter (SDP). Connectivity in SDP is based on a need-to-know model in which device posture and identity are verified before access is granted.

A CRISIS OF TRUST?

The death of traditional perimeters has been greatly exaggerated – until now.

During the pandemic, the perimeter finally perished as companies around the world sent their staff home to work outside the protection of corporate networks. Staff now login from outside the corporate network using 4G and 5G as well as their home network. The applications used every day are in the cloud.

In this new normal, firewalls, VPNs and other traditional defence systems are no longer sufficient to protect a newly distributed workforce. Neither are passwords or other traditional identifiers. Now, the only place to deliver effective security is in the cloud.

Work is no longer a place but an activity, which means security should be designed around an entirely new perimeter built on identity and context – which is where Zero Trust and ZTNA come in.

CENSORNET RESEARCH FOUND THAT JUST 34% OF SECURITY PROFESSIONALS FEEL "VERY PREPARED" TO SUPPORT EMPLOYEES WORKING FROM HOME SECURELY.

WHAT IS ZERO TRUST AND WHO IS IT FOR? (ANSWER: EVERYONE)

Zero Trust is a security model that turns the old idea of "connect then authenticate" on its head when it comes to providing secure access to network resources. **It's a paradigm in which no-one is trusted.**

Rather than inviting users to log into apps using a risky online portal, the Zero Trust model places an intermediary layer between users and the corporate network, resources and applications.

With Zero Trust, users must prove their identity before being granted access. This security posture is designed to stop hackers from gaining easy access to networks through the web applications used by an organisation's users or workers.

Zero Trust is crucial in the age of remote working. The Zero Trust approach involves trusting no-one and assuming no entitlement until trust is earned. **Importantly, this trust must be continually assessed and re-evaluated.**

In addition to verifying the identity of the individual and the device gaining access to the corporate network via the ZTNA layer, **Zero Trust rules and policies can adapt based on the observed behavior of a user or device.**

The new rule is: "Authenticate, then connect."

> **"There are products that work well in Zero Trust environments, but if a vendor comes in to sell you their 'Zero Trust' product, that's a pretty good indication that they don't understand the concept"**
>
> John Kindervag

UNDERSTANDING ZERO TRUST NETWORK ACCESS

If Zero Trust is the idea, Zero Trust Network Access (ZTNA) is the technology which turns the philosophy into a reality.

Before ZTNA, organisations relied on inherently weak identifiers when granting access to the corporate network.

> **"We've used ownership and control of physical assets and location as an implicit proxy for trust... This is a flawed security paradigm."**
>
> Gartner

ZTNA has two main predecessors: Black Cloud and Software Defined Perimeter (SDP). However, it differs from them because it incorporates a level of dynamic trust, **where access is modified based on behaviour**. This adaptability differentiates ZTNA from SDP and Black Cloud.

AUTHENTICATE THEN CONNECT

AS CLOUD ADOPTION HAS RISEN, CYBER ATTACKS HAVE GROWN BY A STAGGERING 50%

With Zero Trust Network Access, authentication comes first via a middle or intermediary ZTNA layer that confirms an individual's identity but also the context in which they are attempting access. Only when the individual has been authenticated are they granted an onward connection to applications and data.

The ZTNA layer, or ZTNA controller, becomes the gateway to an organisation's assets – whether SaaS or legacy data centre apps – isolating systems from potential trespassers or hackers, and hiding applications from the internet.

This layer makes applications impervious to many forms of network-based attack including scans, vulnerability exploits, DoS and DDoS attacks.

ZTNA hides assets from prying eyes. It's focused around giving organisations the ability to implement a need-to-know approach when it comes to data or apps, rather than leaving them open to any individual or device that has passed through authentication.

For many organisations, ZTNA is likely to be the first step on a road to the next great evolution in security: Secure Access Service Edge (SASE).

TRUST NO ONE

CONTEXT AND IDENTITY ARE THE NEW PERIMETERS

To earn the trust of a ZNTA controller, someone who logs on from a remote location may undergo the usual password test and Multi-Factor Authentication (MFA) process.

Behind the scenes, a ZTNA layer analyses the identity of the person trying to log on as well as their behaviour, to provide context.

It works to prove the identity of a person trying to log in, as well as establish if they are behaving in a way that's considered "normal".

WHAT IS NORMAL?

Here are some of the context information points a ZTNA could look for:

LOCATION

Has the person logged on from a known location?

TIME

Is the login happening at an expected time?

IP ADDRESS

Has the user moved to a different address?

DEVICE INTEGRITY

Is the device compromised or behaving strangely?

UNUSUAL BEHAVIOUR = SUSPICIOUS BEHAVIOUR.

Is a trusted employee downloading a large volume of customer data that wouldn't usually be required in their role? Have they logged in from one location and then attempted to gain access from a city on the other side of the world?

If a ZTNA finds the answer to these questions is yes, it could respond by blocking access to the user or device that's behaving strangely. It could also restrict their activity in some way, perhaps by limiting them to read-only access or limiting access to sensitive data.

It's not just user behaviour that can be monitored, but entity behaviour as well. There could be anomalous activity that suggests the device is infected with malware – another trigger point for blocking or limiting access.

To avoid impacting productivity, flexibility is paramount. The system must be adaptable and dynamic, monitoring the behaviour of an individual and device to constantly ask: "What's been going on? Why is that user accessing that data? What are they doing with the data and does that make sense from a business-as-usual perspective?"

Currently, few ZTNAs on the market are this advanced.

Even if the ZTNA solution does support UEBA (user and entity behaviour analytics), the overheads of management and administration are often considered too high, as well as the risk of impacting legitimate business processes.

But as ZTNA becomes the industry norm, behavioural components are likely to be adopted by an increasing number of organisations.

HOW TO IMPLEMENT ZERO TRUST _

These guidelines are based on the sage words of John Kindervag himself, who warned that the attack surface is massive and always growing.

1_ DEFINE YOUR PROTECT SURFACE(S)

Start small by locking down applications which are not mission critical. Don't start with the financial back-end system or ERP application running in the data centre. Zero Trust is not binary. It can be implemented one protect surface at a time. By taking an iterative approach Zero Trust does not have to be disruptive.

2_ MAP THE TRANSACTION FLOWS

Map flows and map users to applications, actions within those applications and associated data.

3_ ARCHITECT THE ENVIRONMENT

When architecting the Zero Trust environment start from the inside out, not the outside in. Move controls closer to the user or device. Reduce services delivered from DMZs and segment users from the data centre network. Log all user and application layer activity.

4_ FORMULATE THE ZERO TRUST POLICY

Be sure to focus on context and conditional policies. Leverage existing technologies such as IDaaS (or Cloud IAM) and adaptive or context-aware MFA. Apply least privilege everywhere.

5_ MONITOR AND MAINTAIN THE ENVIRONMENT

Logging identity edge cases before changing business processes to fix or accommodate them as necessary.

KEY BENEFITS OF ZTNA:

- Greater visibility reduces risk
- Improved control of cloud environments and SaaS applications
- Reduced likelihood of breaches (and lower impact if there is one)
- Supports compliance audits with improved user activity logging
- Better business agility (adopting new processes, workflows and applications)
- Less organisational friction (removing the sub-optimal VPN experience)

CENSORNET – JOIN US ON THE JOURNEY

Most large organisations are already adopting ZTNA. However, for companies with a few hundred to several thousand users, the challenge can seem difficult, if not impossible.

It needn't be.

Censornet's solution already allows companies to handle access requests 24/7 or to endlessly reconfigure their context-based rules to reap the many benefits of Zero Trust security enjoyed by large enterprise organisations.

At Censornet, we have a proven track record for delivering apparently complex, innovative technology in a simpler way that's easy and affordable, with very rapid "time to value".

We're already capturing typical patterns of behaviour relating to users, devices and other entities – such as mailboxes or specific cloud applications.

We already understand identity – fully integrating with AD or Azure AD, or both.

We already have the Autonomous Security Engine built to assess trust and risk continuously.

Soon, ZTNA will be the norm. We can make it easy for you to keep pace with acknowledged security standards and let you make the next logical step towards a safer future.

BEYOND ZERO TRUST

ZTNA is itself a waypoint on the journey to Secure Access Service Edge, or SASE. This is a term coined by Gartner to describe a combination of Network-as-a-Service and Security-as-a-Service which offers a single, cloud-based solution to the global security needs of a mobile workforce.

There are some things you can do now to smooth the way to adopting ZTNA – and eventually SASE. Even if you're not currently planning to adopt a Zero Trust approach, the decisions you make today will affect your ability to employ this technology in the future. It's all about making sure you don't set off down a path that could prove to be a dead end.

FIRST STEPS ON THE ROAD TO SASE

1_ Begin to think about identity and Identity-as-a-Service (IDaaS) for Single Sign-On

2_ Consider context – starting with adaptive (or context-aware) Multi-Factor Authentication (MFA)

3_ Monitor and log all user activity

4_ Review admin rights to ensure least privilege

5_ Limit further investment in VPNs and plan to phase them out

6_ Start evaluating cloud-based ZTNA services for application access

7_ Reduce services delivered from DMZs

8_ Segment users from the data center network

9_ Ringfence critical applications

10_ Carefully consider management of uncategorized web content and links in email.

FIND OUT MORE

Call +44 (0) 845 230 9590
or visit
www.censornet.com

ZERO TRUST AND BEYOND

A Journey For Everyone

censornet.