Zero Trust

Presented by:
Paul Facey
Networks Plus
Managed Services Team

NETWORKS PLUS

Zero Trust and Defense in Depth

Questions:

1. What is Defense in Depth

2. What is Zero Trust and how does it integrate into Defense in Depth

NETWORKS PLUS

Defense in Depth: Protecting Your IT Like a Stadium

Think of IT security like protecting a packed sports stadium. Every layer matters—from gates to staff checks. We'll use the stadium analogy to reveal how layered security creates true protection.

NETWORKS PLUS

The Outer Perimeter: Hardware Firewall

Stadium Walls & Gates

Imagine high fences, locked gates, and initial checkpoints. Only authorized visitors may pass through.

Hardware Firewall in IT

Acts as your digital wall—blocking unwanted network traffic. Examines all packets at the door and follows strict rules (e.g., WatchGuard Firewall).

NETWORKS PLUS

Controlling the Crowd: Network Segmentation

Audience Zones

Fans, staff, and VIPs sit in distinct zones. Access is restricted per role.

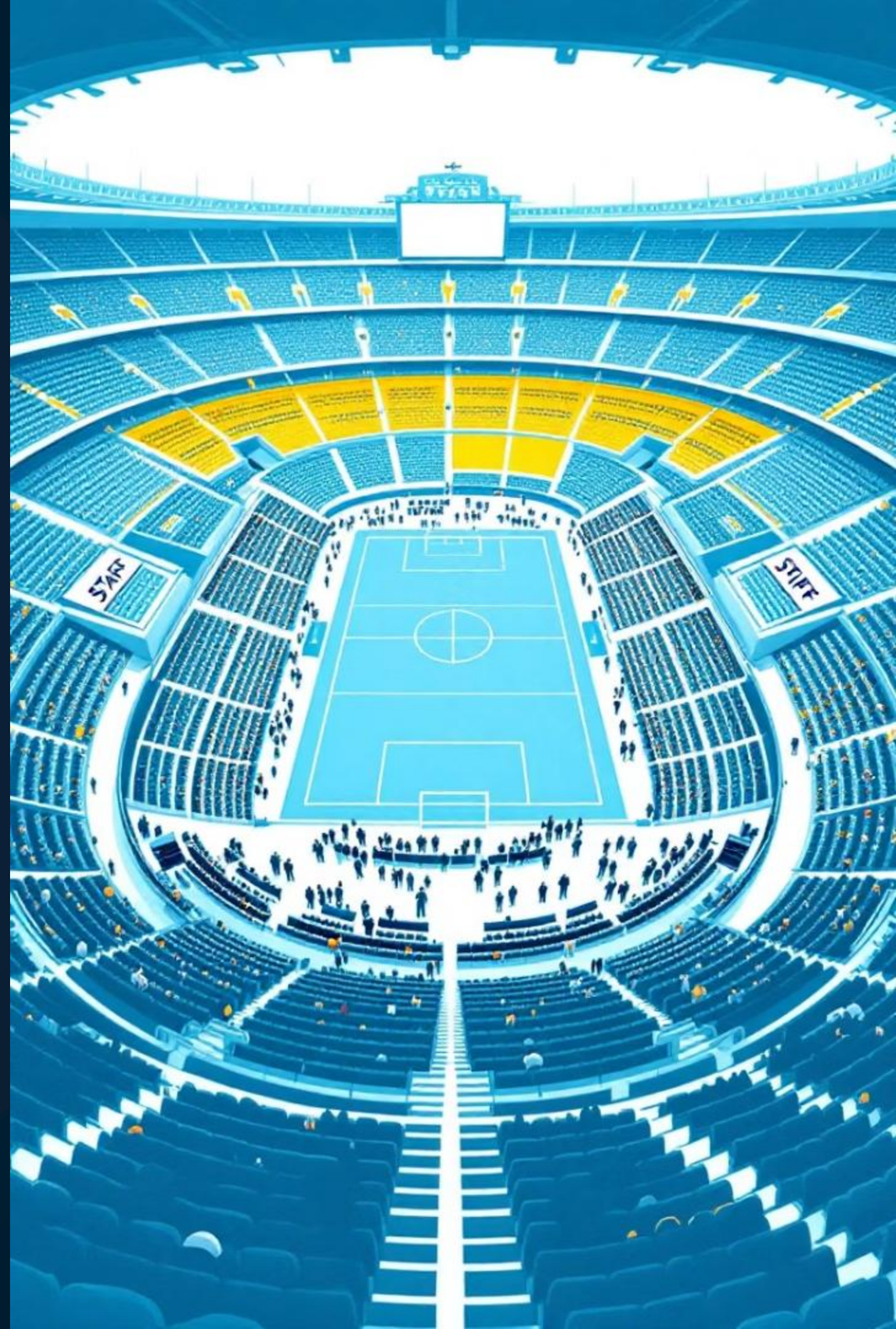
Network Segmentation

IT uses VLANs and ACLs to split the network. Guest Wi-Fi and essential servers stay separate.

Minimizes Risk

Limits the spread of threats and protects key infrastructure.

NETWORKS PLUS



Individual Scrutiny: Endpoint Firewall

Personal Ticket Checks

Every attendee’s ticket is inspected at their section—no assumptions, no shortcuts.

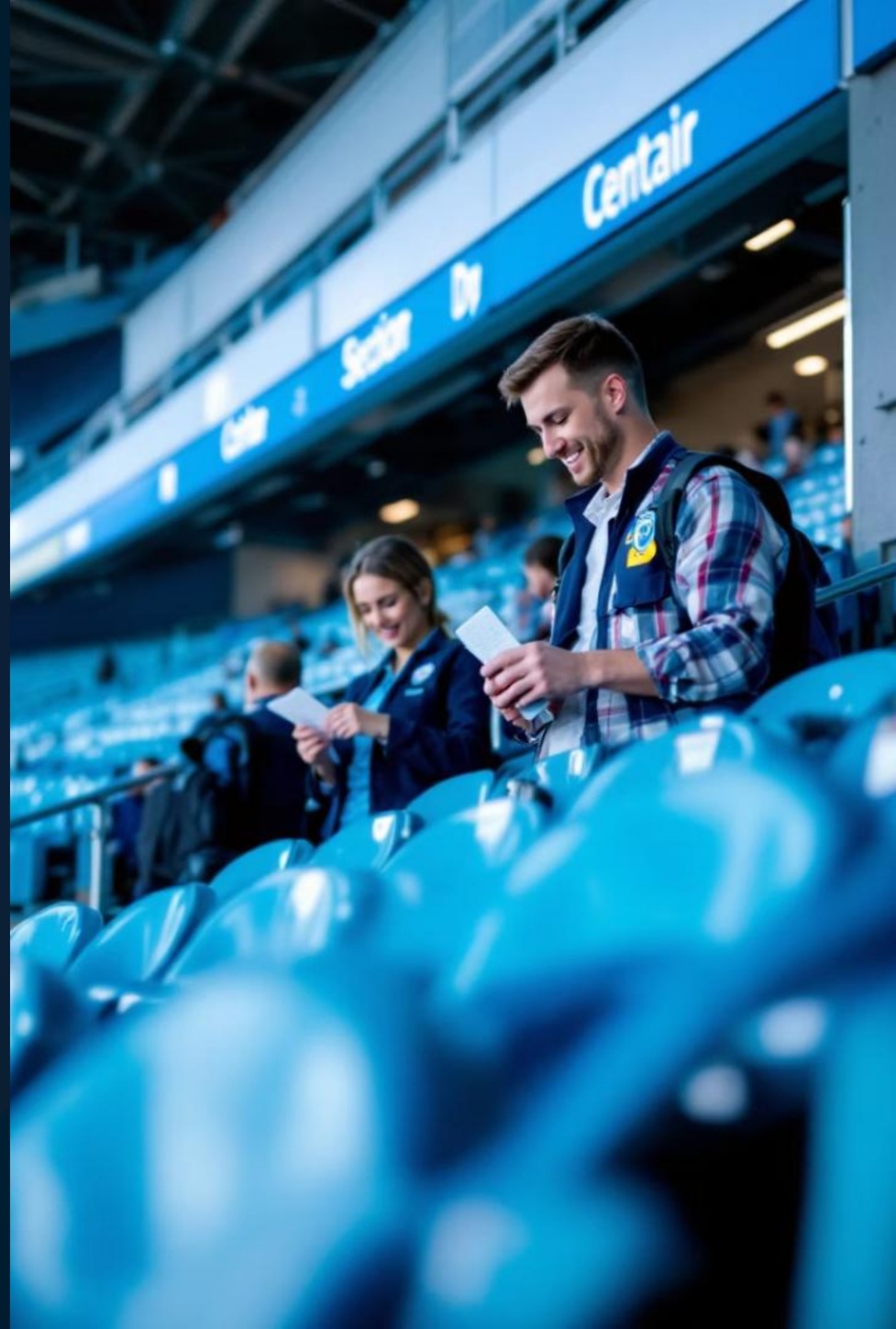
Host Firewalls

Each device sets its own inbound/outbound rules. Only legitimate connections are allowed to pass.

Security by Level

Even if someone bypasses the main gate, section staff add vital scrutiny.

NETWORKS PLUS



Access Control: File Permissions

Locker Rooms

Only players and coaches can enter. Everyone else is locked out.

Role-Based Permissions

In IT, file access mirrors physical restrictions—users get only the rights their role requires.

Least Privilege

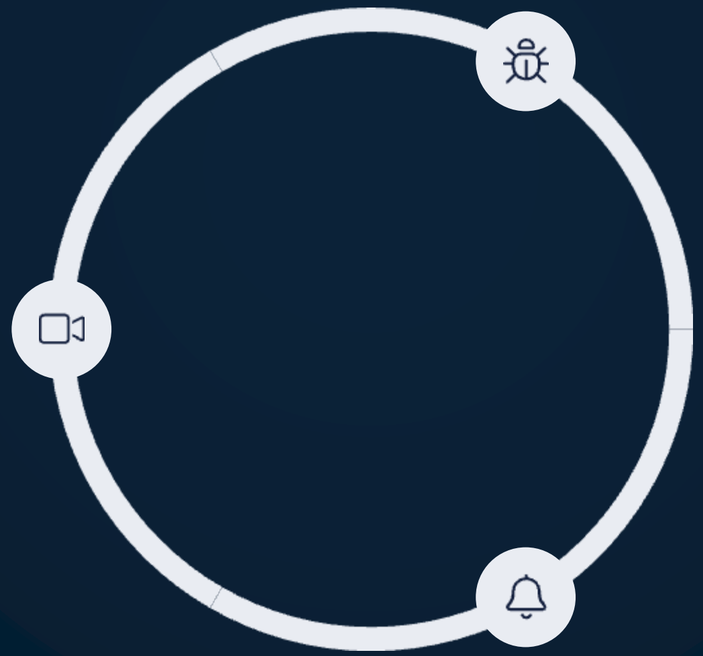
Minimize both physical and data exposure by granting access only when necessary.

NETWORKS PLUS

Detecting Intruders: Endpoint Detection & Response

Active Surveillance

Cameras and guards monitor constantly for threats or suspicious behavior.



EDR Tools

IT uses EDR to watch endpoints for infections, strange actions, and stop attacks fast.

Rapid Response

Alerts enable a quick reaction—whether in the physical stadium or digital network.

NETWORKS PLUS

Trust No One: Zero Trust Approach

1

Verify Everything

Each person and device is repeatedly checked, no matter how familiar.

2

Continuous Checks

No permanent passes—identity and security posture are always under review.

3

Access by Need

Users, like stadium attendees, move only where explicitly approved.

NETWORKS PLUS

Summary: Layered Security for Robust Protection

1

Multiple Layers

No single security measure is enough. Each layer blocks new threats.

2

Stadium Model

Walls, checks, staff, and monitoring work together for full coverage.

3

Defense in Depth

Adopt a comprehensive strategy—integrate people, process, and technology for true protection.

NETWORKS PLUS

Embracing Zero Trust Security

Zero Trust shifts the security mindset:

Trust nothing, always verify

As organizations move to cloud, mobile, and remote-first models, old perimeter defenses no longer suffice. Today, Zero Trust is rapidly becoming the security standard, with the market projected to reach $68.6 billion by 2032.

Core Principles of Zero Trust

Never Trust, Always Verify

Every access request must be authenticated and validated without exceptions.

- Assume attacker may be inside

Least Privilege Access

Users and devices receive only the only the permissions they need. need.

- Limits damage from breaches

Microsegmentation & Monitoring

Networks divided into isolated isolated zones, with continuous continuous threat detection.

- Enables rapid breach containment

NETWORKS PLUS

Benefits of Zero Trust

Reduced Attack Surface Surface

Limits how far attackers can can move if breached.

Enhanced Detection & & Response

Identifies and contains threats faster than legacy models.

Better Compliance & Savings

Meets standards like GDPR; reduces breach costs by 30% on average.

NETWORKS PLUS

Implementing Zero Trust: A Step-by-Step-by-Step Approach

1

Identify Protect Surface

Pinpoint critical data, assets, applications, and services at risk.

2

Map Transaction Flows

Understand data movement and user access patterns.

3

Build Architecture & Define Policies

Design security controls, set and enforce robust access rules.

4

Monitor & Maintain

Continuously adapt to threats, improving protections over time. over time.

NETWORKS PLUS

Real-World Examples of Zero Trust

Google BeyondCorp

Access based on user and device, device, no VPN required.

Department of Defense Defense

Mandating Zero Trust across all all agencies by 2027.

Netflix

Zero Trust for secure content delivery at global scale.

Cloudflare

Protects web applications using using Zero Trust principles.

NETWORKS PLUS

Challenges of Implementing Zero Trust

Complexity

Requires skilled planning, significant resource allocation, and phasing.

Legacy Integration

Older systems may resist or slow down implementation efforts.

User Experience

Security must not hinder productivity or frustrate users.

Cultural Shift

Internal buy-in is critical to transformative security adoption.

Future Trends in Zero Trust

AI-Driven Automation

Intelligent systems to to speed up threat detection and response.

Identity Focus

Access management management centered centered on user and and device identity.

Security Service Service Edge

Cloud-based security security solutions integrated with networking.

Data Access Control

Securing connections connections to critical critical data sources.

Conclusion: The Future of Security is Zero Trust

Proactive Strategy

Adopt Zero Trust as an ongoing, ongoing, evolving security process.

Mindset Shift

Emphasize continued learning and vigilance across the organization.

80% Fewer Incidents

Organizations see a major reduction in security breaches breaches after adoption.

NETWORKS PLUS