Zero Trust Network Access (ZTNA)

Information resilience in the cloud

Introduction

Organizations have been migrating from on-premise infrastructure to a cloud environment at a rapid pace. Due to this migration, the network perimeter security has become less secure, pushing security professionals to approach their defence from a different angle.

The security perimeter is no longer just around the on-premises network. The perimeter has become so fluid and dynamic in nature that the boundaries, in the traditional sense, ultimately disappeared.

The introduction of cloud computing and mobile technology, along with practices such as bring your own device (BYOD) and inter-organization collaborations also contribute to a much higher-level of risk if left unmanaged and unsecured.

Insider threats continue to be a major risk. Remote workers using virtual private networks (VPN) connections expose network IPs to the internet via VPN concentrators that listen for inbound pings that hackers also can use to gain access to your network.

Unlike network-centric solutions like VPNs, Zero Trust Network Access (ZTNA), a new way to help organizations protect their data, takes a fundamentally different approach to securing access to internal applications.

This whitepaper will help you understand the core principles of Zero Trust Network Access (ZTNA) architecture and advantages along with Continuous Adaptive Risk and Trust Assessment (CARTA) Framework to help guide your digital transformation journey.

ZTNA

ZTNA, also known as the Software-Defined erimeter (SDP), is a set of cloud native technologies that operate on an adaptive trust model, where trust is never implicit, and access is granted on a “need-to-know,” least-privileged basis defined by granular policies. ZTNA gives users seamless and secure connectivity to private applications without ever placing them on the network or exposing apps to the internet.

SDP is a term coined by the Cloud Security Alliance (CSA) where organizations can now use software, instead of traditional network security appliances, to seamlessly connect remote users to privately managed applications running in multi-cloud, hybrid, or private cloud environments.

The SDP technologies are usually client-initiated which means that a client must be installed on the devices of the user for access to private applications to take place. Because of this necessity, they are not fit or certain use cases in which access from unmanaged devices such as third-party users or in cases where BYOD is important. This is where ZTNA’s service-initiated architecture comes into play.

Architecture of ZTNA

ZTNA endeavours to clear up some of the primary differences between the various vendors that participate in this zero-trust security space by dividing them into two architectural designs.

Client-initiated architectures

– ZTNA services under this category meticulously follow the original Cloud Security Alliance SDP architecture., An agent installed on authorized devices sends information about its security context to a "controller." The controller prompts the user on the device for authentication and returns a list of applications the user is allowed to access. Following the authentication of the user and device, the controller provides connectivity from the device through a gateway that safeguards services from direct internet access. This defence safeguards the applications from Distributed Denial of Service (DDoS) attacks.

Service-initiated architectures

– ZTNA services have a connector installed in the same network as the application, which initiates and maintains an inside-out connection to the cloud service where the application-to-user connection is connected together. This process takes place after the user and device are authenticated. The highlight of the inside-out connection is that it makes the applications invisible to the internet.

The main advantage of this conceptual model is that no agent is required to be installed on the user device. Because of this, it becomes an alluring approach for unmanaged devices. One of its limitation is that the application's protocol has to be based on HTTP/HTTPS which limits the approach to protocols such as Remote Desktop Protocol (RDP) or Secure Shell (SSH) over http and web applications.

Based on the organization requirements, they can choose either client-initiated architecture or service-initiated architecture models.

CARTA

Continuous Adaptive Risk and Trust Assessment (CARTA) is a security framework developed by Gartner. It is a contemporary cloud-first technology ecosystem that includes a ZTNA service, endpoint security vendors, identity providers, and mobile device management (MDM) and security information and event management (SIEM) providers all working together. Whilst zero trust in itself is important, it is only a component of a greater journey. A one-time gate at the initiation of a session is not a framework in itself. This is where CARTA comes in.

Some of the main concepts of the CARTA method include:

- Decisions, security responses, risk and trust must be continuously adapted
- The initial block or allow security assessments for access and protection leave enterprises exposed to credential theft, zero-day, targeted attacks, and insider threats
- Trust and risk must not be static, rather dynamic and must be continuously assessed as communications take place and additional context becomes available
- Digital business outcomes can only be enhanced when digital trust is flexibly managed as a set of fine-grained measures of confidence with multidimensional risk and response attributes

So, be it SDP or ZTNA, identifying a user and granting them access to specific applications instead of the enti e network is an integral piece of the overall CARTA framework.

ZTNA endeavours to clear up some of the primary differences between the various vendors that participate in this zero-trust security space by dividing them into two architectural designs.

Advantages or what makes SDP or ZTNA stand out

Application access does not require network access

An application centric approach is taken by the SDPs. It allows only the authorized users to connect to a particular application(s), and not at any time the internal network. This scales down the attack surface dramatically. To put it simply, it is an internet based access via a secure multi-tenant brokered cloud approach, neither VPN appliances nor fi ewalls. The ZTNA services can be implemented with minimal business disruptions.

Exposure of services

ZTNA or SDP technologies can be used to reformulate application access. These technologies construct an isolated environment around an application, which makes the application invisible to the internet and to any unauthorized users.

The architectures of services utilizing the proxy or cloud brokers differ in important ways. When utilizing a proxy, a request reaches an identity-aware proxy that front ends the application. The proxy then connects the user to the application. In the case of the cloud broker, the user initiates a request that calls out to the broker hosted in the cloud, while software that front ends the application also calls out the broker. The broker then connects the application and user connection.

Visibility

ZTNA provides enhanced visibility on the activity of users with real time log streaming, applications that were undiscovered previously and health monitoring of the environment.

Trust

SDP or ZTNA technologies treat everything as equally untrusted, either accessing an application remotely or sitting at an organizational office. ccess is purely based on the identity of the user, device posture, and the policies defined or a specific application. This kind o dependent or combinational access is what creates a secure segment of one between a named app and named user on a per session basis.

Conclusion

The traditional hub and spoke network, castle and moat security models have become less effective in the cloud and mobile world which lead to the rise of SDP, ZTNA, and CARTA. Organizations are considering ZTNA as an alternative to traditional network security because of its security advantages.

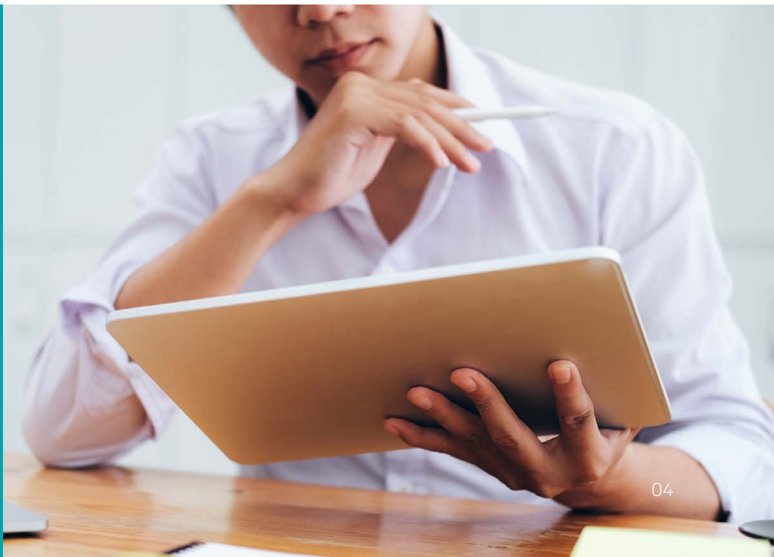
Gartner predicts by 2023, 60% of enterprises will phase out most of their remote access VPN's in favour of ZTNA solutions. It also further predicts that 40% of enterprises will have adopted ZTNA for other uses besides VPN replacement, such as multi-cloud access, third-party access, and activities around mergers and acquisition or divestitures.

Until now organizations have followed the principle "trust, but verify", but in this current cyber environment the principle should be changed to "Never trust, always verify." Even a small change in how users access applications in large global organizations can be an enormous task to put in action. Organizations need to keep adopting new technologies, rebuild their security strategies such as adopting leading edge technologies for better security and efficient p oductivity in this rapidly growing digital world.

Disclaimer

BSI is an accredited Certification Body or Management System Certification an Product certification. o BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 ear period following completion of consultancy.

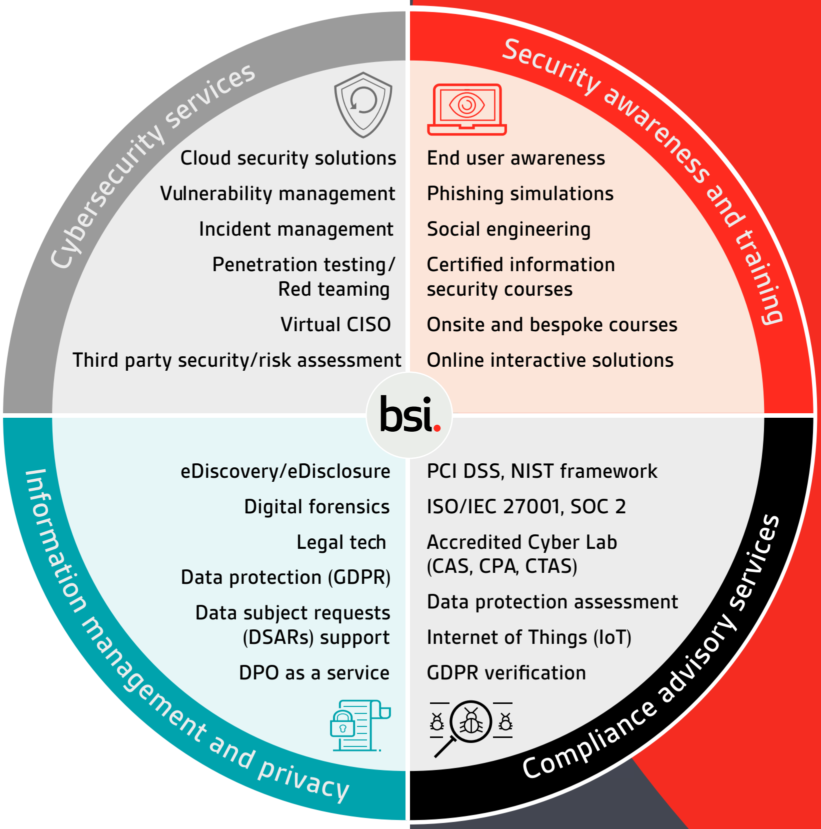
ZTNA provides enhanced visibility on the activity of users with real time log streaming, applications that were undiscovered previously and health monitoring of the environment.



Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Digital Trust Services include:



Cybersecurity services
- Cloud security solutions
- Vulnerability management
- Incident management
- Penetration testing/ Red teaming
- Virtual CISO
- Third party security/risk assessment

Security awareness and training
- End user awareness
- Phishing simulations
- Social engineering
- Certified information security courses
- Onsite and bespoke courses
- Online interactive solutions

Information management and privacy
- eDiscovery/eDisclosure
- Digital forensics
- Legal tech
- Data protection (GDPR)
- Data subject requests (DSARs) support
- DPO as a service

Compliance advisory services
- PCI DSS, NIST framework
- ISO/IEC 27001, SOC 2
- Accredited Cyber Lab (CAS, CPA, CTAS)
- Data protection assessment
- Internet of Things (IoT)
- GDPR verification

Our expertise is accredited by:

Find out more

EMEA	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: digitaltrust.consulting.IE@bsigroup.com	digitaltrust.consulting@bsigroup.com	digitaltrust.consulting.US@bsigroup.com
Visit: bsigroup.com/digital-trust	bsigroup.com/digital-trust	bsigroup.com/digital-trust

Subscribe to our newsletter

Follow us on