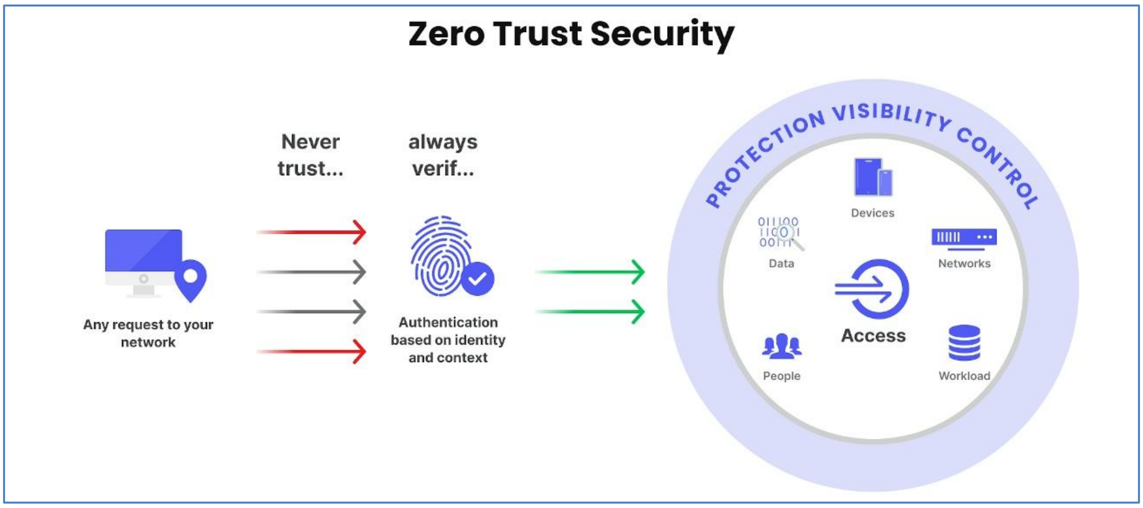
# Zero Trust Network (ZTN)

## 1. Definition

Zero Trust Network is a cybersecurity framework **that assumes no user, device, or system is trusted** by default — even inside the network perimeter. Every request must be **verified continuously** before granting access. It's based on the principle of "**Never trust, always verify**."


Zero Trust Security
Never trust...
always verif...
Any request to your network
Authentication based on identity and context
PROTECTION VISIBILITY CONTROL
Devices
Data
Networks
Access
People
Workload

## 2. How Does It Work? (Complete Working Process):

1. **Identity Verification**
   - User or device requests access.
   - The system checks credentials, device posture (antivirus, OS patches), location, etc.
2. **Policy Engine (PE) Decision**
   - A policy engine evaluates the access request against predefined rules.
   - E.g., "John can only access Salesforce between 9am-6pm from corporate devices."
3. **Continuous Monitoring**
   - Even after access is granted, user behaviour is monitored in real-time.
   - If behaviour is unusual (e.g., downloading too much data), access is revoked.
4. **Logging and Alerting**
   - Every access attempt (approved or denied) is logged.
   - Violations trigger alerts sent to SIEM or SOAR platforms.

## 3. What Log Formats Does It Generate?

Depends on the vendor, but typically:

- **Syslog (UDP/TCP/Encrypted TLS) – most common**
- **API Integration** – for cloud-native Zero Trust tools
- **CEF (Common Event Format)** — used by tools like Zscaler
- **LEEF (Log Event Extended Format)** — for QRadar
- **JSON/REST API logs** — used in cloud-native tools
- **Cloud-native connectors** – like Azure Monitor, AWS CloudTrail

**Log fields might include:** Username, device ID, location, requested resource, risk score, action (allow/deny), reason, timestamp

### 4. Successor Of Which Tools/Methods?

ZTN evolved from traditional "Perimeter-based security", where:

- Firewalls assumed everything inside the network was safe.
- VPNs gave full network access once inside.
- Network segmentation was static.

ZTN replaces this with dynamic, identity-based, granular access control.

### 5. Advantages:

- Strong protection against **insider threats**
- Prevents **lateral movement** (critical in ransomware cases)
- Access is **context-aware** (device, location, time)
- Scales well with **remote workforce/cloud environments**
- Helps meet **compliance** (HIPAA, PCI-DSS, etc.)

### 6. Disadvantages:

- Complex to implement; needs **integration across multiple tools**
- Initial user friction (e.g., more authentication steps)

### 7. Top Zero Trust Use Cases for SOC Analysts:

1. **Unauthorized Access Attempt from Unknown Device**
    - Detect access attempts from devices not registered or failing compliance checks (e.g., unpatched OS, no antivirus).
    - Blocked by Zero Trust and logged in SIEM.

2. **Access Outside Business Hours**
    - Users accessing sensitive resources at odd hours (e.g., 3 AM) trigger Zero Trust policies.
    - Especially useful for detecting compromised credentials.

3. **Privilege Escalation Attempt**
    - Zero Trust systems can detect sudden elevation of privileges (e.g., from HR to Admin group).
    - Alerts SOC if policy violation or potential insider threat.

4. **Lateral Movement Detection Blocked by Micro-Segmentation**
    - Malware or a compromised user tries moving from HR subnet to finance — ZTN blocks & logs this.
    - SIEM correlates with endpoint and network logs.

5. **Access to High-Risk Resources Without Justification**
    - User tries to download or access a financial report, payroll data, or sensitive database with no prior history or ticket.

### 8. Top Vendors

1. **Zscaler**
2. **Okta**
3. **Cisco Duo**

4. **Palo Alto Networks (Prisma Access)**
5. **Illumio**
6. **Microsoft (Entra ID, Defender suite)**
7. **Cloudflare Zero Trust**
8. **Akamai Guardicore**
9. **Tailscale / ZeroTier** (for small orgs)

## 9. Zero Trust-related Q&A for SOC Analysts:

### 1. Q: How do you differentiate Zero Trust logs from traditional firewall logs in a SIEM?

**A:** Traditional firewalls just log source IP, destination IP, port, and action (allow/deny). But Zero Trust logs include identity context, device posture, location, risk score, and policy decision.
For example, instead of just saying "blocked port 443," Zero Trust logs might say:

> *"User 'jane@org.com' on non-compliant device from Brazil denied access to 'Payroll App' due to device posture failure."*

### 2. Q: How would you investigate an alert triggered by Zero Trust denying access to a user within the company?

A: I'd start by checking the Zero Trust logs in SIEM for the denied event. Then I'd correlate it with:

- User identity logs (Okta/AD)
- Device logs (EDR/MDM)
- Time and location
- Change tickets or HR info (Was the user transferred/terminated?)

It could be a legit user trying to access something outside their scope — or a compromised account trying lateral access.

### 3. Q: How do Zero Trust principles help reduce lateral movement?

A: Zero Trust uses micro-segmentation and least privilege. This means each user/device can access only what they explicitly need — like putting every door in a building behind its own keycard.
If malware compromises one endpoint, it cannot spread unless its lateral traffic also passes policy checks (device health, user auth, time, behaviour). This contains the blast radius.

### 4. Q: Can Zero Trust logs generate false positives? How do you tune them?

A: Yes, especially during initial deployment when access policies are strict. A new legitimate device or user role change can trigger denies.
Tuning involves:

- Creating baselines of normal behaviour
- Building exception rules for known use cases
- Reviewing denied attempts that were later approved manually