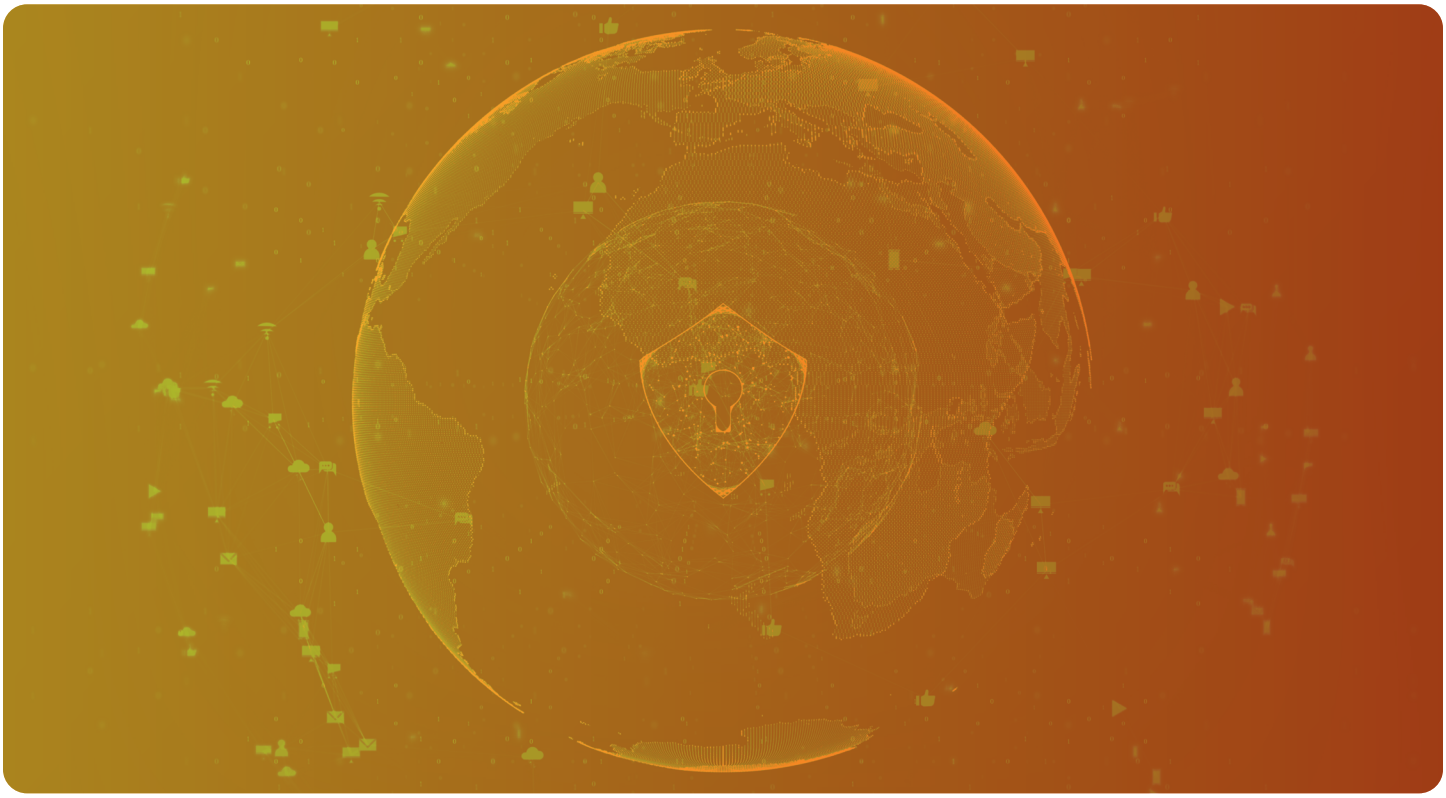
Centrilogic

Whitepaper



CYBERSECURITY: A REQUIRED PILLAR FOR DIGITAL TRANSFORMATION

Learn the different types of vulnerabilities, security threats, and the frameworks for cybersecurity risk management for your organization.

Centrilogic

Whitepaper

TABLE OF CONTENTS

WHY IS NETWORK SECURITY IMPORTANT?

- Cybercrime will cost the world **$6 trillion annually** by 2021, up from $3 trillion in 2015.
- Every organization has tons of sensitive data to protect (i.e. crucial business data, customers' personal information, confidential files, etc.).
- A cybercriminal can find various **vulnerable points** and cause damage to your internal system.
- Implementing and learning about network security will help **protect company data** and find effective ways to control your heavy files.

Centrilogic

Whitepaper

DIFFERENT TYPES OF CYBERSECURITY ATTACKS, THREATS, AND VULNERABILITIES

TYPES OF ATTACKS

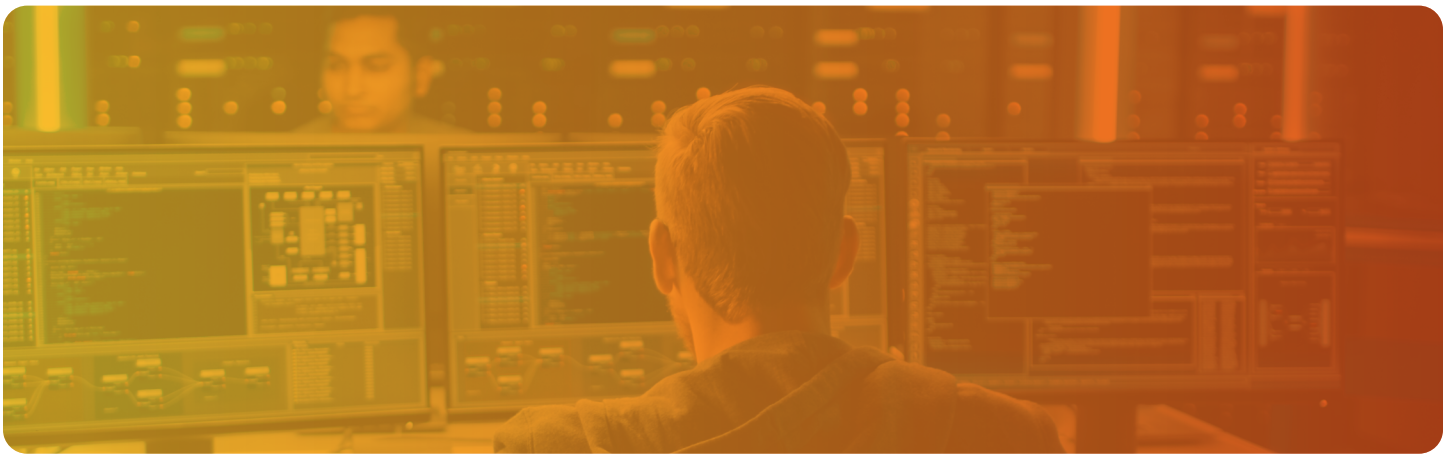
- Malware
- Phishing
- Man in the Middle
- Spear Phishing
- Denial of Service
- SQL Injection
- Zero-Day Exploit
- Advanced Persistent Threats
- Ransomware
- DNS Attacks

TYPES OF THREATS

- Trojan Viruses
- Deep Attacks
- Accessibility Framework Attacks
- Overlay Attacks
- Keyloggers and Screenloggers
- Insider Threats
- Supply Chain Threats

TYPES OF VULNERABILITIES

- Missing Data Encryption
- Old Command Injection
- SQL Injection
- Buffer Overflow
- Missing Authentication for Critical Function
- Missing Authorization
- Unrestricted Upload of Dangerous File Types
- Weak Password
- Cross-Site Scripting and Forgery
- Download of Codes Without Integrity Checks
- Use of Broken Algorithms
- URL Redirection to Untrusted Sites
- Path Traversal
- Bugs
- Reliance on Untrusted Inputs in a Security Decision



Centrilogic

Whitepaper

NETWORK SECURITY GAPS AND BEST PRACTICES

Cybersecurity Risk Management Framework

- CYBERSECURITY AWARENESS
- CYBERSECURITY ASSESSMENT
- CYBERSECURITY CONTINUOUS MONITORING AND TESTING
- CYBERSECURITY INCIDENCE RESPONSE
- CYBERSECURITY GOVERNANCE, AUDITING AND COMPLIANCE

TOP 10 NETWORK SECURITY GAPS

- Network Segmentation
- Firewall Security Review
- Server and Network Patching / Upgrades
- Endpoint Security
- Poor Authentication and Authorization
- Latest Encryption Support Hardware
- Physical Security
- Insufficient Access Control in Network Security
- Syslog Monitoring
- Threat Management and Actions

TOP 5 NETWORK BEST PRACTICES

- Risk Assessment
- Zero Trust Approach
- Network Visibility
- Policy-Based Access Control
- Network Segmentation

Centrilogic

Whitepaper

HOW TO FILL THE GAPS WITH NETWORK SEGMENTATION, NETWORK VISIBILITY, ZERO TRUST, NAC, AND ENDPOINT SECURITY

WHAT IS NETWORK SEGMENTATION AND WHY DO YOU NEED IT?

- Network segmentation improves the overall network security and performance by dividing a computer network into subsystems or segments to control the flow of traffic. A flat network does not have defense in depth.
- Damage can be controlled by the IT team and limited in each segment of the network in case of an incident. This means that a bad actor or malware that penetrates the system will not have access to the entire network.
- Why is this important? According to the Ponemon Institute, it takes an average of 280 days to locate the breach and shut it down.[1] This means that the attacker is in your system with access to your secure data for more than half a year.

1 Ponemon Institute. (n.d.). Retrieved September 30, 2021, from https://www.ponemon.org/

BENEFITS OF NETWORK SEGMENTATION

There are several core benefits that enterprises have experienced with segmentation. Those benefits include:

- Improved Security and Reduced Cyber Threats
- Created Fences Between Resources
- Breaches can be Limited and Isolated
- Minimized Security Overheads

Best Practices for Network Segmentation

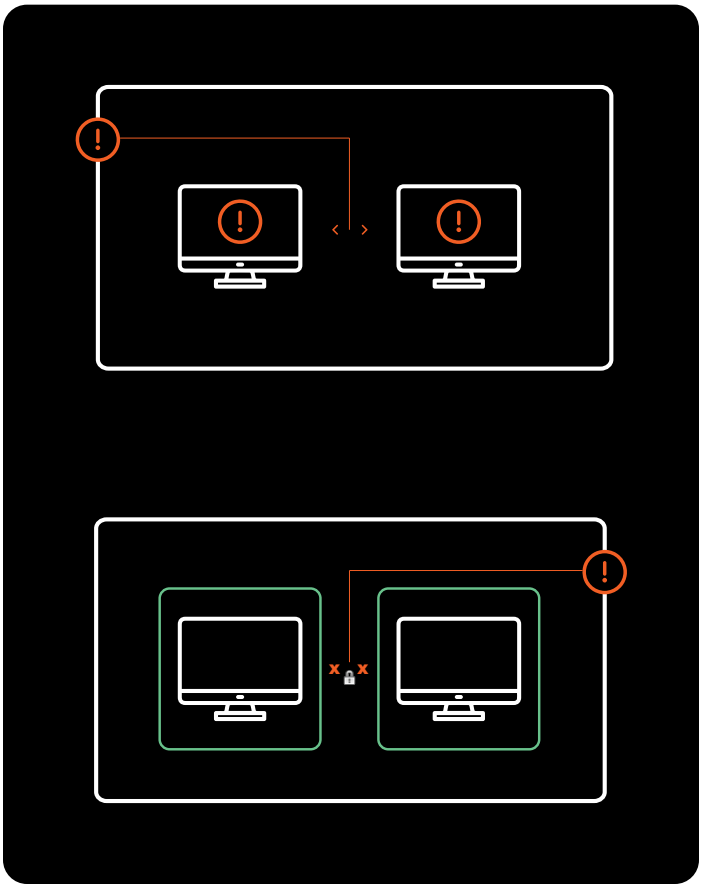
- **KNOW** who is connecting to your network (and what data they need to do their jobs)
- **PROTECT** your endpoints
- **CONDUCT** regular network audits
- **PRIORITIZE** performance AND security
- **DO** under-segment or over-segment
- **ISOLATE** access portals for your third parties

Centrilogic

Whitepaper

NETWORK SEGMENTATION PREVENTS LATERAL NETWORK ATTACKS

A segmented network stops attackers from moving between specific networks or systems.



WITHOUT NETWORK SEGMENTATION:

- Attacker breaches security perimeter
- Attacker moves freely between networks and systems
- Attacker gains access to sensitive data

WITH NETWORK SEGMENTATION:

- Attacker breaches security perimeter
- Attacker gets stuck inside the main perimeter and must breach each segment's security perimeter to gain access
- Attacker cannot move laterally

WHAT IS NETWORK VISIBILITY AND WHY DO YOU NEED IT?

Network visibility refers to having an awareness of all the different components at work within your network to be able to analyze the following aspects:

- Performance
- Traffic
- Big Data Analytics
- Managed Resources
- Applications
- Cloud Issues
- Mobile and IoT Issues
- Wireless Networks

This list is by no means exhaustive, as different monitoring solutions offer varied capabilities. A comprehensive solution can also provide you with more control, allowing you to make changes based on the metrics that are being monitored.

MSPs can also help improve security for customers with a solution for visibility, thus revealing signs of network compromise. Better visibility also results in improved analytics, which enables MSPs to make informed decisions on data protection strategies that can be applied moving forward.

ENTERPRISE NETWORK VISIBILITY CHALLENGES

- The complexity of the network minimizes the ability to monitor and measure the performance from one end to another.
- Hybrid and multi-cloud network architectures are causing serious gaps in end-to-end visibility.
- IOT/BYOD also cause networks to extend network visibility due to the lack of organizational controls and endpoint sensors compatibility issues with these devices.

WHY IS NETWORK VISIBILITY IMPORTANT?

- **THREAT MANAGEMENT**
- **BANDWIDTH TRACKING**
- **IDENTIFYING UNAUTHORIZED USE**
- **MINIMIZE OPERATIONAL TROUBLESHOOTING**
- **DOWNTIME REDUCTION**

THREAT MANAGEMENT: A threat usually maneuvers through a network to get past protections and establishes itself. A piece of code is typically planted on a workstation or web server. From there, additional code is loaded and it begins moving laterally to get at the secure data. Visibility helps in recording and tracking the malware lifecycle; giving IDS, SIEM, and SOAR systems access to all the information they need to spot security issues.

BANDWIDTH TRACKING: Inadequate data movement equates to a slow network. If a data path has become a bottleneck, reconfiguring the network or upgrading a connection could get things back up to speed.

IDENTIFYING UNAUTHORIZED USE: All unauthorized uses have the ability to reduce performance and compromise security, but not all are considered malicious. "Shadow IT" is a problem in many organizations, where employees install software or use devices without going through their IT department. Visibility is key to identifying risk and the necessary actions to fix the problem.

TROUBLESHOOTING: The cause isn't always obvious when something goes wrong. Visibility aids in finding processes that are unresponsive and connections that have become unreliable.

DOWNTIME REDUCTION: Detailed information on network problems allows for quicker fixes. It also lets administrators confirm that the problem is truly gone. In instances when the problem still persists, trying to find the issue should remain a priority. By doing so, there will be fewer cases of having to re-investigate these issues going forward.

WHAT IS ZERO TRUST AND WHY DO YOU NEED IT?

Zero Trust architecture - where no person/devices/application in the enterprise network should be trusted by default, no matter if it's an internal or external network. The fundamental basis of the trust should be based on the refactored access control using the right authentication and authorization. Zero Trust architecture has changed the traditional access control mechanism and its essence is adaptive trusted access control based on identity.[1]

It's A Marathon, Not A Sprint

Zero Trust implementation is a gradual process. Defining a big-bang sprint project to move to Zero Trust is unlikely to be successful.

Work with existing security capabilities and migrate gradually to the Zero Trust model. Implement significant, strategic change over a two-year timeframe.[2]

This framework is defined by various industry guidelines such as Forrester eXtended, Gartner's CARTA, and more recently NIST 800-207, as an optimal way to address current security challenges for a cloud-first, work from anywhere world.

---

1 *Zero Trust Architecture and Solutions* (Rep.). (2020). Retrieved September 30, 2021, from Gartner website: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf

2 *A Practical Guide To A Zero Trust Implementation* (Rep.). (2021, March 3). Retrieved September 30, 2021, from Forrester website: https://reprints2.forrester.com/#/assets/2/716/RES157736/report

CORE ZERO TRUST LOGICAL COMPONENTS

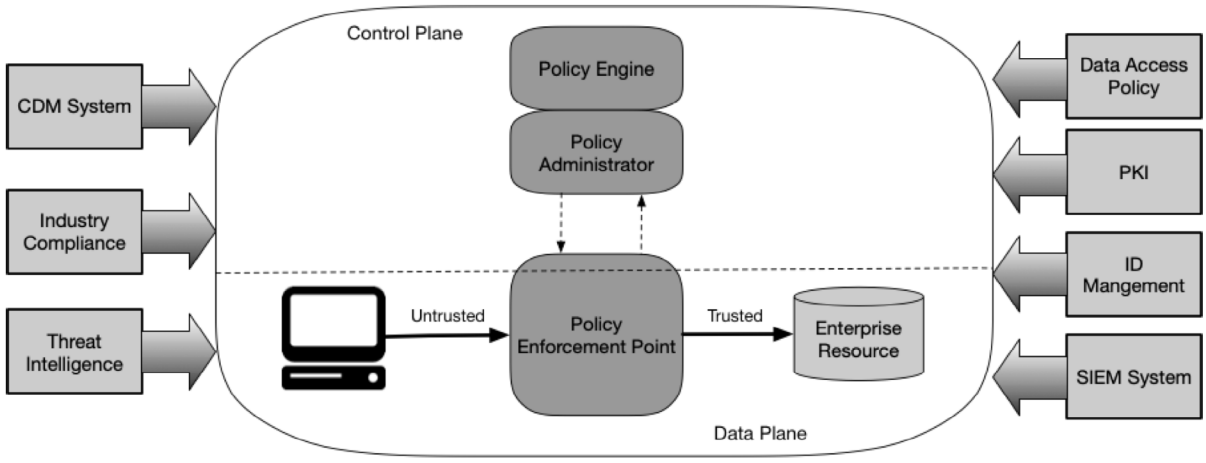


Figure 1: Core Zero Trust Logical Components[1]

The Component Descriptions

- Policy Engine (PE): this component is responsible for the ultimate decision to authorize access to a resource for a given client or subject. The Policy Engine uses enterprise policy as well as input from external sources (e.g., IP blacklists, threat intelligence services) as input to a "trust algorithm" to determine whether or not to grant access to the resource. The Policy Engine is paired with the Policy Administrator component. These components work in tandem; the Policy Engine makes and logs the decision and the Policy Administrator executes this as approved or denied.

- Policy Administrator (PA): this component is responsible for establishing the connection between a resource and a client. It would create the authentication token or credential used by a client to access an enterprise resource. It is closely tied to the Policy Engine and relies on its decision to ultimately grant or deny the connection. Implementations may treat the Policy Engine and Policy Administrator as an individual service; here, it's split into its two logical components. The PA communicates with the Policy Enforcement Point (PEP) when creating the connection. This communication is done through the control plane.

- Policy Enforcement Point (PEP): this system is responsible for sanctioning, monitoring, and eventually terminating connections between a subject and an enterprise resource. This is a single logical component in ZTA, but it may be divided into two distinct components: the client (e.g., an agent on a user's laptop) and resource side or a single portal component acting as a sentry for communication pathways.[1]

1 *Zero Trust Architecture* (Rep.). (2020, February). Retrieved September 30, 2021, from National Institute of Standards and Technology website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf

THE CORE PRINCIPLES OF THE ZERO TRUST MODEL, EXPLAINED

ESTABLISH YOUR CURRENT BASELINE: In a Zero Trust model, there is no such thing as a trusted source. Assess your current Zero Trust maturity and establish a baseline of proficiencies.

DETERMINE CURRENT BUSINESS INITIATIVES AND EXISTING SECURITY CAPABILITIES: Before starting a Zero Trust initiative, review the other business dynamics that are at play. Security leaders need to leverage migrations and IT changes, which result in delivering Zero Trust effectively within their organizations.

SET YOUR DESIRED MATURITY STATE AND OUTLINE TIME FRAMES TO ACCOMPLISH IT: Once you have conducted a maturity assessment, the next step is to set the desired time frame and future state maturity. Forrester Research, Inc. recommends a two to three year horizon as a typical time frame to plan a detailed Zero Trust roadmap. This period of time gives companies a purposeful advance in maturity without the expectation of achieving perfection.[1]

1 *A Practical Guide To A Zero Trust Implementation* (Rep.). (2021, March 3). Retrieved September 30, 2021, from Forrester website: https://reprints2.forrester.com/#/assets/2/716/RES157736/report

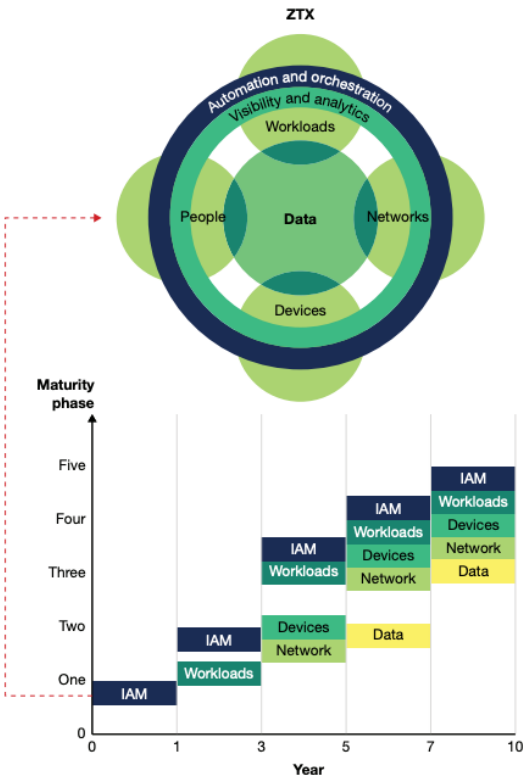


Figure 2: Zero Trust Maturity Phases[1]

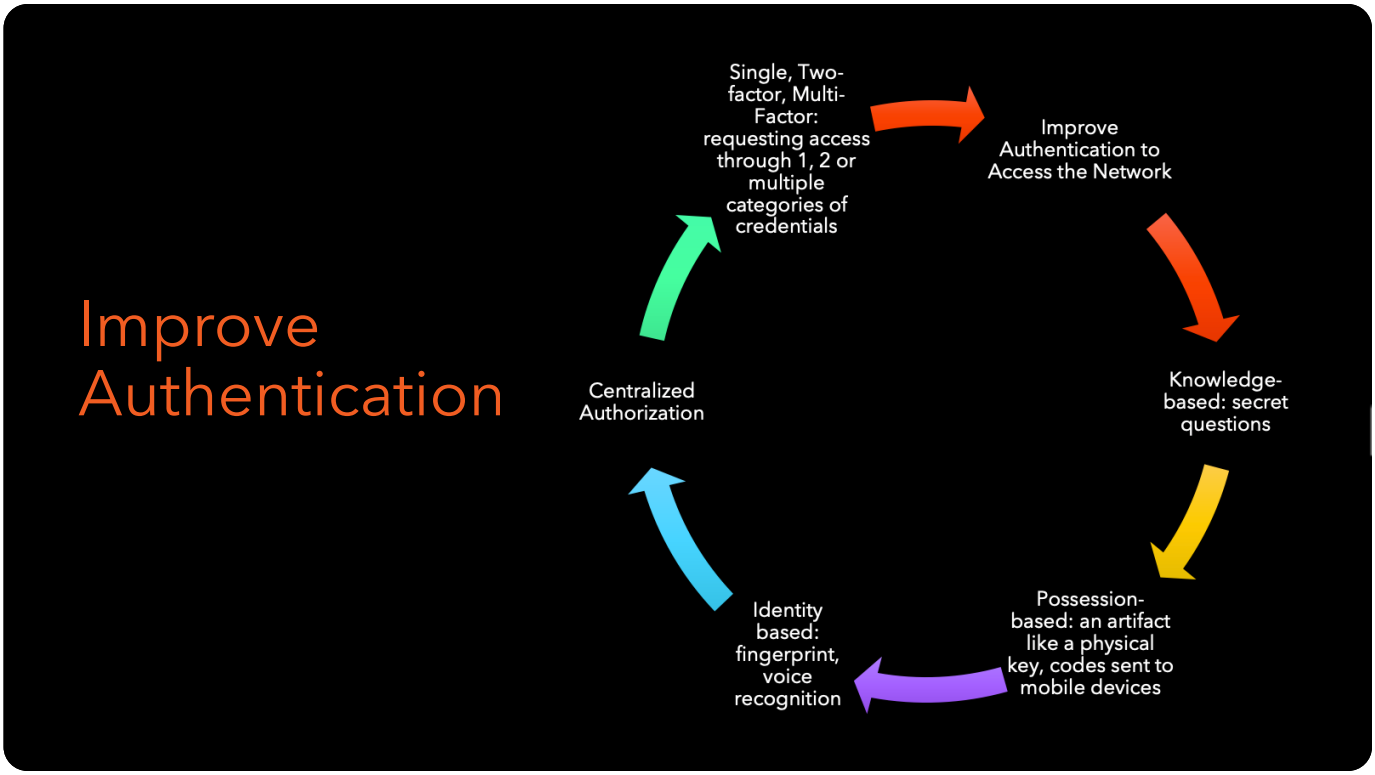
ADDITIONAL SYSTEMS IN AN ENTERPRISE ZTA IMPLEMENTATION

DATA ACCESS POLICIES: This is the set of attributes, rules, and policies about data access created by the enterprise around the enterprise resources. This set of rules could be encoded in the Policy Engine or dynamically generated by the PE. These policies are the starting point for granting access to a resource as they provide the basic access privileges for actors and applications in the enterprise. These roles and access rules should be based on user roles and the mission-based needs of the organization.

ENTERPRISE PUBLIC KEY INFRASTRUCTURE (PKI): This system is responsible for generating and logging certificates issued by the enterprise to resources, actors, and applications. This also includes the global CA ecosystem and the Federal PKI3, which may or may not be integrated with the enterprise PKI.

ID MANAGEMENT SYSTEM: This system is responsible for creating, storing, and managing enterprise user accounts and identity records. It contains the necessary user information (e.g., name, email address, certificates, etc.) and other enterprise characteristics such as role, access attributes, or assigned systems. This system often utilizes other systems (such as a PKI above) for artifacts associated with user accounts.

SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) SYSTEM: This is an enterprise system that aggregates system logs, network traffic, resource entitlements, and other events that provide feedback on the security posture of enterprise information systems. The data is then used to refine policies and warn of possible active attacks against enterprise systems.



WHAT IS NETWORK ACCESS CONTROL (NAC)?

WHAT IS 802.1X NETWORK ACCESS CONTROL (NAC)?

802.1X network access control (NAC) enables administrators to provide uniform access control across wired and wireless networks. It is comprised of two major elements:

- 802.1X protocol—An IEEE standard for port-based network access control (PNAC) on wired and wireless access points. 802.1X defines authentication controls for any device or user trying to access a LAN or WLAN.
- NAC—A proven networking concept that determines devices and users by regulating access to the network. NAC controls access to enterprise resources using authorization and policy enforcement.

PROBLEMS 802.1X NETWORK ACCESS CONTROL ADDRESS

The effect of wireless network access, bring your own device (BYOD), mobility, social media, and cloud computing on enterprise network resources is massive. Using 802.1x helps companies improve their ingress security in this type of environment, while lowering the total cost of ownership.[1]

1 *What is 802.1X Network Access Control (NAC)?* (Rep.). (n.d.). Retrieved September 30, 2021, from Juniper Networks website: https://www.juniper.net/us/en/research-topics/what-is-802-1x-network-access-control.html

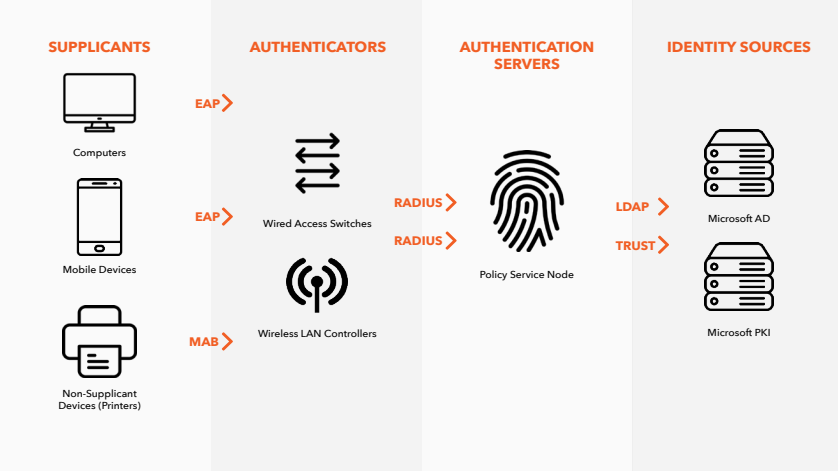
NETWORK ACCESS CONTROL (CONT.)

WHAT CAN YOU DO WITH 802.1X NETWORK ACCESS CONTROL?

There are various ways to deploy a NAC and the essentials are:

- Pre-admission control
- Device and user detection
- Authentication and authorization
- Onboarding
- Profiling
- Policy enforcement
- Post-admission control

802.1X provides L2 access control by validating the user or device that is attempting to access a physical port.



HOW DOES 802.1X NETWORK ACCESS CONTROL WORK?

The 802.1X NAC operation sequence is as follows:

1. Initiation
2. Authentication
3. Authorization
4. Accounting
5. Termination[1]

1 *What is 802.1X Network Access Control (NAC)?* (Rep.). (n.d.). Retrieved September 30, 2021, from Juniper Networks website: https://www.juniper.net/us/en/research-topics/what-is-802-1x-network-access-control.html

Centrilogic

Whitepaper

ENDPOINT SECURITY

WHAT'S CONSIDERED AN ENDPOINT?
Endpoints can range through commonly thought of devices such as:

- Laptops
- Tablets
- Mobile devices
- Smartwatches
- Printers
- Servers
- ATM machines
- Medical devices

Endpoint Security Components

Machine-learning classification to detect zero-day threats in near real time
Advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoints
Proactive web security to ensure safe browsing on the web
Data classification and data loss prevention to prevent data loss and exfiltration
Integrated firewall to block hostile network attacks
Email gateway to block phishing and social engineering attempts targeting your employees
Actionable threat forensics to allow administrators to quickly isolate infections
Insider threat protection to safeguard against unintentional and malicious actions
Centralized endpoint management platform to improve visibility and simplify operations
Endpoint, email, and disk encryption to prevent data exfiltration[1]

1 *What Is Endpoint Security?* (Rep.). (n.d.). Retrieved September 30, 2021, from McAfee website: https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint.html

PREVENTING CYBERSECURITY THREAT RISKS

- First Thing's First – Awareness
- Security Control Standards – Definitions and Applications
- Developing a Security Mindset and Mindshare - Staff Training
- Cybersecurity Industry Participation and Contributions – Intel Sharing

CYBERSECURITY FRAMEWORK

- NIST Cybersecurity Framework
- ISO 27001 and ISO 27002
- SOC2
- NERC-CIP
- HIPAA
- GDPR
- FISMA

Centrilogic

Whitepaper

CRITICAL QUESTIONS FOR DIGITAL ORGANIZATIONS

WHAT CRITICAL QUESTIONS MODERN ORGANIZATIONS NEED TO BE ASKING ON A REGULAR BASIS:

- Do we understand our organization's security posture and associated risks?
- Do our employees have a security mindset?
- Do we have a process in place to respond to a security incident? If not, how vulnerable are we right now?
- Do we have a Cybersecurity Maturity Model?
- How do we measure up to a Cybersecurity Maturity Model?

To learn more about how Centrilogic can work with you to achieve your IT transformation goals, contact us at centrilogic.com/contact-us or via any of the communication channels below.