

LAN Security: The Future of Network Security Policy Enforcement



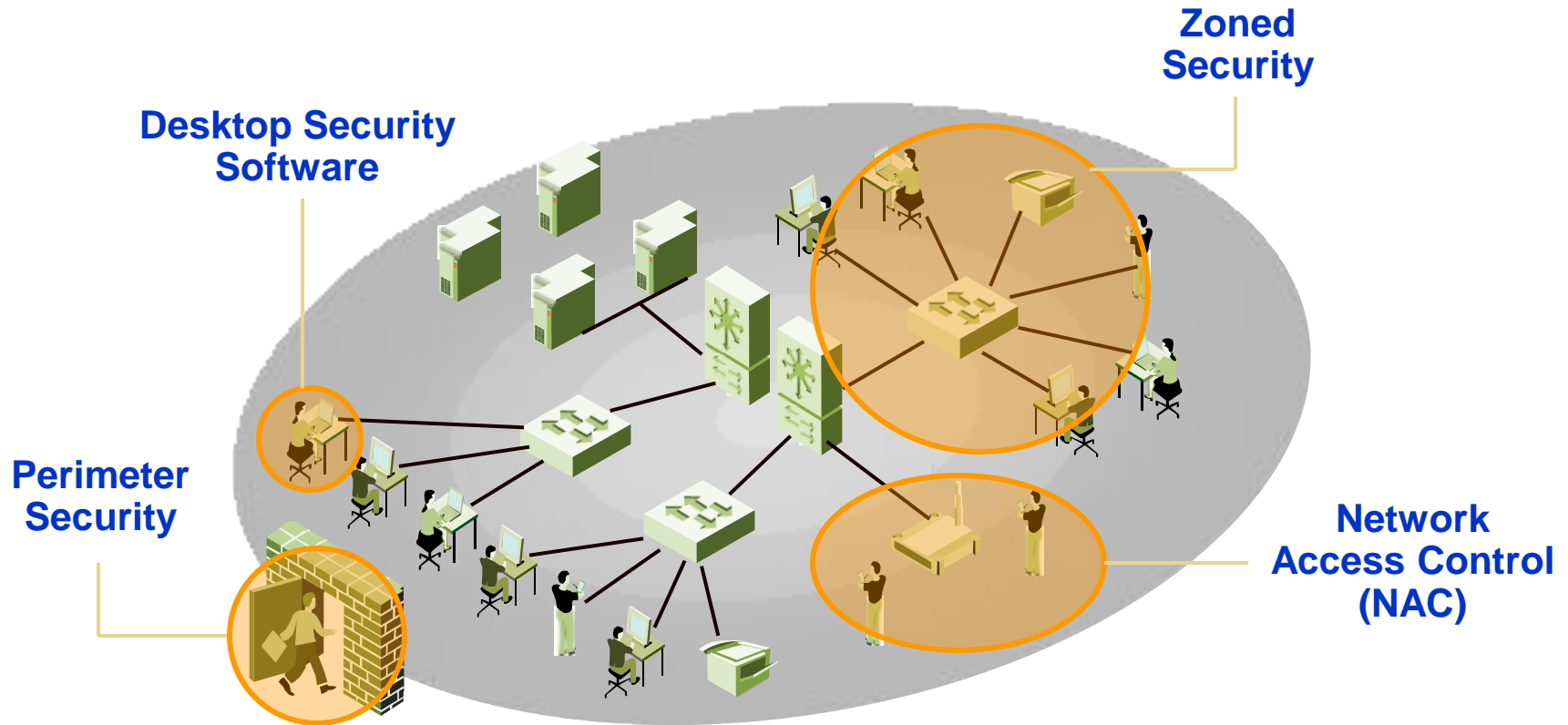
Kevin O'Connor
VP Sales
Nevis Networks
June, 2008

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?**

Traditional Security Approaches...



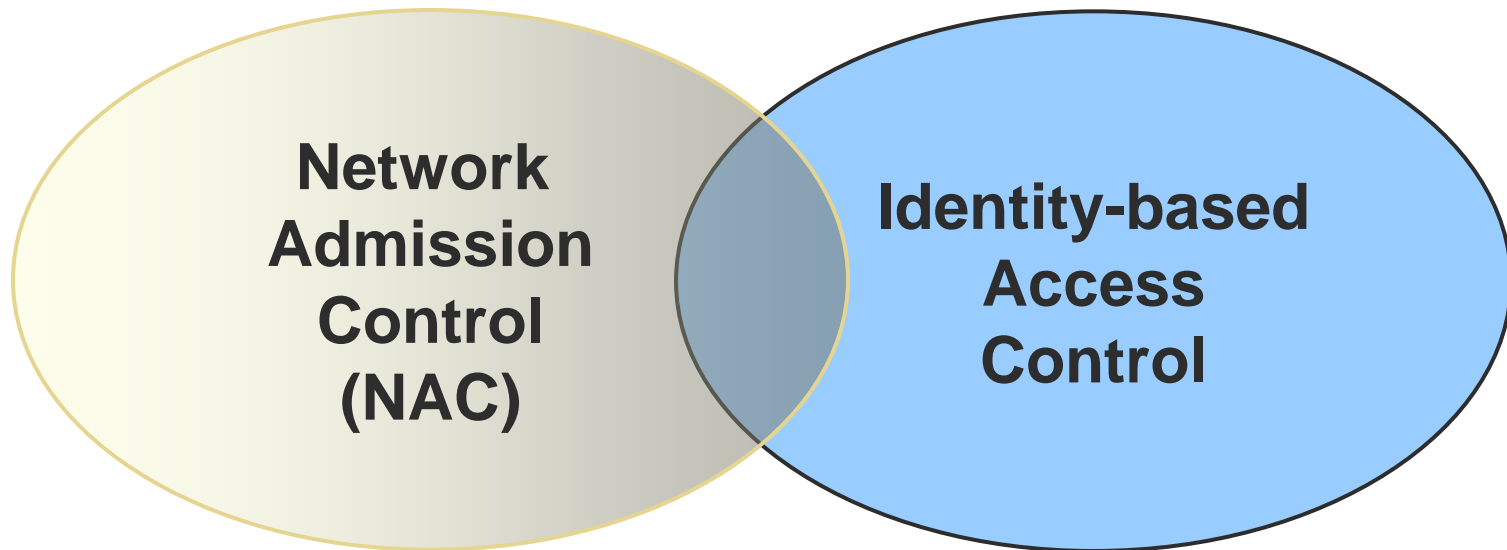
... are **Expensive and NOT Effective**
against **New Malware**

Assessment and Enforcement



- NAC can be broken up into three stages
 - First stage determines the assessment of the incoming endpoint (NAC) Network Admission Control.
 - Second Stage is a decision point based on the endpoint assessment and access control (Policy)
 - Third Stage is where those decisions are enforced

An Integrated Solution



A complete access solution requires:

- **Compliance checks for network access**
- **Differentiated access to applications and data**

Getting the NAC



Three significant parties have championed the NAC formalization.

- Cisco 2003 NAC (Network Admission Control)
- Leverage Network Hardware
- Microsoft followed with NAP in late 2004
- Leverage its Operating System
- The Third NAC frame work is TCG (Trusted Computing Groups)
- This provides open standards for multi venders

*Cisco may require homogenous environments (all their hardware)

*NAP You need Vista, XP SP3 or Server 2008

Answer Three Core Questions—At All Times



- **Is my network secure?**
 - Threat assessment?
 - Un-authorized access?
 - Looking beyond the perimeter security measures.
 - Do I know who is on my network?
- **Is my network compliant?**
 - What is my response: “Is my security policy enforced properly”?
 - Can I demonstrate regulatory compliance?
 - Guest Access?
- **Is my network at risk?**
 - Confidence: “The number of point products needed to address the threats can become an unmanageable number”
 - Antivirus, Malware/Spyware, and OS patching
 - Can I tell if my risk is increasing or decreasing over time?

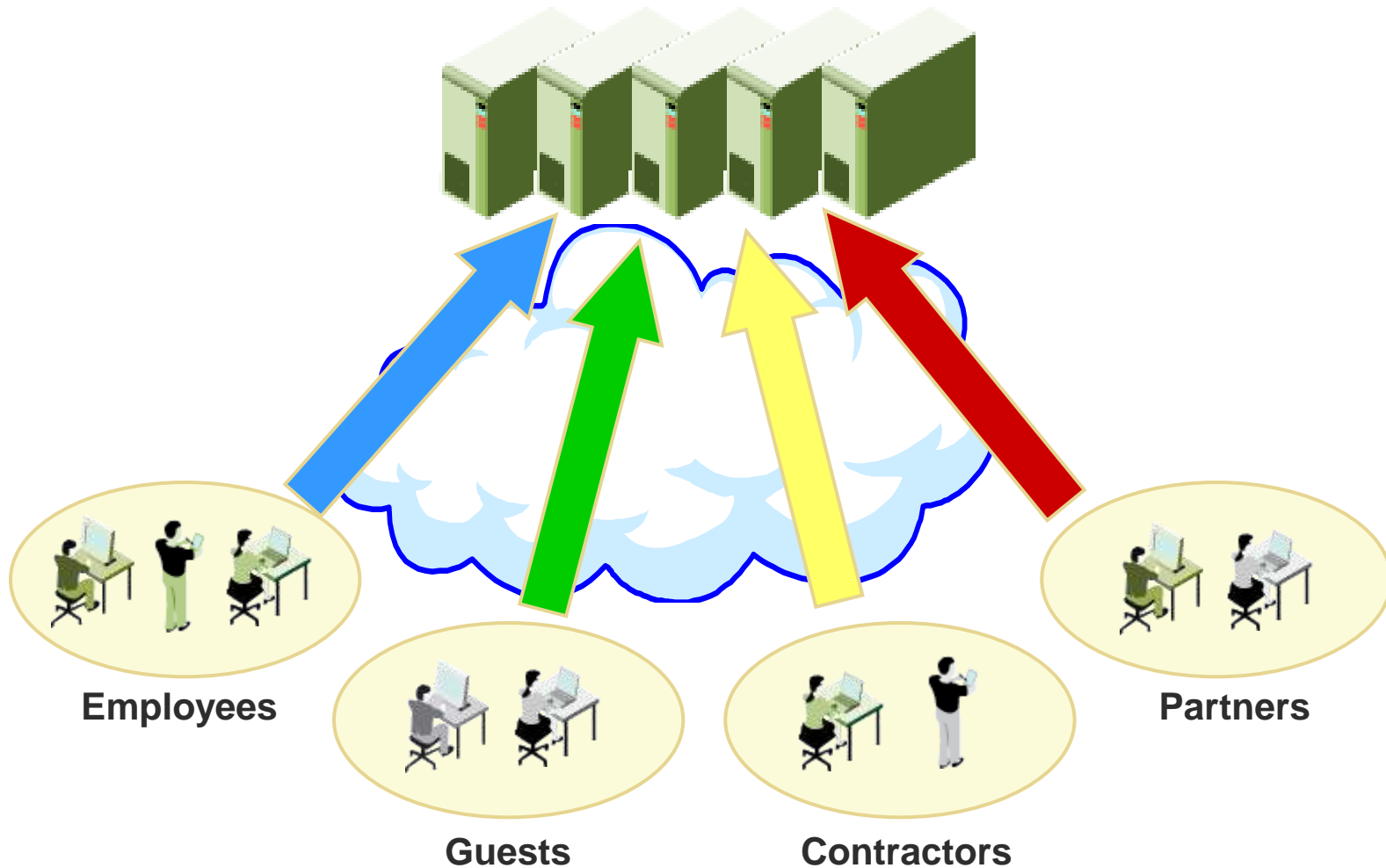
So what are the problems?



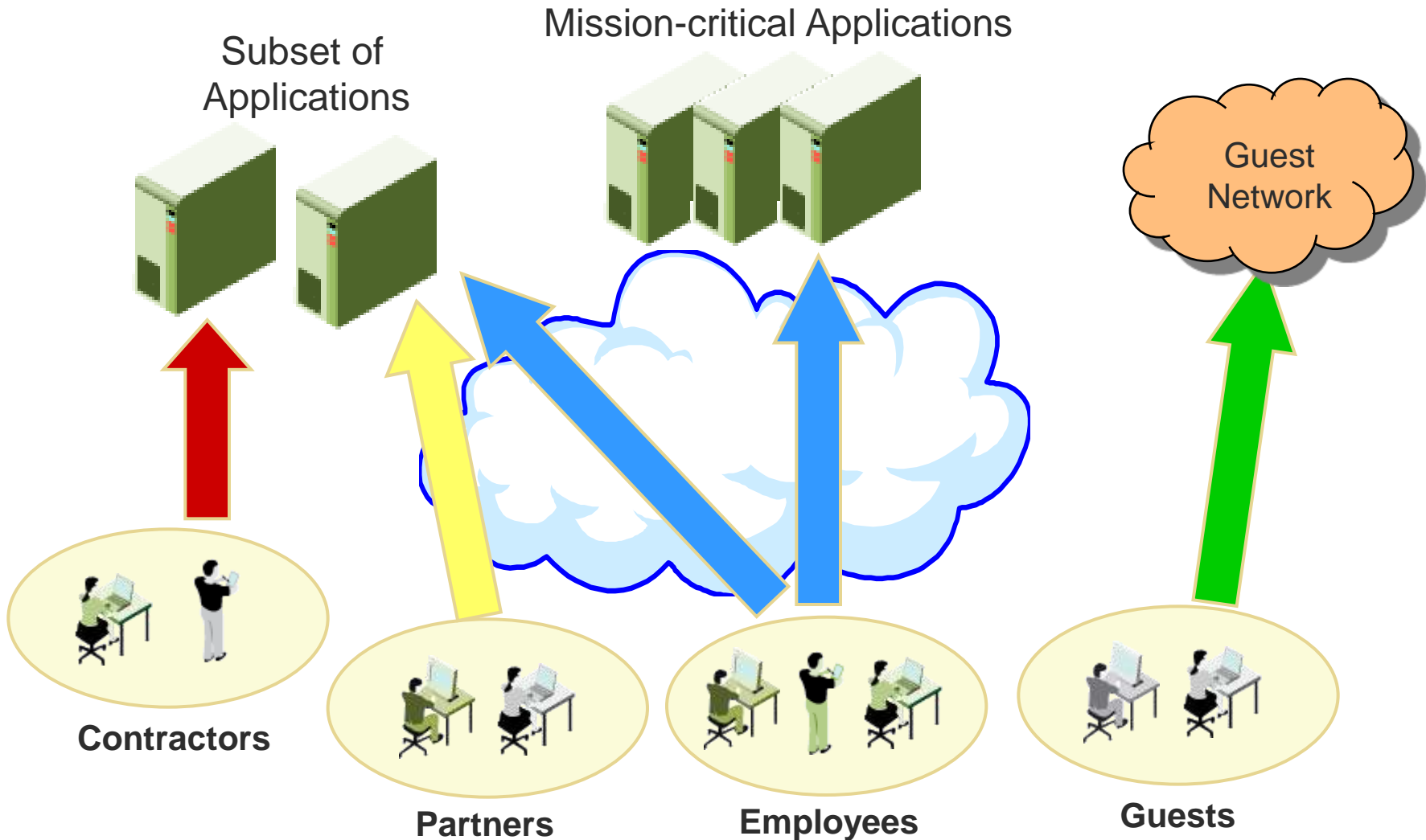
- Enterprise Malware Trends: Crimeware, spyware, malware – out breaks and the impact to the network....
- End Point Posture Checks: anti virus, malware software, and OS patch levels
- Guest Access limited access (can see your network) unknown endpoints that are not managed by your organization
- Internal employee access while you own these they are still a challenge keeping up with policy enforcement
- Monitoring and Reporting for corporate compliance or regulatory.

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.

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

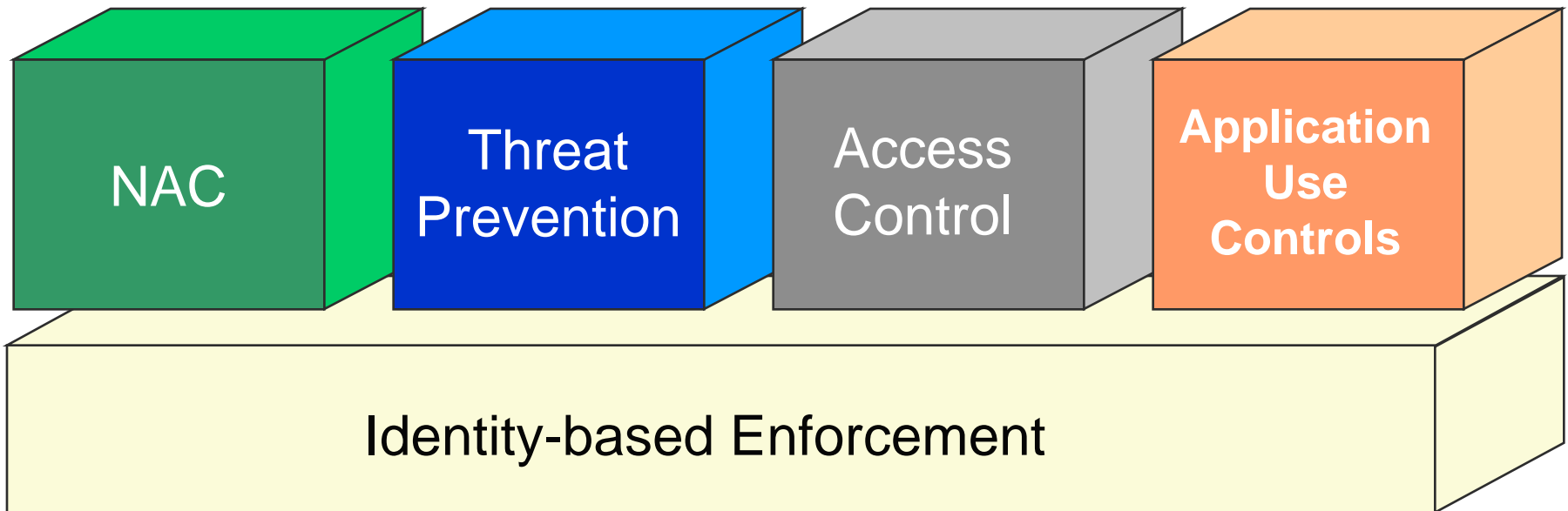
What's New? – Cisco TrustSec



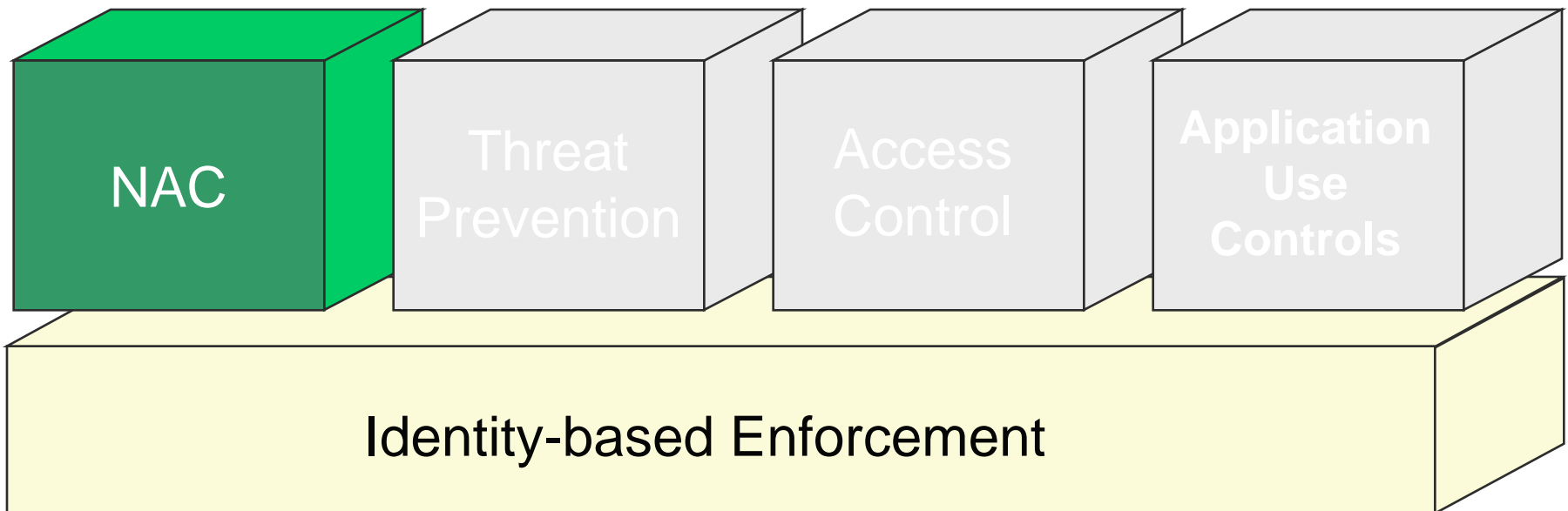
Cisco has validated Identity-Driven Access Control for the LAN
TrustSec is proof that Topology-Driven approaches are unworkable

- What is it?
 - Next phase of Cisco Self Defending Network Story
- What does it include?
 - Role based ACLs on campus switches
 - Converged policy framework
 - Confidentiality of communication between campus endpoints
- When is it available?
 - Q1 2008 on Cat 6k, other switches will be supported later
- How does it work?
 - Based on IEEE 802.1AE standard for Link layer Security
 - Leverages IEEE 802.1X and IEEE 802.1AF for key management
 - Extra “tag” field in Ethernet header maps to user role
 - Provides link layer encryption on a hop-by-hop basis
- Does it replace Cisco NAC?
 - No, they pitch this as complementary to NAC and other security products (?!?)
 - This is Cisco’s version of post-connect access control

An Integrated Policy Approach



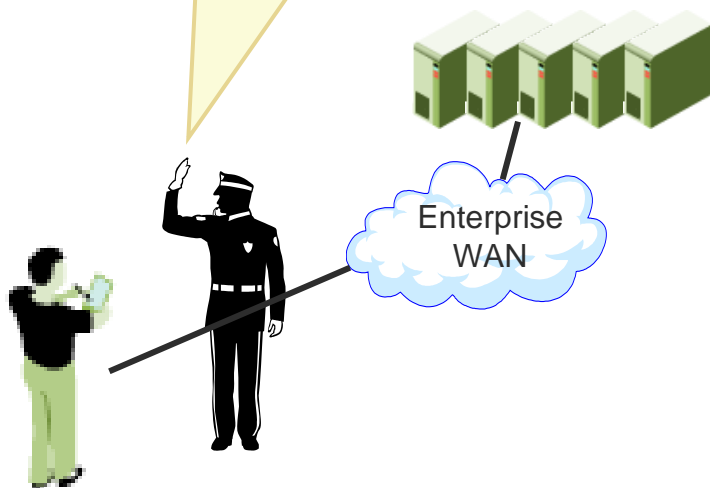
Network Admission Control



Network Admission Control

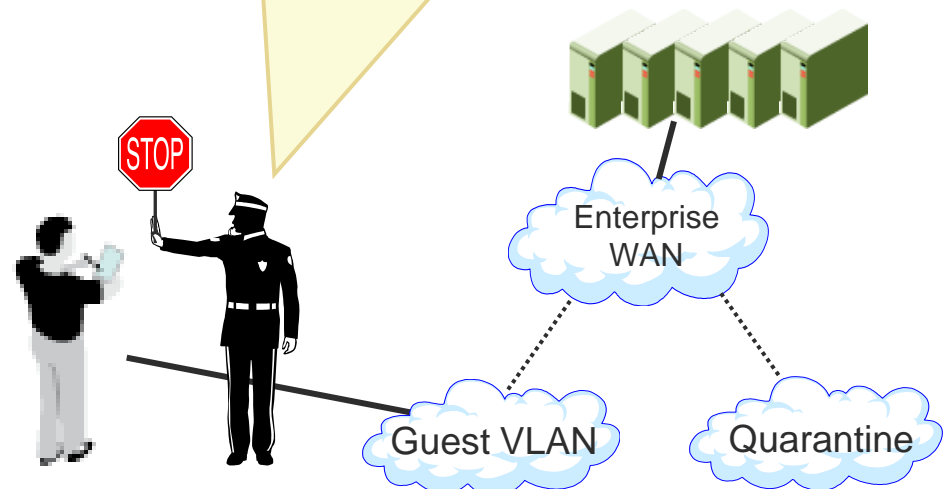
Without NAC

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?

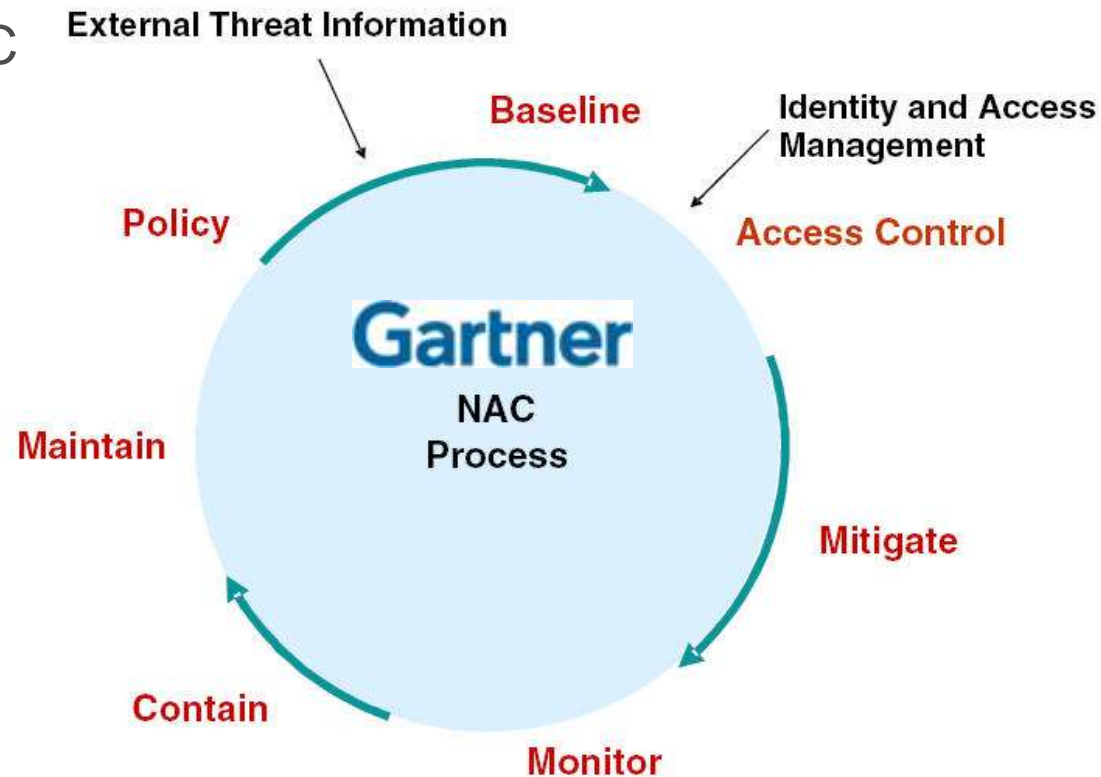


Gartner's View: NAC Done Right



According to Gartner, the NAC process should:

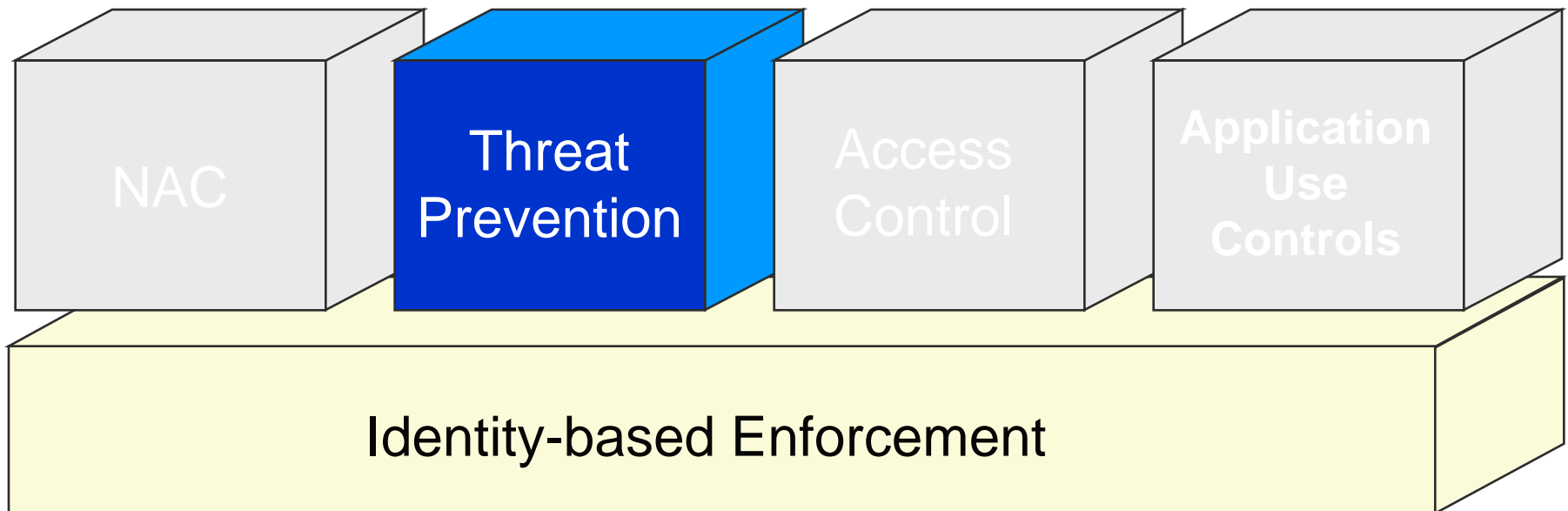
- be *continuous*
- include both pre- and post-authentication controls



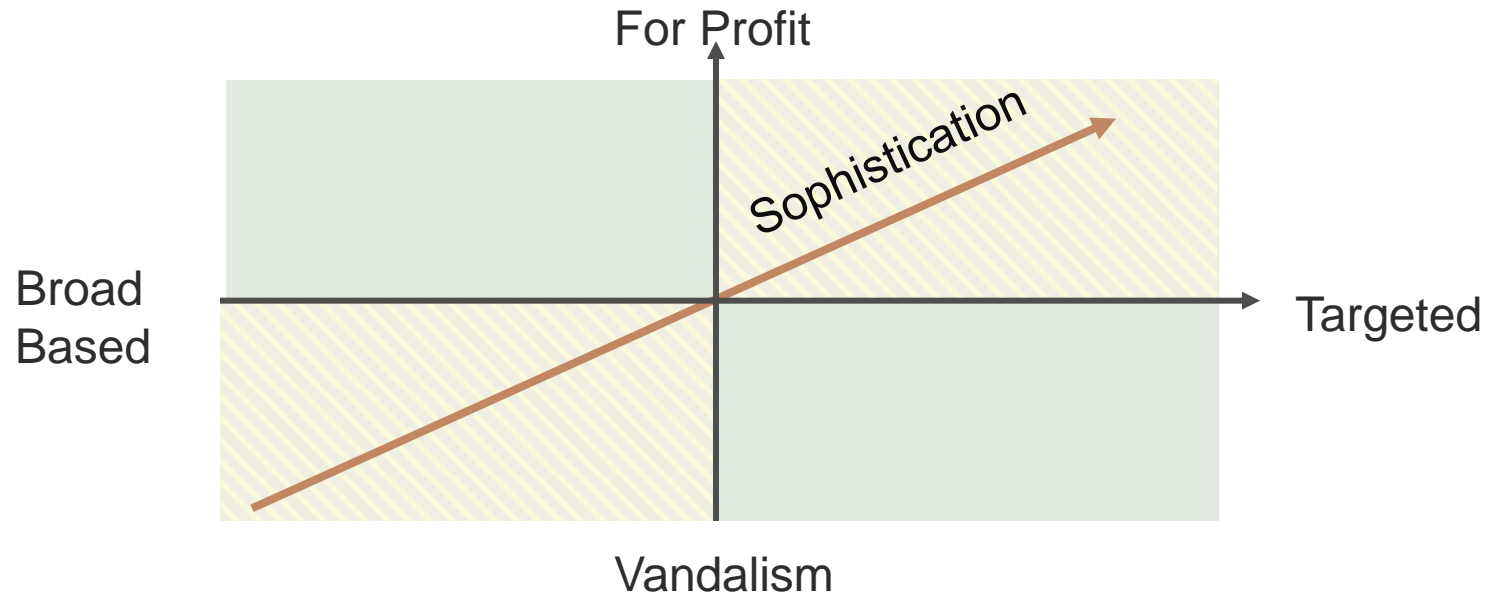
Source: Gartner Research (December 2004)

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

Threat Prevention



Enterprise Malware Trends



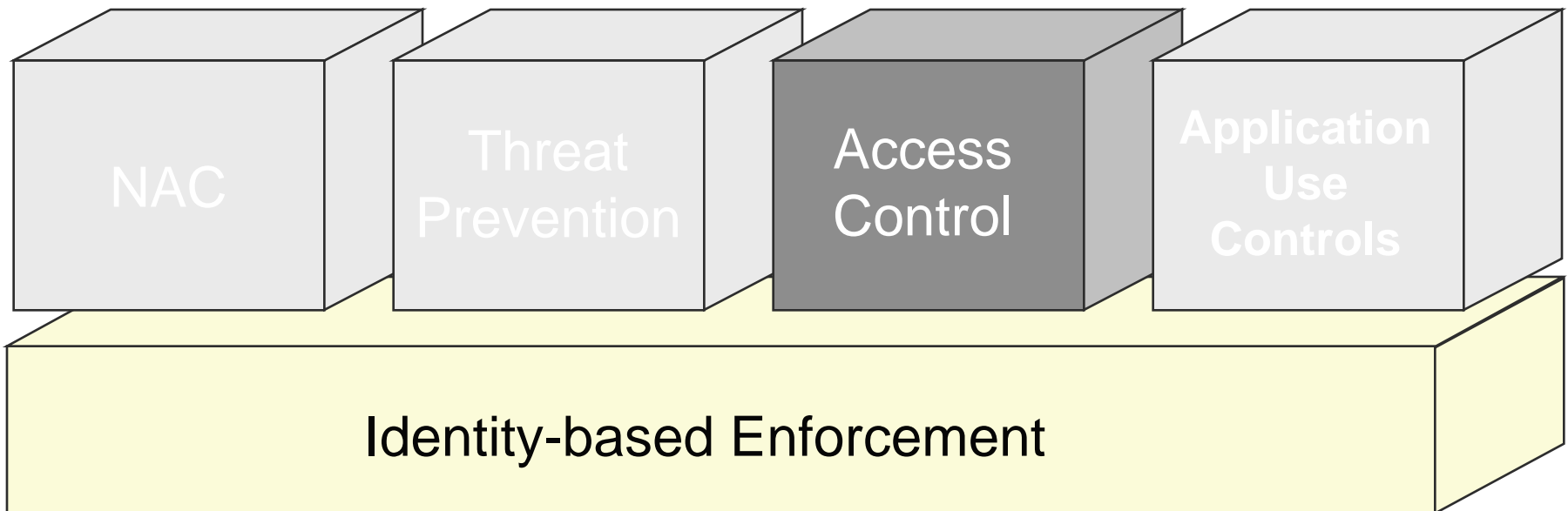
By year-end 75% of enterprises "will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses"

Source: Gartner Group

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

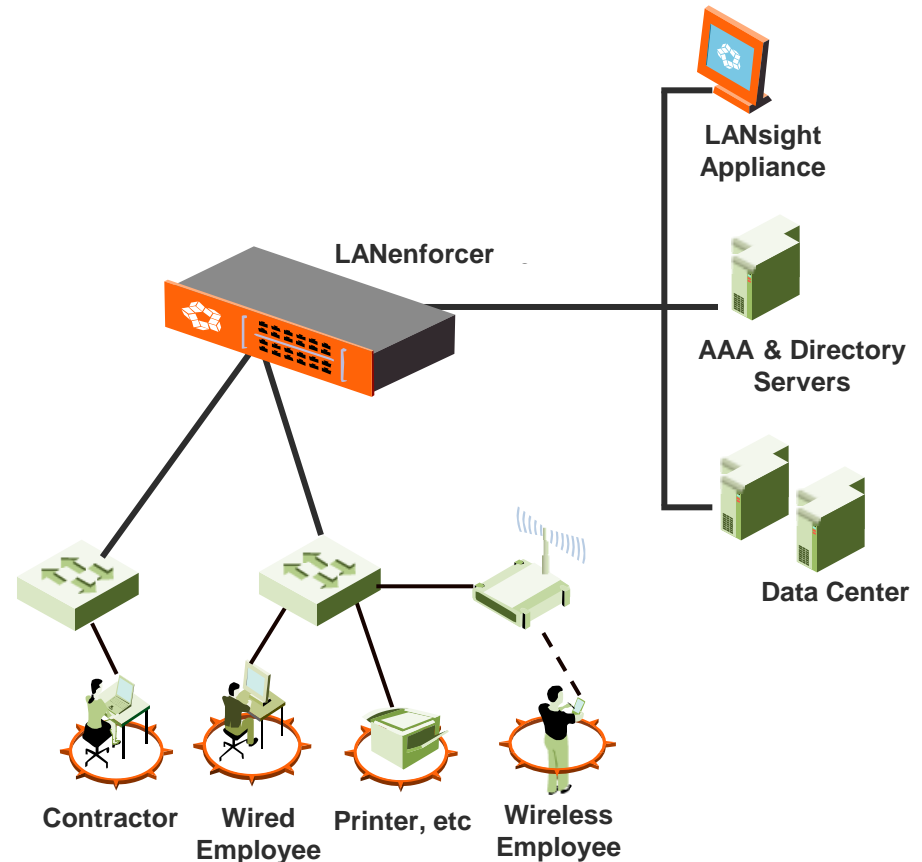
Source: Google Research

Identity Based Access Control

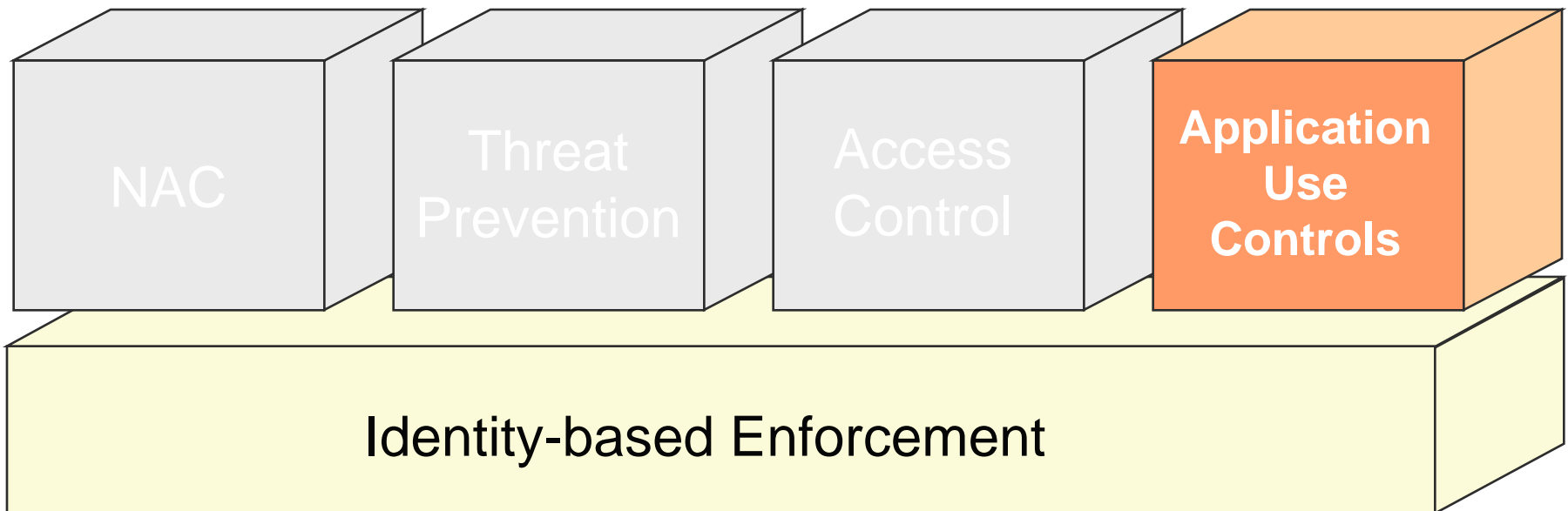


How Nevis Does It

- 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

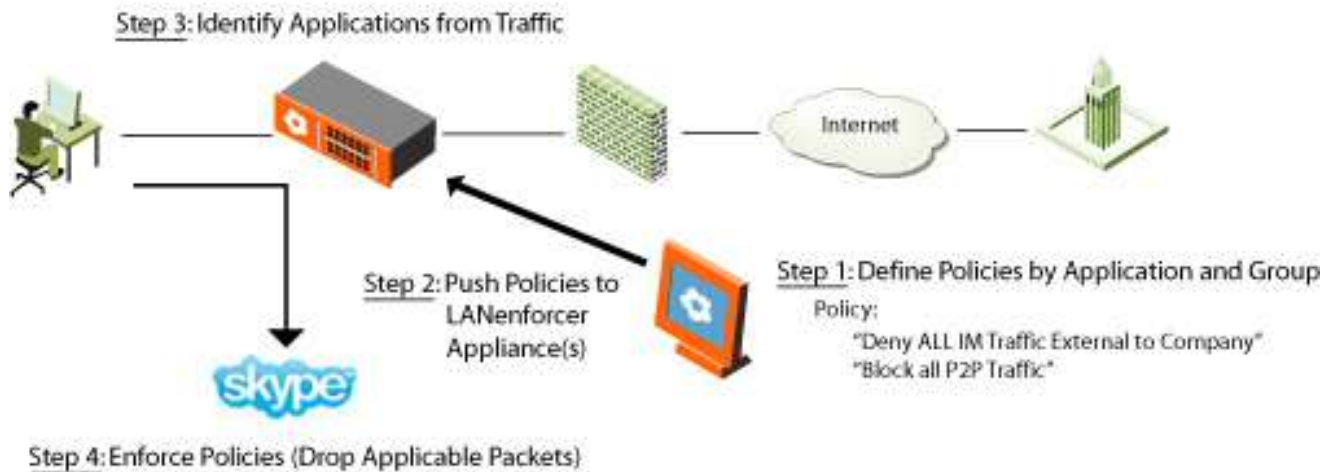


Application Use Controls

Peer-to-Peer (P2P) Applications



Instant Messaging (IM) Applications

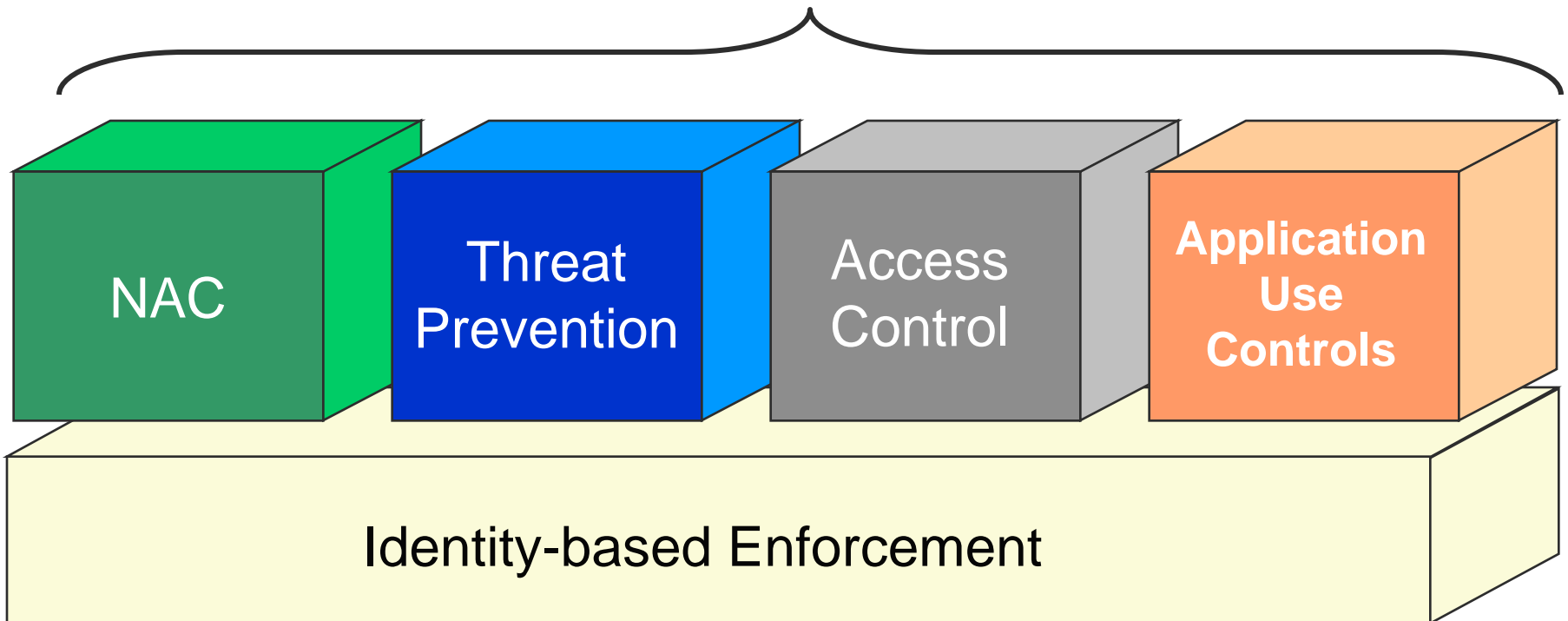


Appropriate use policies linked to user identity

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

