ZTEdge™
DEFEND WHAT MATTERS

What's the Zero Trust - SASE Connection?

Contents

ZTEdge™
DEFEND WHAT MATTERS

Introduction

By every measure, cybercrime has reached unprecedented levels. Attacks are more frequent, more sophisticated, involve higher ransom demands, and impact a huge range of targets, from small businesses to vital infrastructure and government agencies. No industry or type of public service has remained untouched.

In response, businesses, not-for-profit organizations, and government agencies that have been considering moving to Zero Trust security are now actively seeking architectures that put Zero Trust concepts into practice.

The cloud-based Secure Access Service Edge (SASE) security model is widely accepted as an effective way to achieve a Zero Trust security “end-state” that provides enhanced protection for organizations' users, devices, applications and networks. This paper explores the principles of Zero Trust security and describes how SASE solutions enable organizations to move from conceptual acceptance to practical implementation.

SASE solutions enable organizations to move from conceptual acceptance of Zero Trust security to practical implementation

ZTEdge™
DEFEND WHAT MATTERS

As Cyber Crime Reaches New Highs, New Answers are Needed

In response to heightened levels of cyberattacks, the US government has issued numerous guidelines recommending adoption of Zero Trust:

- DHS cybersecurity directives for pipeline companies
- CISA Capacity Enhancement Guide on secure browsing for federal agencies
- NIST draft guidance on ransomware risk management
- White House executive order on improving cybersecurity

Cybersecurity is more crucial than ever—but current solutions are failing to protect the organizations that depend on them. Powerful players including organized crime and nation states–and their proxies--are successfully leveraging sophisticated phishing and zero-day exploits to launch ransomware attacks against businesses of all sizes. Researchers recently found that 74% of threats detected started as zero-days[1] – the highest percentage on record.

Ransomware delivery systems have been upgraded to combine email, web browsing, hacking and supply chain attacks. "Ransomware as a service" enables "any doofus to be a cybercriminal now," in the colorful phrasing of one former hacker[2]. While gallons of (electronic) ink is spilled on high-profile attacks, the lion's share of attacks are never publicly disclosed.

In the wake of some exceptionally brazen cyberattacks, the US government is taking a more active stance: The Department of Homeland Security issued cybersecurity directives for pipeline companies[3]; CISA published a Capacity Enhancement Guide[4] on securing web browsers for federal agencies; the National Institute of Standards and Technology published draft guidance on ransomware risk management[5]; and the White House issued an executive order[6] calling, among other things, on federal government agencies to adopt a Zero Trust security architecture. The executive order fact sheet also calls on private sector companies to take the same steps:

> *We encourage private sector companies to follow the federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.*

[1] https://www.helpnetsecurity.com/2021/06/29/zero-day-malware-q1-2021/
[2] https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html
[3] https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators
[4]https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Securing_Web_Browsers_and_Defending_Against_Malvertising-Guidance_for_Non-Federal_Organizations.pdf
[5] https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf
[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Perimeter-based Defense, Detection and User Awareness Can No Longer Protect You (If They Ever Did)

In the past, the conventional approach to cybersecurity largely entailed securing the network perimeter against threats by deploying firewalls and tools such as antivirus and anti-malware software to detect and block threats. The primary line of defense against phishing attacks was user education.

IT concepts and configurations have changed a lot in recent years, with the months of remote work accelerating what had long been a gradual process. Many organizations that have made headlines following ransomware attacks are now painfully aware that detection-dependent approaches cannot adequately defend against the zero-day exploits that are flooding the web and the myriad new malware variants that are developed each day. User education is likewise only partially effective, with failure rates of 1-3% for the most basic phishing attempts, and in double digits for more sophisticated lures. Of course, even one single click on a malicious URL in a phishing email is sufficient to enable ransomware to paralyze an entire enterprise.

The concept of a perimeter-based defense has been rendered obsolete as resources and computing move to the cloud, apps move to the web, and more workers are working remotely. It's a completely new ecosystem, with users who may be within or outside of the network accessing resources that may be on the network, on private or public clouds, or online.

Perimeter-based defense has become obsolete as resources and computing move to the cloud, apps move to the web, and businesses move to remote work.

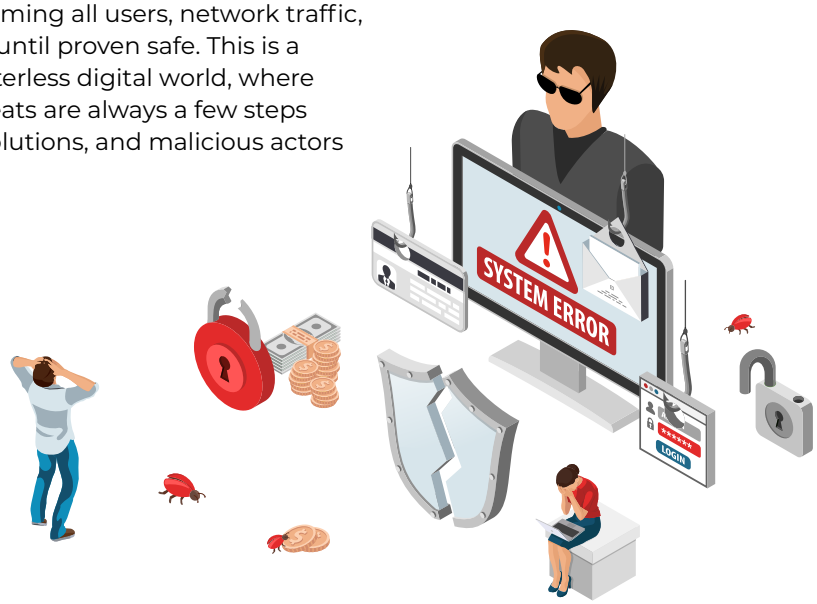
ZTEdge™
DEFEND WHAT MATTERS

The Zero Trust Security Paradigm

Zero Trust addresses both the new cyber landscape and long-standing security challenges by assuming all users, network traffic, websites, and emails are dangerous until proven safe. This is a prudent approach in today's perimeterless digital world, where zero-day exploits and other new threats are always a few steps ahead of signature-based security solutions, and malicious actors are ever-resourceful.

The assumption of danger leads directly to the basic principles of the Zero Trust approach:

- Never trust, always verify
- Grant only least privilege access
- Assume breach



The assumption of danger leads directly to the basic principles of the Zero Trust approach

Never trust, always verify

Grant only least privilege access

Assume breach

As these principles indicate, Zero Trust is not a specific action, service or technology but rather, a security philosophy and strategy that must guide and underpin every aspect of cybersecurity management.

So when we talk about today's organizations, whose operations depend on diverse combinations of legacy hardware and software, cloud-based resources and SaaS apps, transitioning to a Zero Trust approach – just what does that mean? Where do they start?

How do organizations "do" Zero Trust? Where do they start?

ZTEdge™
DEFEND WHAT MATTERS

A Digital Architecture That Puts the Paradigm into Practice

Establishing secure access from anywhere, to all resources, from wherever users are, in accordance with Zero Trust principles is no simple task. On the one hand, different processes and protections are needed for different paths. On the other, elements that enable application of the three basic Zero Trust principles form a common core for all digital activity in today's distributed organizations.

Secure Access Service Edge platforms—known as SASE—integrate diverse technologies that intelligently enable secure access for users anywhere, to the resource they need, in accordance with Zero Trust tenets. In order to apply the principles consistently, efficiently and across all resources, devices and users of today's distributed organizations, SASE platforms operate at the cloud edge, via which all access is routed.

		Resource location		
		Local/Private cloud	Public cloud/SASE	Web
User location	Local	ZTNA	CASB Anti-virus	SWG + RBI Firewall + IPS
	Branch	SD-WAN ZTNA	CASB Anti-virus	SWG + RBI Firewall + IPS
	Remote	ZTNA	CASB Anti-virus	SWG + RBI Firewall + IPS

To cover each of the myriad access scenarios encountered by users in their everyday work, SASE platforms include a large variety of functions and technologies. One set of technologies, such as SD-WAN, firewalls, anti-virus, and SSL inspection, are familiar solutions that are now being applied at the cloud edge, rather than at the physical network perimeter, as they previously had been. A second set, including cloud access security brokers (CASB), secure web gateways (SWGs) with remote browser isolation (RBI), and Zero Trust network access (ZTNA) address newer access scenarios that have more recently emerged.

A third set of SASE technologies are those that support enforcement of Zero Trust controls across all of these access scenarios, in concert with the other technologies. These include identity and access management, microsegmentation, policy management, network traffic analysis/monitoring, and intrusion prevention.

Secure Access Service Edge platforms—known as SASE—integrate diverse technologies that intelligently enable secure access for users anywhere, to the resource they need, in accordance with Zero Trust tenets.

ZTEdge™
DEFEND WHAT MATTERS

Anatomy of a SASE Platform

Let's dive into each of these SASE platform elements outlined above. We'll start with the capabilities that together comprise the Zero Trust security brains that govern SASE-based controls.

Foundational Zero Trust Controls

Identity and access management (IAM)

Identity and access management (IAM) is the core verification and permission engine that controls user access to applications and resources, per the "never trust, always verify" and least privilege access principles of Zero Trust. As such, IAM encompasses a comprehensive directory of users and the detailed policies that govern their access privileges for all system resources. It also controls authentication requirements for each user, generally requiring multi-factor authentication (MFA). Additional capabilities that may be managed by the IAM function include single sign-on (SSO) and password-based and passwordless access.

Policy management

Granular policy creation and management lies at the very heart of the SASE platform—and is one of the most challenging aspects for the teams that manage it. In short, policies must be customized for each individual user and kept current as their responsibilities evolve to maintain the required granularity for least privilege access.

Microsegmentation

Microsegmentation enables organizations to strictly limit access to each network resource based on privileges stipulated in per-user policies, creating, in effect, one-to-one networks that reflect the Zero Trust least privilege access principle. Some microsegmentation technologies also restrict user visibility to only resources they are permitted to access, to prevent lateral movement in the event of a breach by a hacker or malicious insider. Thus, microsegmentation also addresses the Zero Trust principle of "assuming breach" by limiting the damage in the event of a breach.

Network traffic analysis and intrusion prevention

Like microsegmentation, network traffic analysis and intrusion prevention capabilities address the Zero Trust principle of assuming breach. Via these functions, SASE platforms constantly monitor activity on endpoints, networks and clouds, to rapidly identify anomalies and minimize impact in the event of a breach.

	IAM	Policy management	Microsegmentation	Network traffic analysis/IPS
Never trust, always verify	√			
Least privilege access	√	√	√	
Assume breach	√		√	√

ZTEdge™
DEFEND WHAT MATTERS

Zero Trust Access Controls

This group of SASE capabilities focuses on providing secure access to cloud and internet resources, and on securing access to on-premises resources from remote locations.

Cloud access security broker (CASB)

CASB controls restrict access to public SaaS cloud services to protect data, prevent malicious as well as unintentionally risky insider activity, and monitor activity, regardless of where users are when they access cloud services, or which device they are using. Only authorized and authenticated users can gain access to sanctioned cloud resources, and cloud services that are not authorized for use can be fully blocked, or certain actions – like uploading data – can be restricted.

Zero Trust network access (ZTNA)

ZTNA simplifies and secures remote access to on-premise and private cloud resources by establishing one-to-one connections between users and apps. It enforces least privilege access controls for all users, wherever they are, and prevents lateral movement on the network, thereby dramatically reducing the risks that arise from stolen credentials, brute force attacks or malicious insiders.

Web isolation gateway (SWG + RBI)

A Web isolation gateway applies threat intelligence data, secure web gateway, remote browser isolation and other protective technologies to secure user access to the web while blocking malware, ransomware, and other advanced threats. It can block suspected phishing sites or display them in a special ‘read-only’ mode to prevent users from having credentials stolen. It may also integrate content disarm and reconstruction (CDR) technology to sanitize email attachments and web documents prior to download.

	CASB	ZTNA	Microsegmentation	Web isolation gateway
Never trust, always verify	√	√	√	√
Least privilege access	√	√	√	√
Assume breach		√	√	√

ZTEdge™
DEFEND WHAT MATTERS

Traditional Secure Access Functions, Updated for the Cloud and Distributed Organizations

The final group of SASE capabilities perform familiar tasks – but on a whole different scale and at levels of sophistication never reached by their on-premises counterparts.

Cloud-delivered firewall

Just as on-premises firewalls control traffic flows to and within the old network perimeter, SASE cloud firewalls control flows throughout the entirety of today's distributed networks, to verify that they are legitimate and permitted.

Cloud SD-WAN

Cloud SD-WAN provides efficient, secure connections between main offices, branch offices and users, eliminating the need for costly MPLS lines. Critically, it also allows for "local internet breakouts", where security policies for internet use can be applied and enforced in the cloud for remote and branch users, thereby eliminating the costs, complexity and latency added by backhauling internet traffic to on-premises security stacks for screening and policy enforcement. Cloud SD-WAN, when combined with SWG and RBI, sends local branch traffic directly to the internet while ensuring Zero Trust security principles are still applied.

Anti-virus

Like its on-premises counterpart, SASE anti-virus scans web content and downloads for known threats, verifying that harmful content is blocked before it can reach endpoints.

SSL inspection

Applies policy-based web SSL traffic inspection to identify and block malware hidden in encrypted packets.

	Cloud-delivered firewall	Cloud SD-WAN	Anti-virus	SSL inspection
Never trust, always verify	√	√	√	√
Least privilege access		√		
Assume breach				

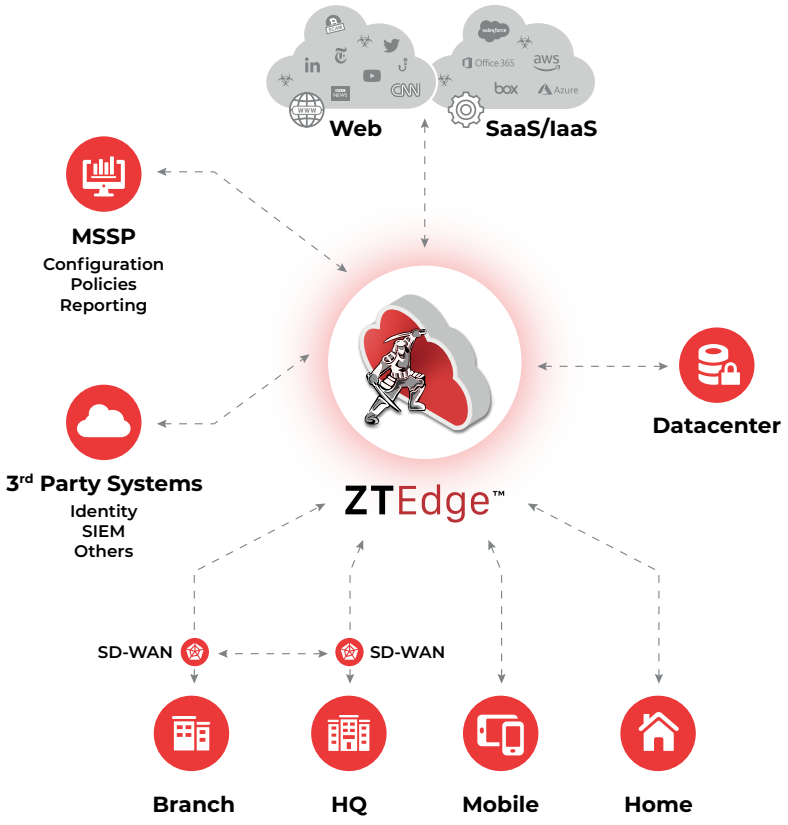
ZTEdge™
DEFEND WHAT MATTERS

Cybersecurity You Can't Afford *Not* to Have

Zero Trust is a principle-driven, comprehensive approach to securing the modern threat environment. SASE platforms apply that approach to narrow gaps that allow malware in and automate effective response in the event that it does.

Today, in a world that is dramatically different from what it was just a few years ago, Zero Trust provides the proactive, principle-driven, comprehensive approach to cybersecurity that is required to face the challenges of the modern threat environment. In a similarly integrative vein, SASE platforms provide comprehensive security solutions that narrow the gaps that allow malware in, and integrates detection and automated response in the inevitable instances when it does.

Zero Trust security, as applied via SASE, is a major advancement. And as with most major advances that require significant development efforts, the first SASE platforms were costly, complex solutions suitable for only the largest organizations – leaving midsize enterprises inadequately protected and vulnerable to attack. Fortunately, lower cost platforms that are remarkably simple for smaller organizations to manage, despite the broad capabilities they offer, are now available. With the attacks increasing in severity, frequency and reach, there is no time to lose before starting your organization on its Zero Trust journey via the adoption of SASE capabilities.



ZTEdge™

Introducing ZTEdge, the Zero Trust Cloud Security Solution Designed for Midsize Enterprises and Small Businesses

The ZTEdge security platform leverages a Zero Trust security approach to protect what matters to midsize enterprises and small businesses: their users, their networks, their data, their applications and especially their customers.

Designed with simplicity in mind and operating at the cloud edge, the platform is flexible to support businesses as they grow and transition digital operations to the cloud.

Delivered on a distributed, scalable enterprise-class cloud infrastructure, ZTEdge is available as a service provided by certified, market-leading ZTEdge MSSP partners.

Key security capabilities provided by ZTEdge include:

- Identifying users and authenticating devices
- Secure web and internet access from any location
- Secure remote access to private applications
- SaaS application access control
- Network protection and monitoring
- User-branch-internet connectivity

For more information about how the ZT Edge Zero Trust security platform can protect your organization from cyber threats

Contact us

www.zerotrustedge.com
info@zerotrustedge.com
US: (201) 767-2210
Europe: +44 (0) 1905 777970
ROW: +972-2-591-1700