

# LAN Security: The Future of Network Security Policy Enforcement



**Andy Patrick**  
**Senior Systems Engineer**  
Nevis Networks  
April, 2008

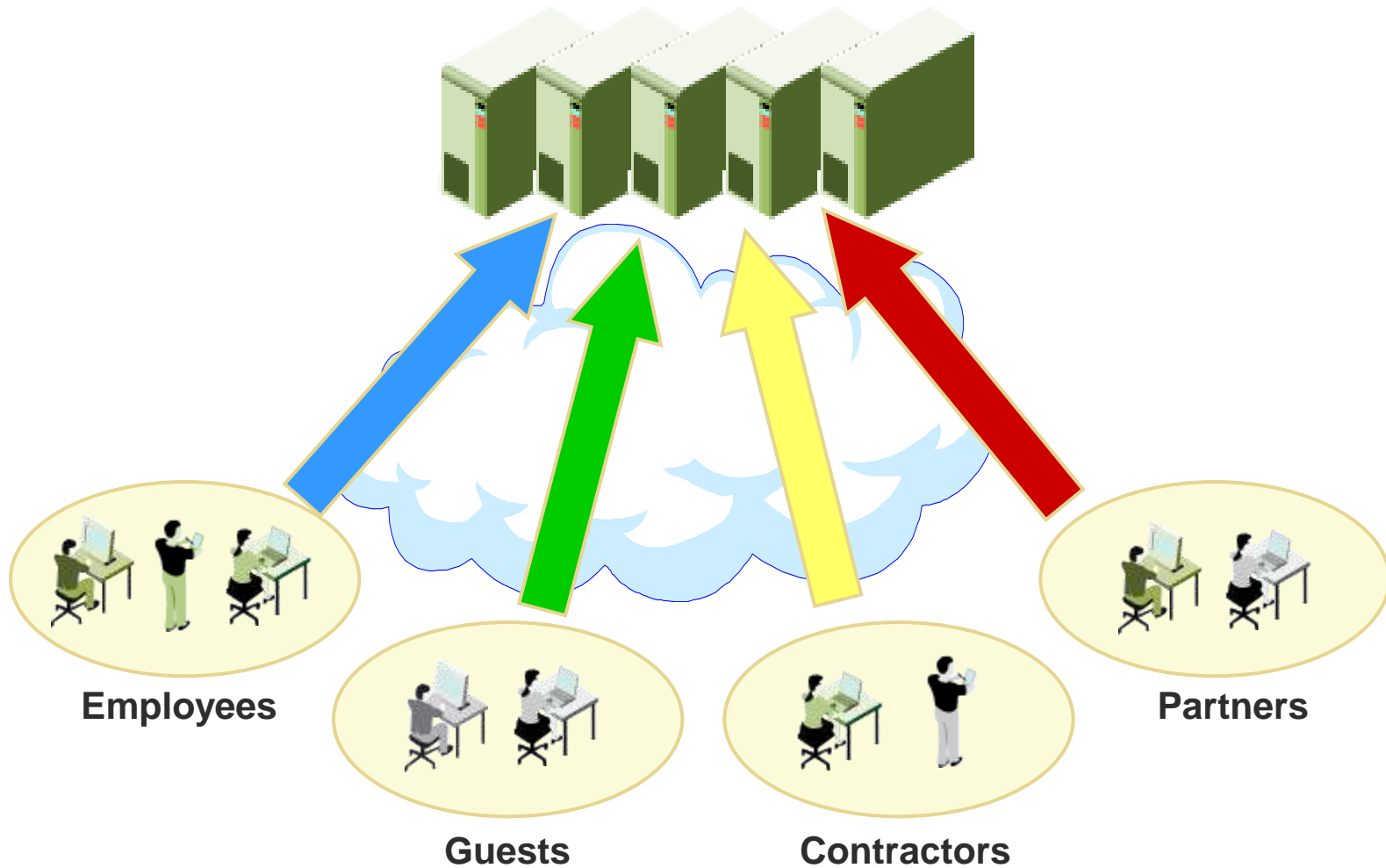
# The LAN Security Challenge



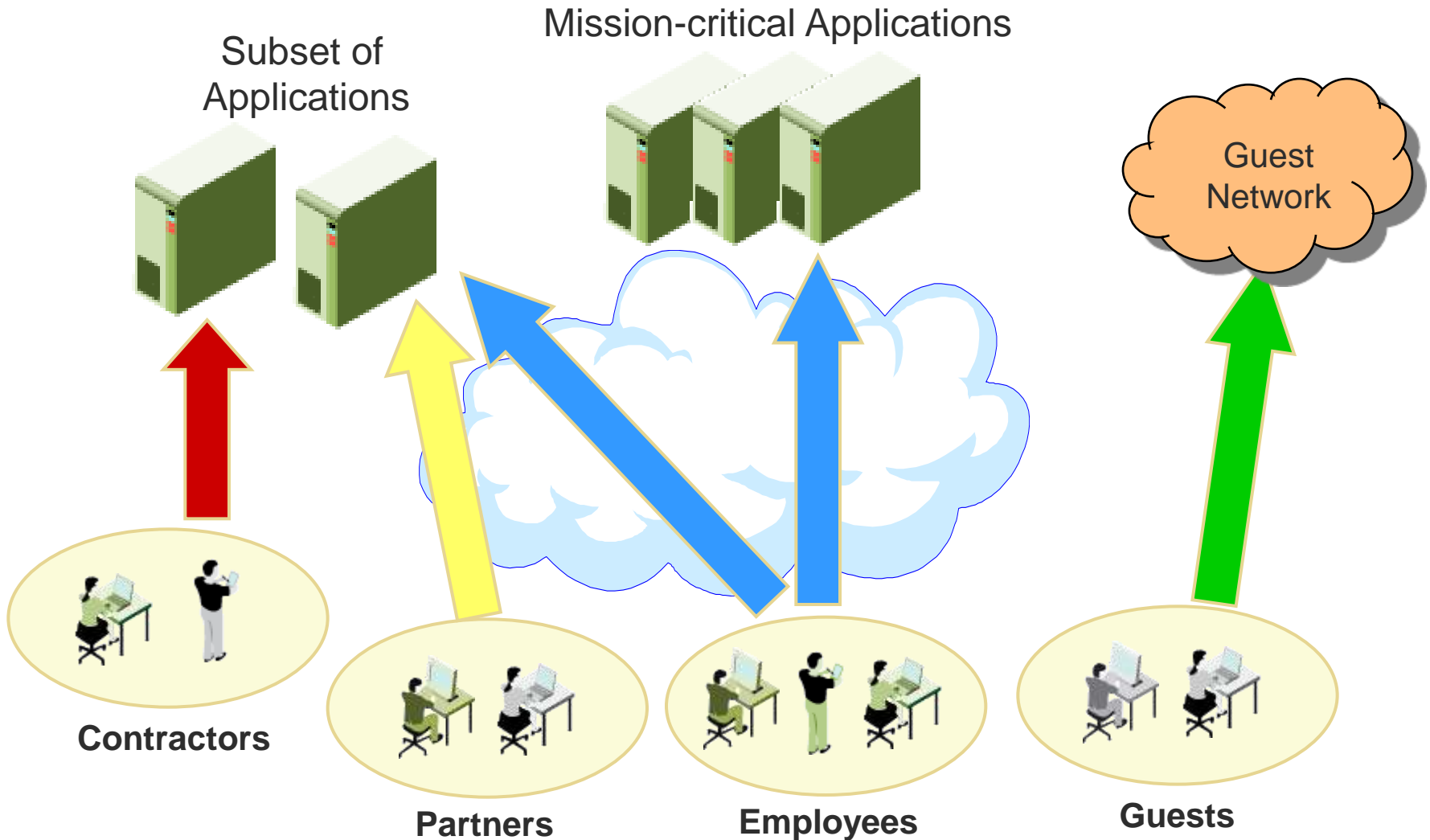
- Do you know **who's** on your network?
- What they're doing?
- Where they're going?
- Where they came from?
- Can you control their behavior?
- **Would you like to?**

# Enterprise Networks Are Anonymous

Mission-critical Applications and Servers



# The Identity-Aware Network



# Drivers for Identity-based LAN Security



## Network Availability

Guest PCs present a threat to the network.

## Protect Intellectual Property

Who has access to corporate secrets?

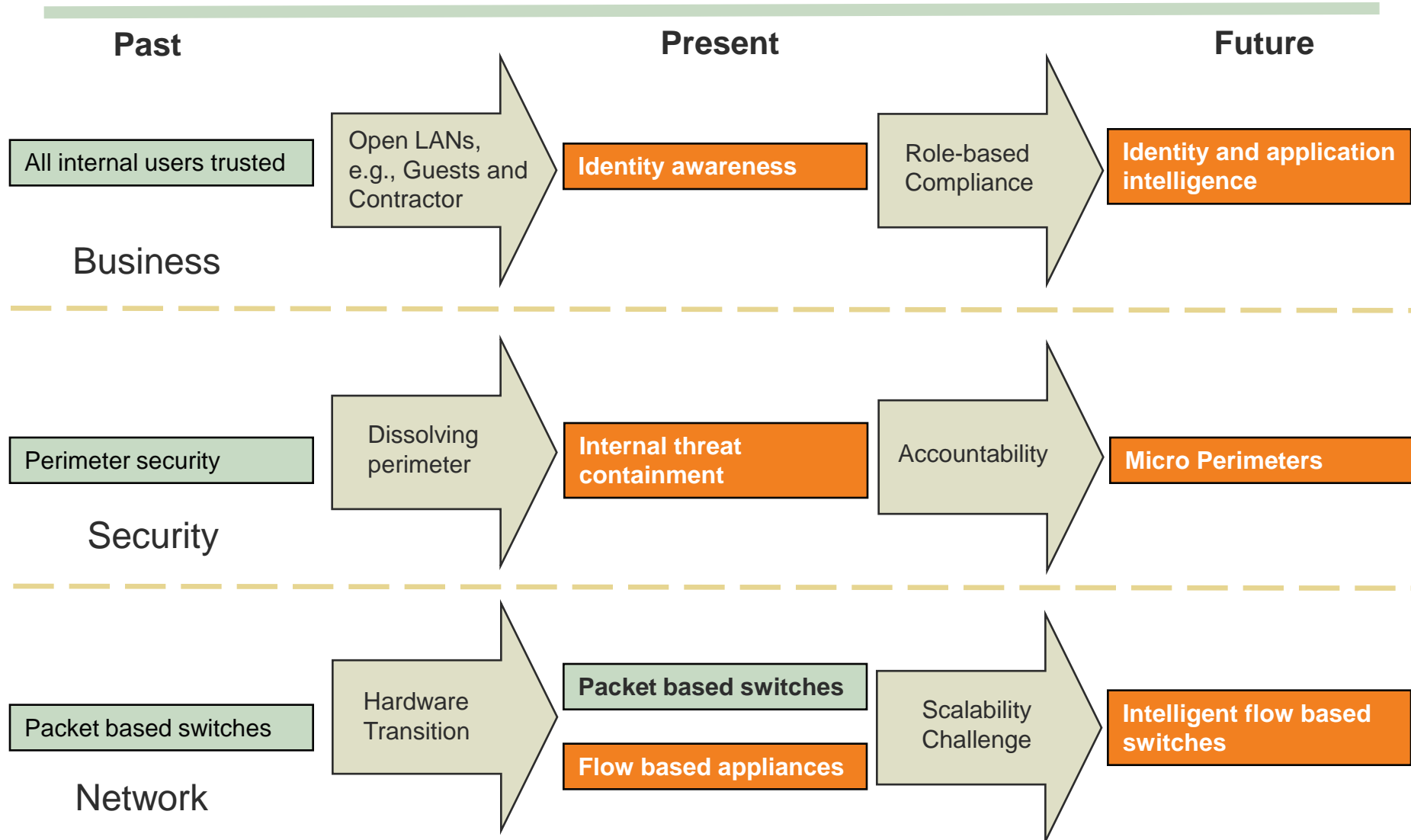
## Regulatory Compliance

- SOX
- HIPAA
- Other

## IT Cost Savings

Align network security architectures with business policies, and reduce costs of user mgt.

# Enterprise LAN Evolution



# Forrester's View

- The Problem: Managing all endpoint risks to the network
- Proactive Endpoint Risk Management (PERM)\*:
  - **Policy-based technology**
  - **Identity-based enforcement**
  - **Integrated security services**
    - Endpoint verification
    - Identity-based Access control
    - Threat prevention
    - Monitoring and reporting



- “PERM goes beyond NAC’s limited endpoint policy view”\*.

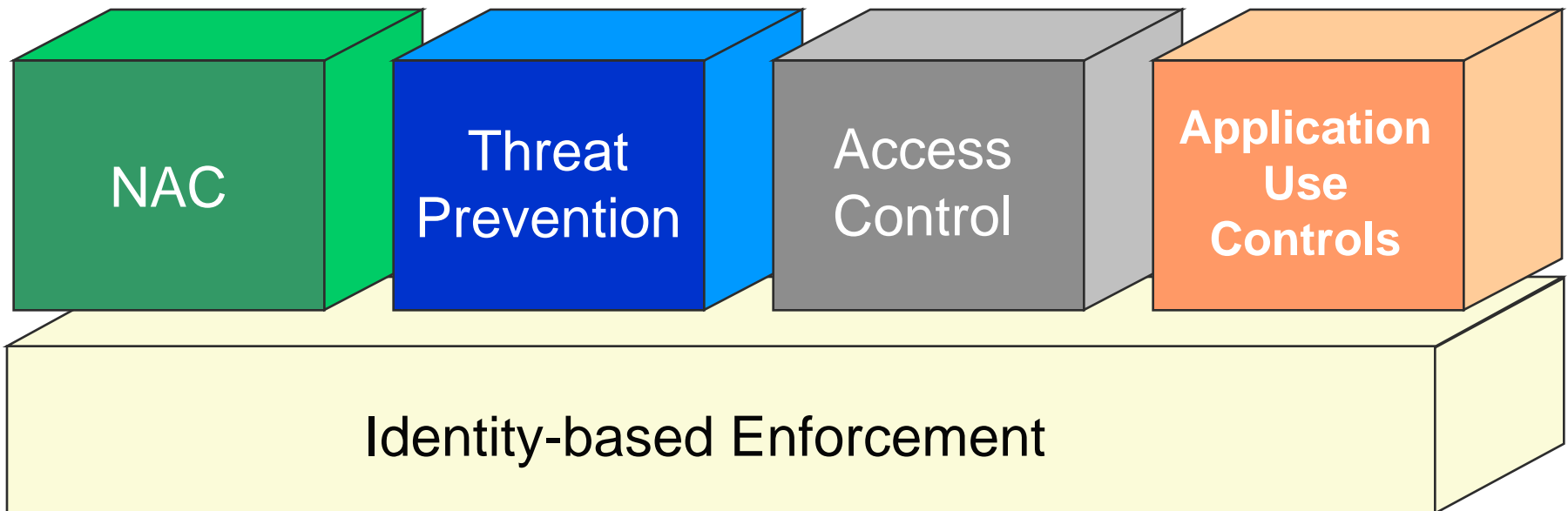
\* Source: Forrester Research, Client 2.0, March, 2007, Robert Whiteley and Natalie Lambert

# Alternative Identity-based Approaches

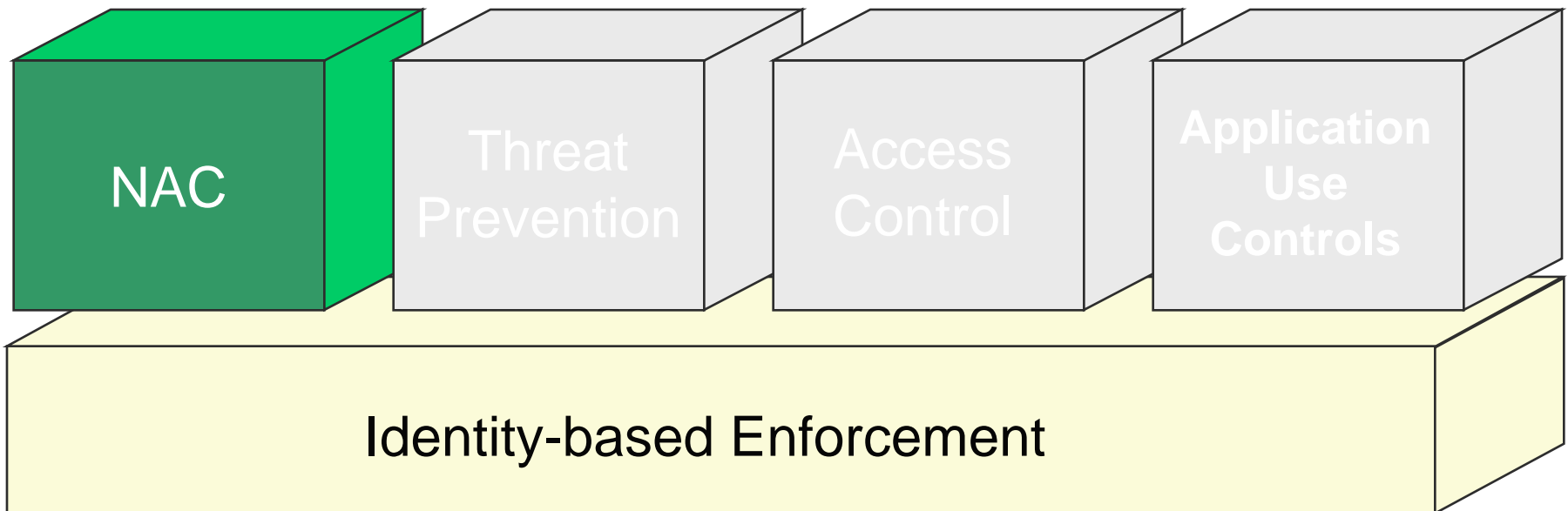


- 802.1X
  - Too many moving parts that don't work well together
  - Limited to identity checks for admission controls
  - No checks for posture compliance like NAC
  - Enforcement via VLAN steering is hard to manage/maintain
- Standalone (Pre-connect) NAC Solutions
  - Most "NAC" solutions limited to pre-connect admission checks
  - Most solutions are out-of-band with limited enforcement capability
  - Virtually no access control policy enforcement
  - No ability to detect malware after admission
  - VLAN steering not a viable remediation for non-compliant hosts
- Endpoint Security Suites
  - Designed to protect endpoints, not the LAN from endpoints
  - Can't enforce policies in the network where they can be most effective

# An Integrated Policy Approach



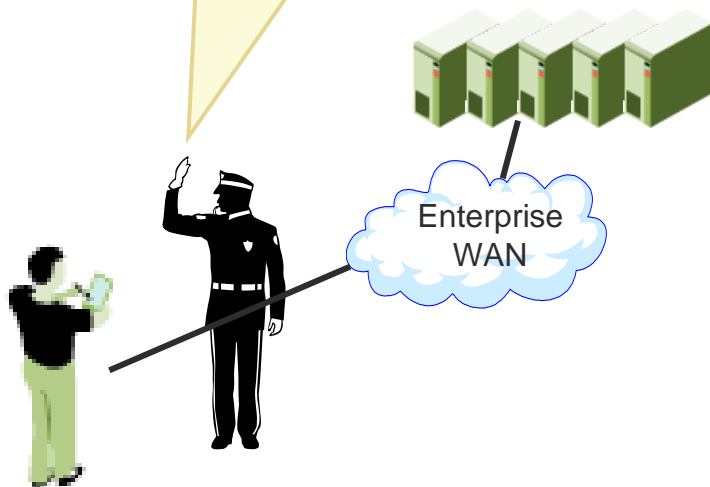
# Network Admission Control



# Network Admission Control

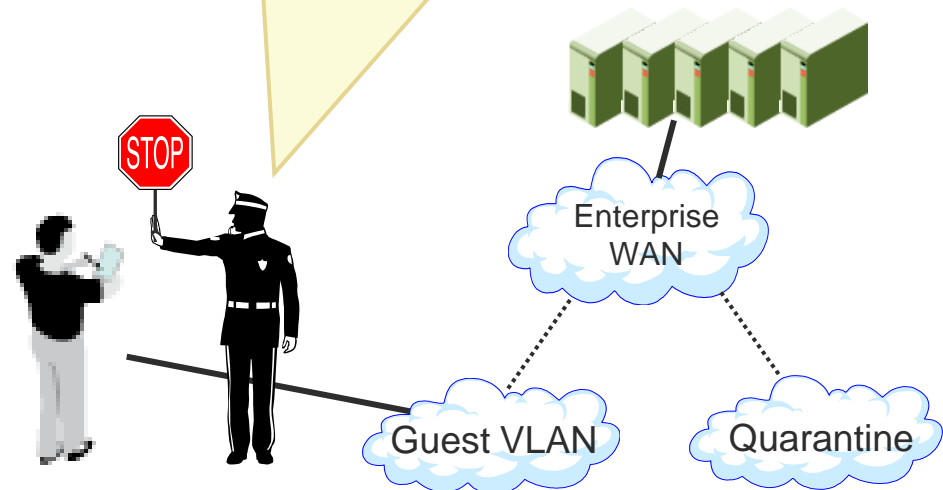
## Without NAC

Come on in, Everyone is Welcome. Here's your IP address...



## With NAC

1. Who are you? Are you in our directory?
2. Are you running current anti-virus, anti-spyware?
3. What OS? Is it patched?

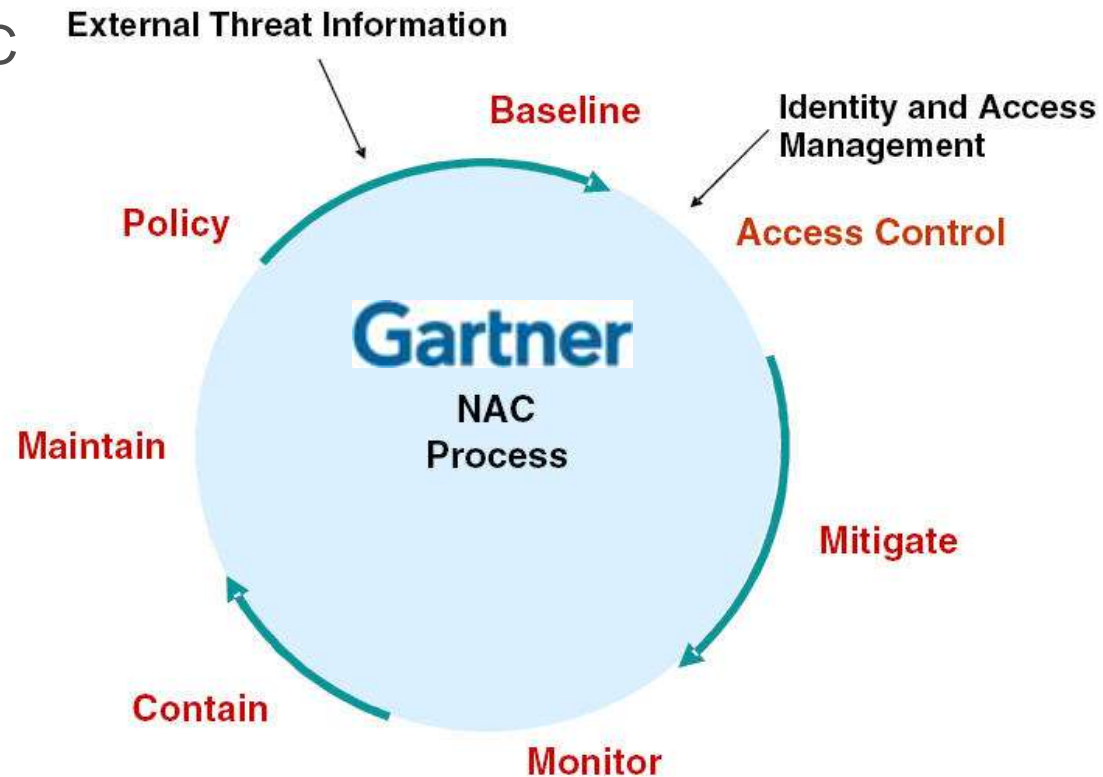


# Gartner's View: NAC Done Right



According to Gartner, the NAC process should:

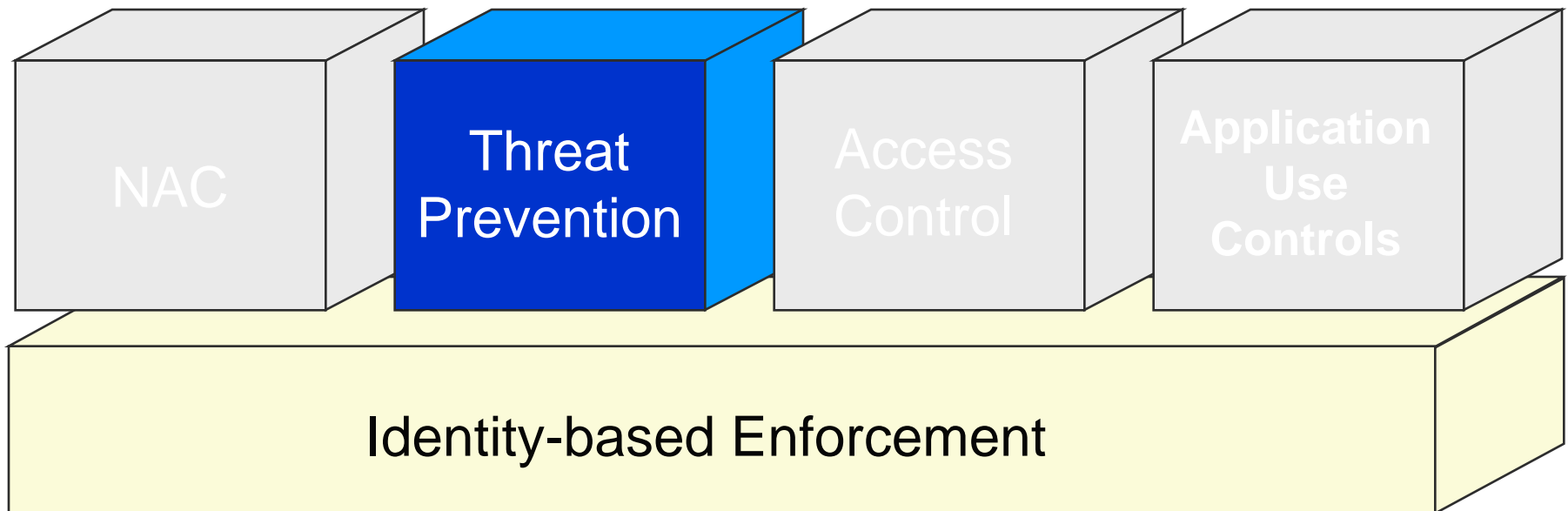
- be *continuous*
- include both pre- and post-authentication controls



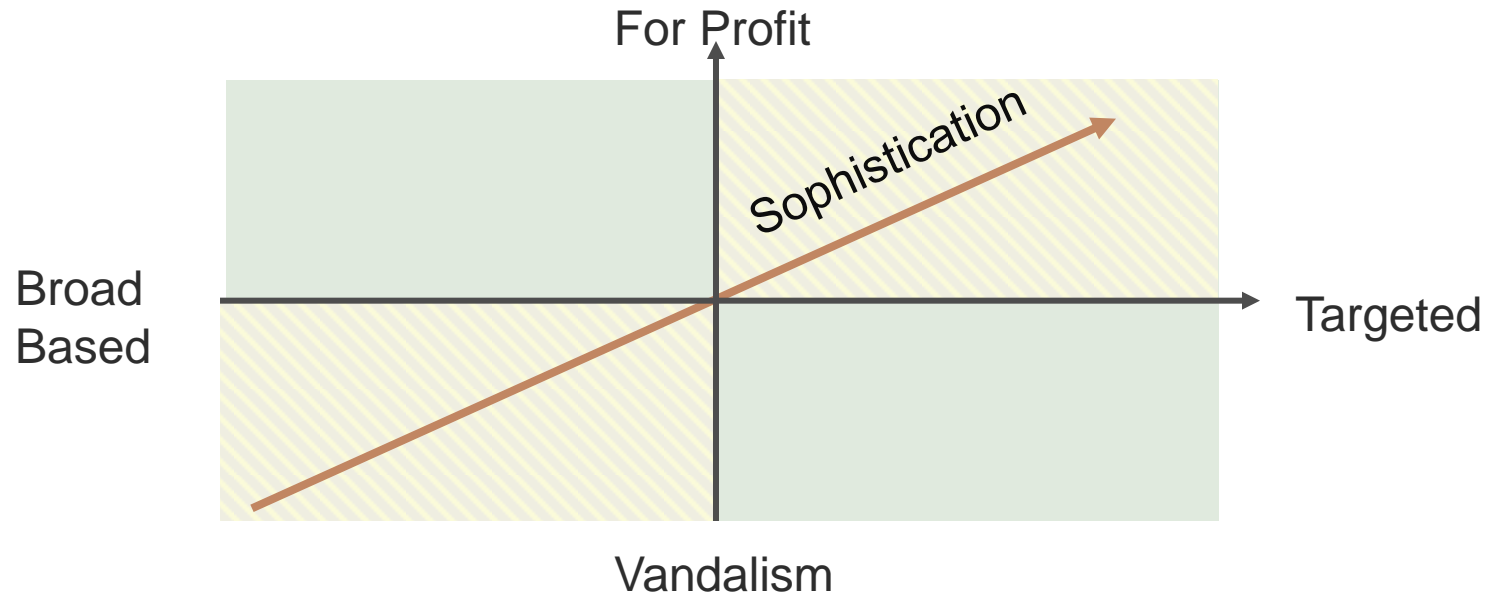
Source: Gartner Research (December 2004)

*“Continuous protection ensures availability and integrity of the IT infrastructure within a rapidly changing threat environment.”*

# Threat Prevention



# Enterprise Malware Trends



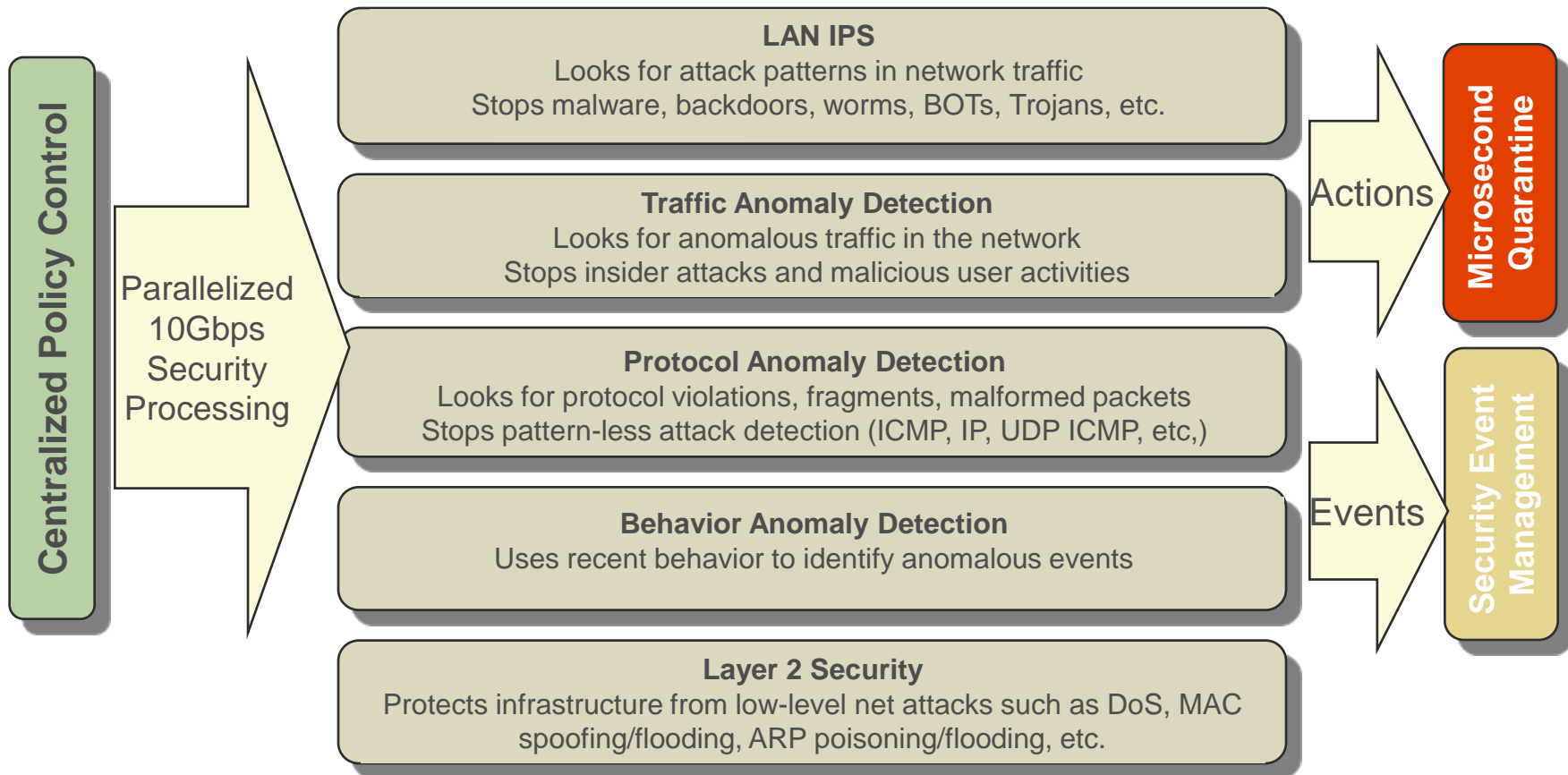
By year-end 75% of enterprises "will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses"

Source: Gartner Group

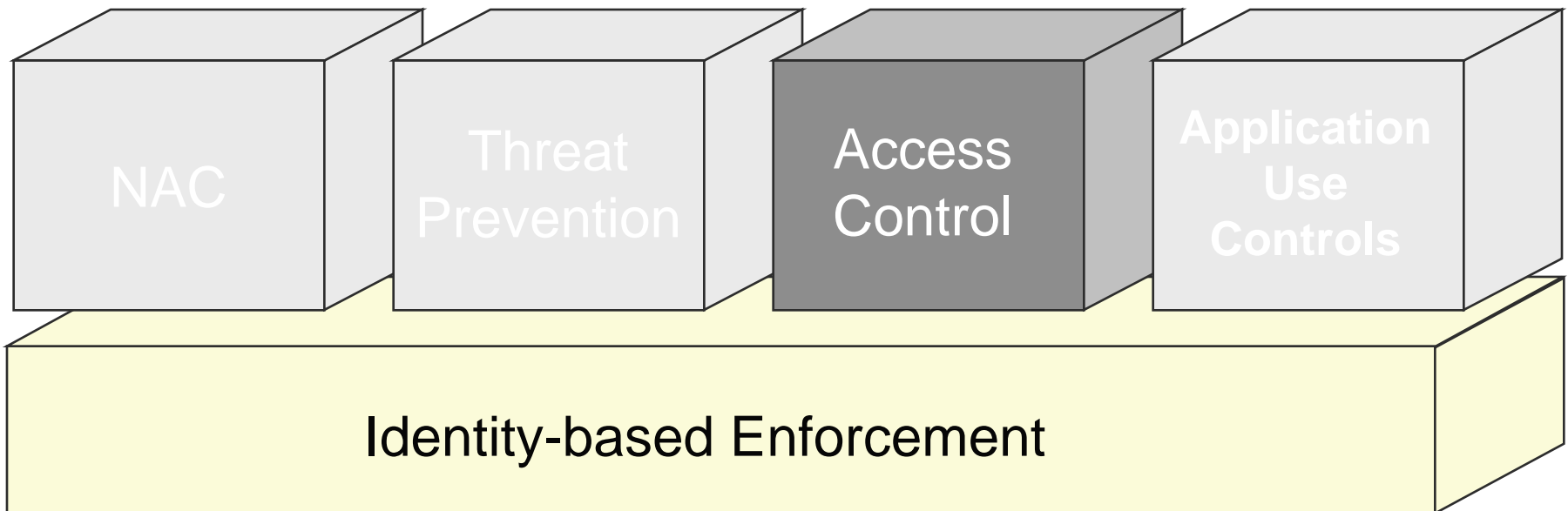
Of 4.5 million URLs analyzed, 450,000 - one in 10 - were "successfully launching drive-by-downloads of malware binaries."

Source: Google Research

# Integrated Threat Containment

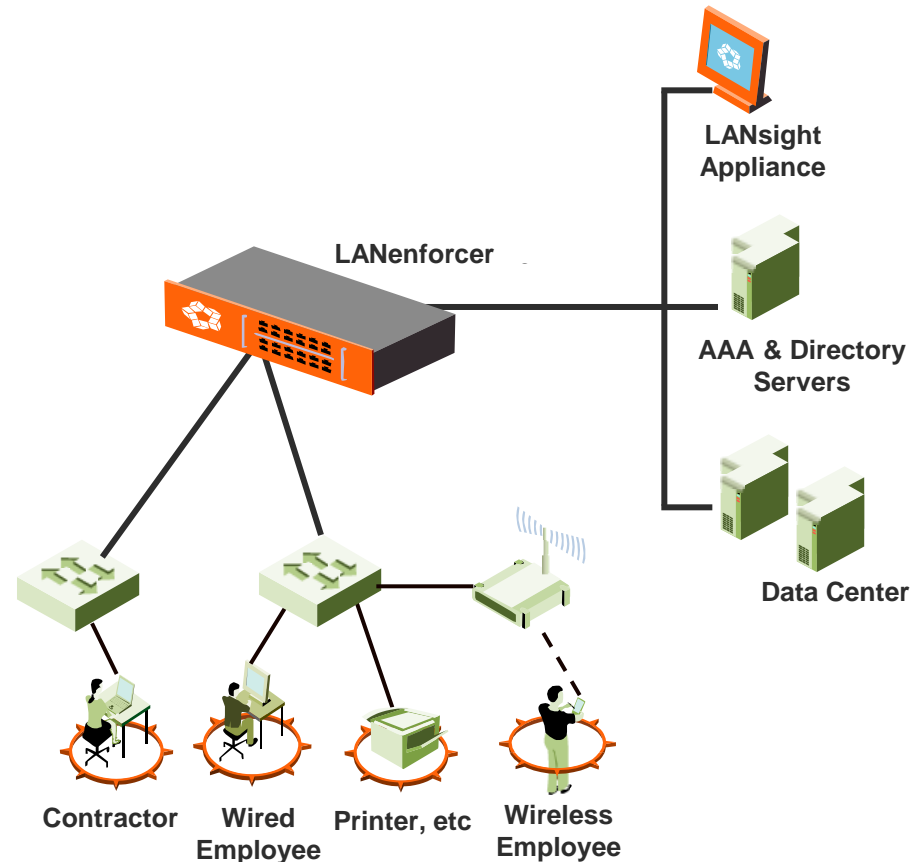


# Identity Based Access Control

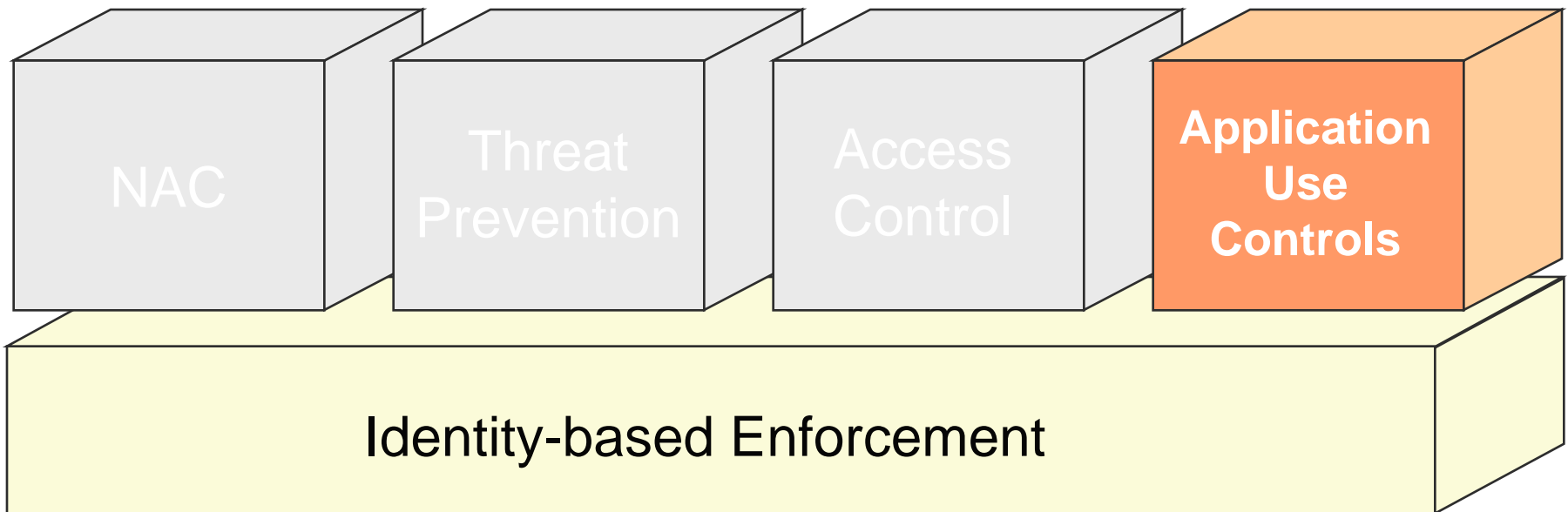


# How Nevis Does It

- Associates each network session with a specific user ID
- Uploads role-based access policies from AAA server and LANsight management console
- Analyzes each packet flow for conformance with access policy at wire speed (10 Gbps)
- Non-compliant packets dropped in the network, not at the server
- Deployed as an access layer switch or transparent appliance (bump in the wire)



# Application Usage Control

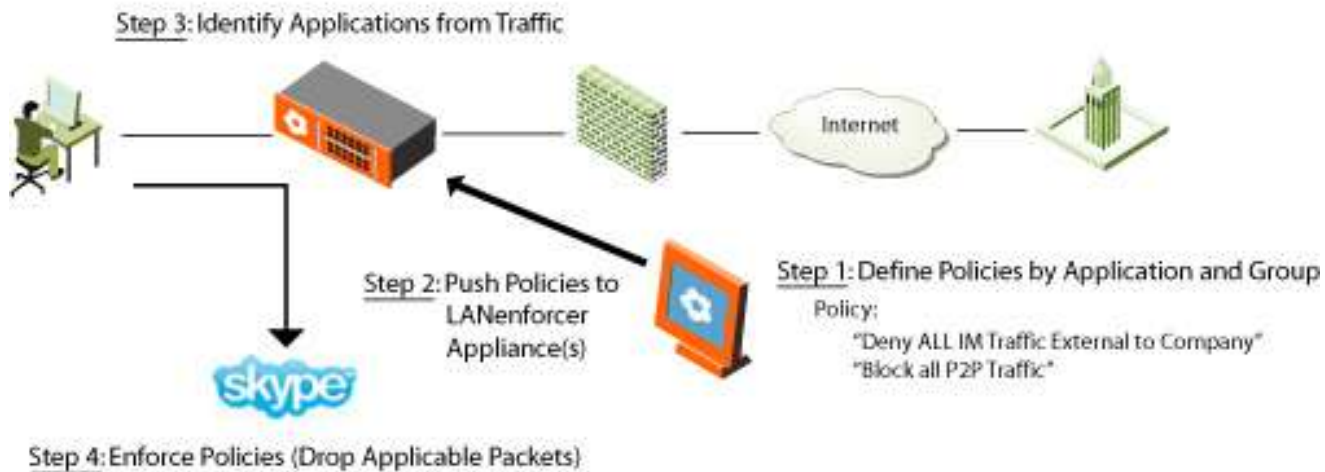


# Application Use Controls

## Peer-to-Peer (P2P) Applications



## Instant Messaging (IM) Applications

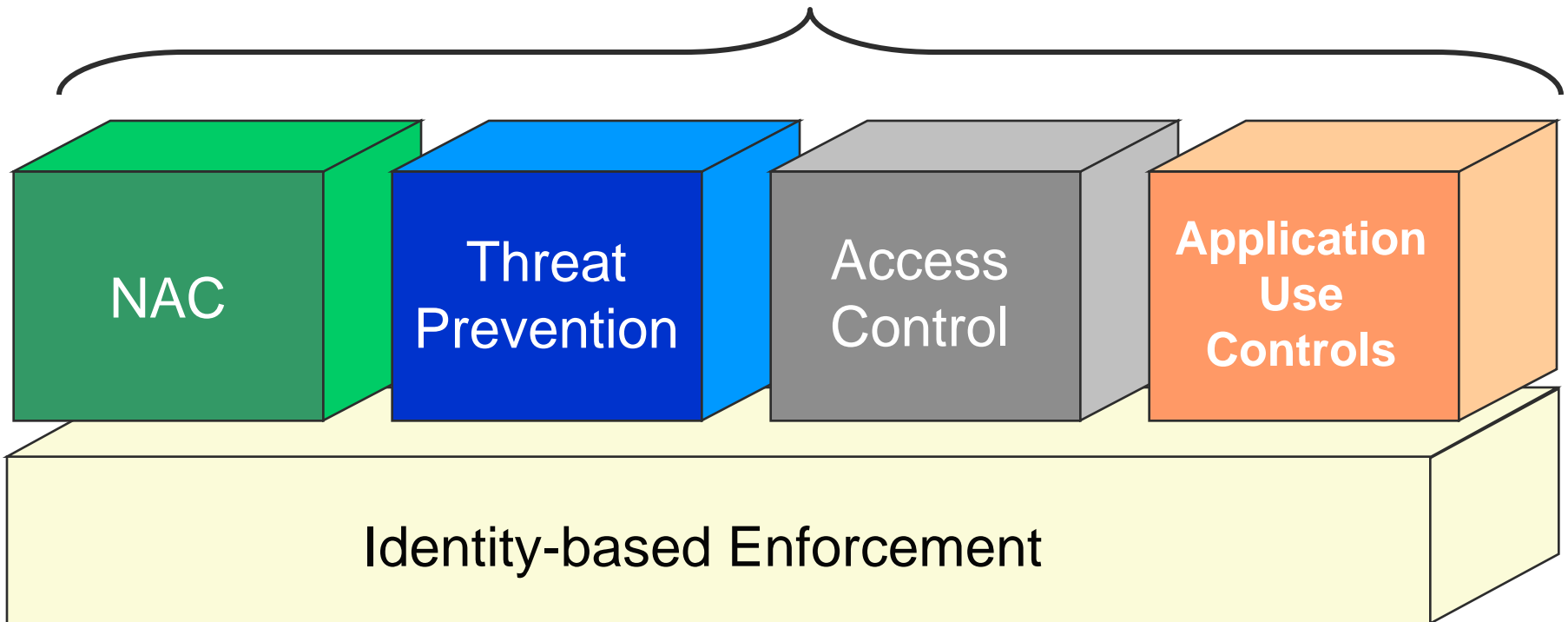


Appropriate use policies linked to user identity

# LAN Security Done Right



## *Identity-driven LAN Security*



# Implementing Identity-driven LAN Security



- Key Considerations:
  - Define primary and secondary goals
    - Securing guest access?
    - Checking endpoint compliance?
    - Enforcing employee access policies?
    - Monitoring user activity?
  - Cost and complexity of initial deployment and maintenance overtime
  - Impact on end-users – level of transparency
  - Scalability and growth plan
  - Phased implementation is recommended
- Architectural options:
  - Agent-based
  - Agent-less
  - Inline appliances
  - Out-of-band appliances
  - Secure Switches



# Thank You!

- LANenforcer 1048 secure switch
- LANenforcer 2024/2124 LAN security appliance
- LANSight security management appliance

