Building a cost-efficient zero trust network

Maximise network security and minimise costs

Solution brief

Alcatel·Lucent Enterprise

Cybersecurity and zero trust

Cybersecurity is an increasingly important concern as technology continues to advance, and the number and complexity of cyber threats continue to rise. There are rapidly evolving threats that make it challenging for organisations to predict and defend against them, requiring cybersecurity experts to stay up-to-date with the latest trends and vulnerabilities.

With many different sources and attack vectors, such as phishing emails, social engineering, and software vulnerabilities, defending against cyber threats requires a unique approach for each type of attack.

It can be challenging to identify and protect all potential vulnerabilities in a complex system, making it crucial for cybersecurity experts to understand how different systems and networks work together to develop effective security measures.

Human error is a common cause of cybersecurity breaches, and by 2025, it is estimated that lack of talent or human failure will be responsible for over half of significant cyber incidents.[1]

Meeting complex cybersecurity regulations and standards, such as General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), is another challenge, requiring specialised knowledge and expertise.

[1] Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight, January 2023.

Cybersecurity breach process

The following figure shows the stages that a cyber attacker follows to breach a network and steal valuable data. It starts with reconnaissance, where attackers research, identify and select targets, and scan for network vulnerabilities.

The next stage is weaponisation, where attackers determine how to compromise a target endpoint and deliver a weaponised payload.

After that comes exploitation, where the attacker triggers the weaponised payload and escalates privileges on the compromised endpoint to move laterally across the network.

The next stage is installation, where attackers establish remote shell access and install malware to establish persistence.

In the command-and-control stage, attackers establish encrypted communications channels back to command-and-control servers to remotely direct the attack and execute the objectives.

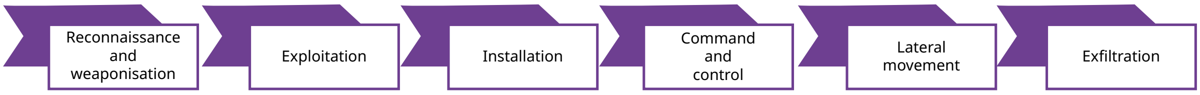
The last stage is lateral movement and exfiltration, where attackers may have multiple objectives, including data theft, destruction or modification of critical systems and denial of service.

The key to stopping attackers is to detect the different stages of the attack lifecycle early and disrupt their progress.

To prevent this, you need to undertake a range of measures such as vulnerability and patch management, malware detection and prevention, blocking risky applications and services, and logging and monitoring all network, endpoint, and of course, cloud activity.

On the network side, you need to implement technologies that provide granular control of applications and monitor traffic between zones or segments in a zero trust model. Zero trust operates on the principle that everything should be considered untrusted by default.

The zero trust concept was developed in response to the increasing number of sophisticated cyberattacks on computer networks. Traditionally, organisations have relied on perimeter-based security solutions, such as firewalls and antivirus software, to protect their networks. However, as cyberattacks have become more advanced and complex, these perimeter-based solutions have proven to be insufficient and instead, every access request must be verified and authenticated before granting access to resources.



Source: XDR for Dummies, Palo Alto Networks Special Edition, 2022

Advancing your zero trust strategy

Alcatel-Lucent Enterprise helps customers become more secure and move toward a zero trust environment with simplicity and cost-efficiency. At ALE, we understand the importance of implementing a zero trust model to ensure our clients' network and data security. We offer a range of solutions designed to help organisations implement a zero trust network and address the challenges posed by cyber threats.

Network hardening

We offer a **hardened network – both inside and out**. It starts with a secure infrastructure and ensuring that the device itself isn't compromised. Our Alcatel-Lucent OmniSwitch® product family runs on the secure Alcatel-Lucent Operating System (AOS), which uses secure diversified code to protect networks from potential vulnerabilities and attacks. The code is continuously updated to address current and future threats, with software diversification through Address Space Layout Randomisation (ASLR) used to protect against buffer overflow attacks. Independent Verification & Validation (IV&V) is also used to analyse and test the AOS source code for potential vulnerabilities, backdoors, malware and system exploits. Third-party cybersecurity experts conduct these tests, which are executed on general availability software images to ensure software integrity.

We apply macro- and micro-segmentation to ensure zero trust network access. Both are critical components of a zero trust security strategy. **Macro-segmentation** refers to the partitioning of the network into separate zones or domains based on function, application or user group. This provides a high level of network segmentation, enabling organisations to isolate critical assets and resources from the rest of the network. **Micro-segmentation**, on the other hand, focuses on segmenting the network at a more granular level, down to the individual user or device. This approach provides more fine-grained control over network access, enabling organisations to enforce security policies at the individual user or device level.

Shortest Path Bridging (SPB) and **Universal Network Profiles** (UNP) provide a powerful solution to help with macro- and micro-segmentation of networks, which improves security and performance by limiting the scope of potential attacks.

SPB is a Layer 2 network protocol that allows for multi-path routing in large networks while simplifying the configuration and management of network infrastructure. Features like virtual network segmentation, provide added protection against unauthorised access and cyberattacks. By using SPB in their network infrastructure, organisations can benefit from improved network efficiency and security, helping to meet their business objectives with confidence.

ALE UNP is profile-based access control, a powerful Alcatel-Lucent Enterprise switch feature that enables network administrators to create and manage user profiles for network access based on identity, location and device. They can implement centralised network policy management, simplifying policy configuration and enforcement. By implementing ALE UNP, organisations can enhance their network visibility, security and control, while also improving network performance, protecting assets and reducing downtime.

Together, SPB and UNP enable network administrators to efficiently manage and secure their network infrastructure to:

- Consistently apply policies across the network
- Segment and isolate IoT devices from other devices
- Minimise the attack surface of the network

Robust authentication

ALE provides robust authentication through a Unified Policy Authentication Manager (UPAM).

A key component of cybersecurity is authentication which is the process of verifying the identity of a user, device or system. It involves confirming that a user or device is who they claim to be, usually by providing some form of identification, such as a username and password.

The ALE solution supports a number of user authentication methods.

- **802.1X**, a network authentication protocol, allows devices to connect to a secure network by providing credentials, such as a username and password. When a device attempts to connect to a network using 802.1X, it is first authenticated before it is allowed access to the network. In an ideal world, the device authenticates through 802.1x. Authentication generates a record that can be shared with a firewall.
- If the device does not support 802.1x, **MAC address** authentication provides an option. A MAC address is a digital ID card for every device on a network. It is unique and identifies each device and allows communications between them, similar to a name tag for your computer or phone.
- ALE supports **device and system fingerprinting**. If no profile is returned with the other 802.1X or MAC authentication, we attempt fingerprinting. Fingerprinting in computer security is the process of collecting information about a device or system, such as its OS, software and open ports to identify and categorise it and assess potential risks and vulnerabilities. It can also be used to map to a profile of a device registered in the IoT inventory database.
- ALE also provides a "catch all" default in case a profile is not returned. The default catch-all rule may allow limited access or completely deny access if the primary authentication fails.

To execute these different types of authentications you need a place to create and manage the credentials of users and devices. UPAM, a component of the ALE Unified Access solution, is required. It provides centralised Authentication, Authorisation and Accounting (AAA) services for the network. It allows network administrators to create and manage user profiles for network access, based on identity and location, among others. UPAM can be configured and managed through the Alcatel-Lucent OmniVista® Network Management System, allowing network administrators to define and enforce network access policies.

Incident responsiveness

Responding to network incidents quickly is a key factor in minimising damage to systems and networks, as well as reducing downtime, caused by security attacks like Distributed Denial of Service (DDoS).

Minimise risks, maximise Quality of Experience (QoE) and enhance security with the Alcatel-Lucent OmniVista Network Advisor. **OmniVista Network Advisor** is an AI-based intelligent and autonomous system that provides real-time network monitoring, issuing of alerts as problems arise, and suggesting solutions for various network and security-related matters, including DDoS attacks. It continuously performs configuration audits and network performance analytics so it can promptly **identify** potential issues, **mitigate** them and **optimise** the network with minimal to no IT intervention.

Partnerships and integrations

An important aspect of authentication is the integration with firewalls. For example, through integration with Fortinet, users or devices authenticated to the LAN and/or WLAN networks can also be simultaneously and seamlessly authenticated to the Fortinet firewall.

With Palo Alto Networks' (PAN) next-generation firewall integration, users or devices authenticated to the LAN and/or WLAN networks can also be simultaneously and seamlessly authenticated to the PAN firewall.

Our partnership with Versa Networks enables secure access to critical resources, regardless of the location of users, data, applications or devices. This is especially beneficial for businesses with regional or branch offices that are remote from the central site or data centre. Unlike traditional wide area networks (WAN) which require multiple network hops and may incur additional costs, SASE and SD-WAN provide a cost-effective and secure solution for the client-to-cloud era. By combining these two solutions, businesses can simplify IT infrastructure management and enable secure access to the Internet and business applications for work-from-anywhere scenarios, including enterprise/DC, regional/branch offices and home/mobile workers.

The ALE-Versa Titan offer is a comprehensive solution that combines Secure Access Service Edge (SASE) and SD-WAN services from the cloud. This includes the Versa Titan SD-WAN, which provides cloud-delivered SD-WAN for lean IT, as well as the Versa Secure Access (VSA), which features next-gen firewall capabilities and geographical blocking, along with Zero Trust Network Access (ZTNA) for work-from-anywhere scenarios. Also, the Versa Secure Web Gateway (SWG) provides secure web browsing and Internet application access (SaaS) for secure remote/home office connectivity. The Versa Titan web portal and app offer integrated networking and security services on a single platform, with all SASE components provided by the same vendor. With a single policy repository that spans network and security policy, businesses can simplify IT management and ensure secure access to critical resources.

The zero trust methodology

To implement a zero trust model, organisations must first address the issues in their existing security infrastructure, such as inconsistent policies, implicit trust and vulnerable IoT devices. The goal is to establish network access and role-based access control, segmentation and monitoring capabilities to combat these issues, with proper segmentation allowing for sensitive resources to be partitioned and limiting access only to those who require it. Monitoring and quarantine capabilities enable customers to identify and isolate potential threats.

A simple yet powerful methodology for building a zero trust network with ALE solutions involves several stages.

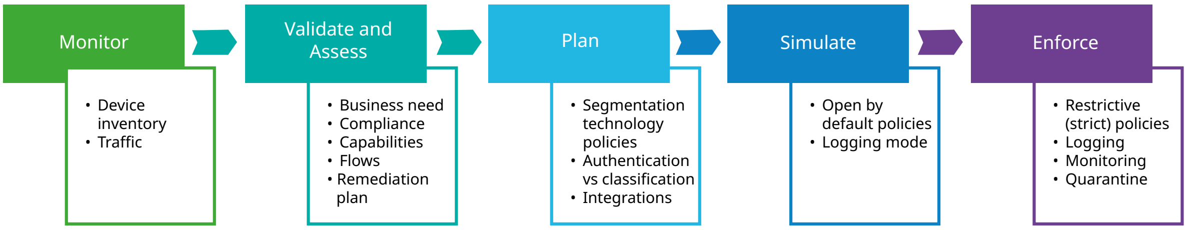
- **Monitor**: Monitoring should be conducted, including device inventory and traffic
- **Validate and Assess**: Validation and assessment involves analysing business needs, compliance requirements, capabilities and flows
- **Plan**: A remediation plan should be created based on the assessment results. Planning includes selecting the right segmentation technology and policies, as well as considering authentication versus classification, and integrations.
- **Simulate**: In the simulate stage, policies are open-by-default and in logging mode, and other features will be tested
- **Enforce**: The enforce stage involves implementing restrictive policies, logging, monitoring and conducting quarantine measures

Total Cost of Ownership

Total Cost of Ownership (TCO) covers all of the expenses associated with owning and operating a product or service throughout its lifespan. These include the purchase price, maintenance, support and upgrades, among others. It's important to select cost-effective solutions that offer long-term value, which can mitigate budget overruns and provide a more accurate return on investment (ROI).

Consider the distinction between the initial capital investment and the ongoing expenses required to keep the system licensed and operational. While some components, such as firewalls, are purely security-focused, other components are also crucial to building a more in-depth security strategy. These include policy management, efficient path network separation technology (advanced and automated macro- and micro-segmentation), automatic virtual network (VLAN) assignment, network encryption protocol, application visibility and independent validation and attestation of the operating system code.

ALE's network cybersecurity strategy addresses the essential elements of network security mentioned above at no cost, while alternatives from other vendors demand specific expertise and numerous costly elements and licenses for operation and upkeep. The ALE approach provides customers with substantial economic benefits while ensuring strong and efficient network cybersecurity.



Conclusion

It is evident that implementing a zero trust network for robust security can present several challenges, such as complexity and cost in terms of creation and maintenance. However, ALE offers a unique and cost-effective approach to address these issues. Advanced macro- and micro-segmentation technologies, in addition to the other components presented in this document, provide a simple and affordable means of implementing a zero trust network that addresses modern cybersecurity requirements. We are committed to helping our customers address their cybersecurity concerns and believe that our approach can help achieve this goal.

ALE solutions include our resilient and secure intelligent Fabric (iFab) and UNP, and robust Network Access Control (NAC) with UPAM, providing profile-based access control. Our innovative OmniVista Network Advisor solution ensures smooth operation and quick recovery and prevention of attacks. In addition, we partner with SASE vendors like Versa Networks and integrate with firewall vendors like Palo Alto Networks to provide customers with more comprehensive and integrated security solutions.

Alcatel·Lucent Enterprise