
# ZERO TRUST AND BEYOND

A Journey For Everyone

ZTNA

BLACK BOX | censornet.

# ZERO TRUST... MAXIMUM SECURITY_

Zero Trust and ZTNA are two of the most important concepts in enterprise security. But any business can benefit from them.

This paper will help you understand Zero Trust, discover how it can benefit your organization 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.

**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.

**2014_** Google rolled out BeyondCorp, its implementation of the zero trust security model that shifted access controls from the network perimeter to individual users and devices.

**2019_** Gartner listed Zero Trust security access as a core component of secure access service edge (SASE) solutions.
The National Cyber Security Centre (NCSC) recommended that network architects consider a zero trust approach for new IT deployments, particularly where significant use of cloud services is planned.

**2022_** Nearly half of UK businesses (45%) use personally owned devices to carry out regular work-related activities.[1]



1 www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

# 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 on from outside the corporate network using 4G and 5G as well as their home network. The applications used every day are in the cloud.

Over half (51%) of mid-market organisations have not yet purchased cybersecurity products designed to specifically protect against threats for hybrid and remote workers.[2]

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. With many hybrid workers not specifically protected, 41% of mid-market firms report that future-proofing their cyber defences "needed development".[2] 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 SHOWS ONLY HALF (51%) OF MID-MARKET ORGANIZATIONS HAVE COMPLETE CONTROL OVER THE USE OF THEIR CLOUD APPLICATIONS.[2]**



2 https://cloud.censornet.com/cybersecurity-red-alert-1

# 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, organizations 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

Zero Trust 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 behavior**. This adaptability differentiates ZTNA from SDP and Black Cloud.

ZTNA hides assets from prying eyes. It's focused around giving organizations 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 organizations, ZTNA is likely to be the first step on a road to the next great evolution in security: Secure Access Service Edge (SASE)

# AUTHENTICATE THEN CONNECT

With Zero Trust, 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 organization's assets – whether SaaS or legacy data center apps – isolating systems from potential trespassers 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

**AS CLOUD ADOPTION HAS RISEN, ONLY FOUR IN TEN (37%) MID-MARKET ORGANIZATIONS ARE ABLE TO PREVENT CROSS-CHANNEL ATTACKS. FOR EXAMPLE, ATTACKS THAT START VIA EMAIL, BUT CONTINUE OVER THE WEB OR CLOUD APPLICATION CHANNELS.[2]**



2 https://cloud.censornet.com/cybersecurity-red-alert-1

# TRUST NO ONE

## CONTEXT AND IDENTITY ARE THE NEW PERIMETER

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 behavior, 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 a ZTNA could look for:

### LOCATION

Has the person logged on from a known location and device?

### TIME

Is the logon 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 on 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 restrain their activity in some way, perhaps by limiting them to read-only access or restricting access to sensitive data.

It's not just user behavior that can be monitored, but entity behavior 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 behavior 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 behavior 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, behavioral components are likely to be adopted by an increasing number of organizations.

# HOW TO IMPLEMENT ZERO TRUST _

**ADOPTING A ZERO TRUST POSTURE MEANS CONTINUALLY REVIEWING USER ACTIVITY TO DETERMINE ACCESS PRIVILEGES.**

Make zero trust a reality at your organization by following these five steps:

## 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 center. Zero Trust is not binary. It can be implemented one protect surface at a time. Taking an iterative approach to Zero Trust means it 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 center network. Log all user and application layer activity(this will help you with step 5).

## 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

Through 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 in the event of one
- Supports compliance audits through improved user activity monitoring and logging
- Better business agility (adopting new processes, workflows and applications)
- Less organisational friction (removing the sub-optimal VPN experience)

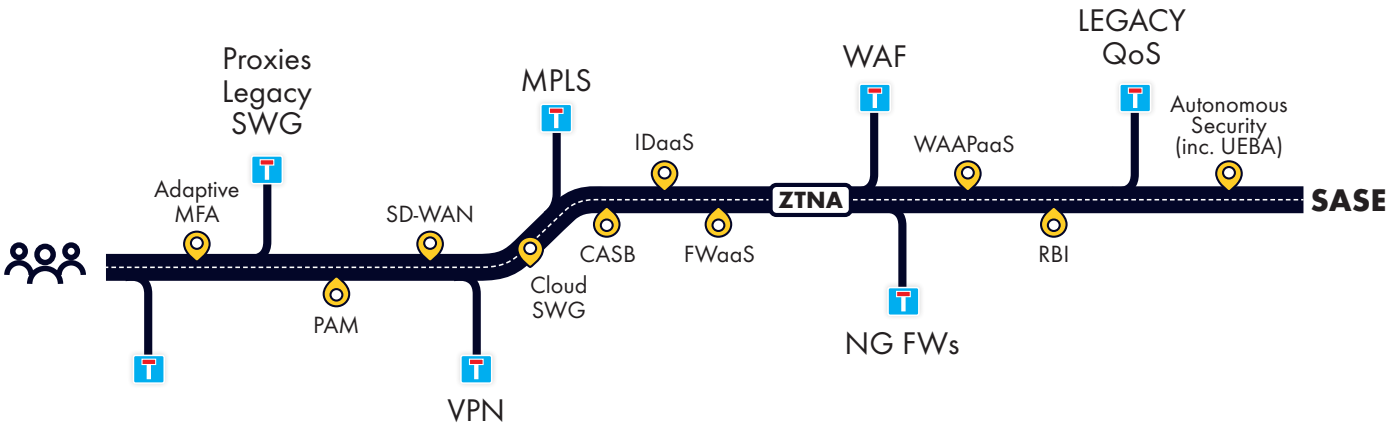
# WHAT COMES NEXT?

**ZTNA is itself a waypoint on the journey to Secure Access Service Edge, or SASE.** First coined by Gartner, SASE is used 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.

# SASE ISN'T A SINGLE PURCHASE. IT'S A STRATEGIC DIRECTION.

**THE NEXT STOP ON THE JOURNEY OF CYBERSECURITY EVOLUTION.**




## FIND OUT THE TEN STEPS YOU CAN TAKE NEXT TO HELP PREPARE FOR SASE ADOPTION

The goal of SASE is to provide the rapid, secure access which businesses require right across their ecosystem - without having to massively scale up investment and manpower. It means working smarter, not harder.

Read our guide to find out the ten steps as you prepare your journey to SASE readiness.

Scan or click QR code

# A PLATFORM APPROACH TO ZTNA

Most large organizations 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 autonomous, integrated cloud security platform does the heavy lifting. It enables mid-sized companies, often with small security teams, to automatically review access requests 24/7, and to deploy intelligent data analysis to determine context-based approvals at lightning speed.

As a result, they can reap the benefits of Zero Trust security enjoyed by larger organizations with bigger budgets to deploy.

The benefits of Censornet aren't confined to ZTNA. Our platform integrates attack intel from email, web, and cloud to ensure cyber defences react at lightning speed. For our millions of users globally, our automated solution is smarter, faster, and safer than humanly possible.

Soon, ZTNA will be the norm. By making the most of next-gen autonomous, integrated cloud security, you can keep pace, and take the next step towards a safer future.

**CENSORNET OFFERS AN IN COUNTRY CLOUD PLATFORM.**

BLACK BOX®

BLACKBOX.COM/EN-AE


**Abu Dhabi**
**Black Box Technologies LLC**
Office 19, 19th Floor.
Al Ghaith Tower,
Hamdan Street,
P.O.Box number 45526
Abu Dhabi, UAE
Phone: **+971 2 508 9002**

**Dubai**
**Black Box Technologies LLC**
Suite # 208, M Square Building
Sheikh Khalifa Bin Zayed Street.
P.O. Box number 44623
Dubai, UAE
Phone: **+971 4 3526 686**