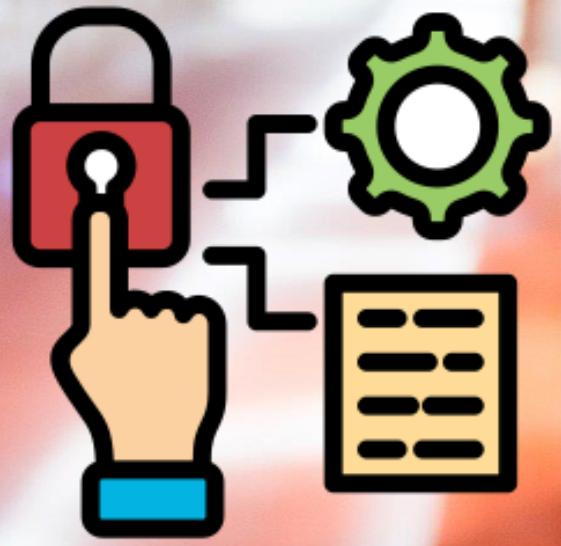
Defense In Dept - Applying Security Controls Across The Network

Sovathnak Kang

Head of Information Security & Risk Management



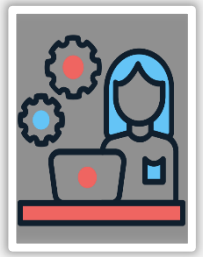
Agenda

1. Understanding the layered security strategy
2. Types of Security Controls
3. Integration of the controls and example of each controls
4. Q & A?

1. Understanding the Layered Security Strategy

Why it Matter:

- Threat Actor must bypass several layers, not just one
- Reduces exposure to vulnerabilities



Distributed Security Domains:

Security measures span technical, managerial, and physical domains for comprehensive protection.

Cross-Team Collaboration:

Encourages teamwork among network engineers, risk managers, and physical security personnel.

Compliance and Best Practices:

Aligns with ISO 27001, NIST CSF, CIS standards emphasizing risk management and layered controls.

2. Type of Security Controls

Physical Controls

- ❑ Protect the physical environment **where systems operate** such as the buildings, rooms, and equipment.
- ❑ Purpose : prevent unauthorized physical access, damage, or interference

Technical Controls

- ❑ **Technology-based** mechanisms that protect systems, networks, and data.
- ❑ Purpose : enforce confidentiality, integrity, and availability through IT systems.

Administrative Controls

- ❑ Define **policies, principle, and processes** that guide how security is managed.
- ❑ Purpose : ensure proper governance, human behavior, and organizational processes.

Legislative Controls

- ❑ Some organizations **treat laws and regulations** as another type of control because they force organizations to comply.

2. 1 Physical Controls (Example Only)

Access Restriction Measures

Locked server rooms and biometric systems prevent unauthorized access to critical hardware and areas.

Monitoring and Surveillance

Surveillance cameras monitor activity to deter malicious behavior and enhance security.

Human Security Presence

Security guards provide active protection and incident response within physical premises

Human Security Presence

Fire suppression and cooling systems maintain safe environmental conditions protecting hardware integrity.

2. 2 Technical Controls (Example Only)

Firewalls and Intrusion Detection / Protection

Firewalls inspect incoming and outgoing network traffic based on security rules to prevent unauthorized access.

Access Control

Control and track access to systems, networks, and data. It ensures only the right users do the right things — and all actions are recorded.

Data Encryption

Encryption protocols like TLS and VPNs secure data transmission to maintain confidentiality and security.

Network Detection and Respond (NDR)

SPAN (or port mirroring) is the mechanism that feeds network traffic to the NDR sensor.

2. 3 Administrative Controls (Example Only)

Policy – The "What & Why"

A high-level management statement that define what must be done and why it is important.

Procedure – The "How to Do It"

A step-by-step instruction explaining how to implement the policy.

Baseline – The Minimum Standard

A minimum security requirement that systems must meet.

Awareness Training

Educate employees on acceptable behavior and reduce human-related security risks..

3. Integration of the Controls

Access Restriction Measures

Locked server rooms and biometric systems prevent unauthorized access to critical hardware and areas.

Monitoring and Surveillance

Surveillance cameras monitor activity to deter malicious behavior and enhance security.

Human Security Presence

Security guards provide active protection and incident response within physical premises

Human Security Presence

Fire suppression and cooling systems maintain safe environmental conditions protecting hardware integrity.

Data Center Management Policy

- Server rooms must remain locked at all times.
- Biometric access is required for entry to designated critical area.
- All access attempts must be logged and monitored.
- Access must be approved by IT Security and Management.
- Vendors or visitors must be escorted by authorized staff at all times.
- All server rooms must be equipped with CCTV surveillance, and recorded.
- All server rooms must protected with fire management system and tested.

3. Integration of the Controls

Firewalls and Intrusion Detection / Protection

Firewalls inspect incoming and outgoing network traffic based on security rules to prevent unauthorized access.

Access Control

Control and track access to systems, networks, and data. It ensures only the right users do the right things — and all actions are recorded.

Data Encryption

Encryption protocols like TLS and VPNs secure data transmission to maintain confidentiality and security.

Network Detection and Respond (NDR)

SPAN (or port mirroring) is the mechanism that feeds network traffic to the NDR sensor.

Network Security Management Policy

- Firewalls must be deployed at all network boundaries.
- Firewall and IDS/IPS rules must be reviewed at least every 6 months.
- Access to network systems must use role-based access control (RBAC)
- All access to network devices must be logged and retained for audit purposes.
- Unencrypted protocols (e.g., HTTP, Telnet, FTP) are prohibited unless explicitly approved.
- SPAN/Port Mirroring or network taps must be configured to forward copies of network traffic to the NDR sensor.


Q &
A