



Nevis
NETWORKS

NAC and Beyond: Securing the LAN



Excellence in
LAN Security



Excellence in
Identity Based
Access Control



Gartner

Cool Vendor, 2006



John Ginsberg
Sr. Systems Engineer
Nevis Networks
September 25, 2008



Best Deployment
Network Security
Solution



2008



Companies to
watch in 2006



2008 Finalist

What is “NAC”?

NAC = Network Access Control

- Resources and services can be accessed by only those users who have the right access privileges.



- The services that the network offers continue to stay up in presence of threats.



Botnets



**Trojans &
Rootkits**



**Worms &
Viruses**

Redefining NAC → LAN Security



“Done right, NAC enables pre- and post-admission compliance checks, which, effectively, stop the bad guys from getting on the network in the first place, as well as kicking off legitimate users if they don’t comply with company policy.” --Robert Whiteley, Forrester



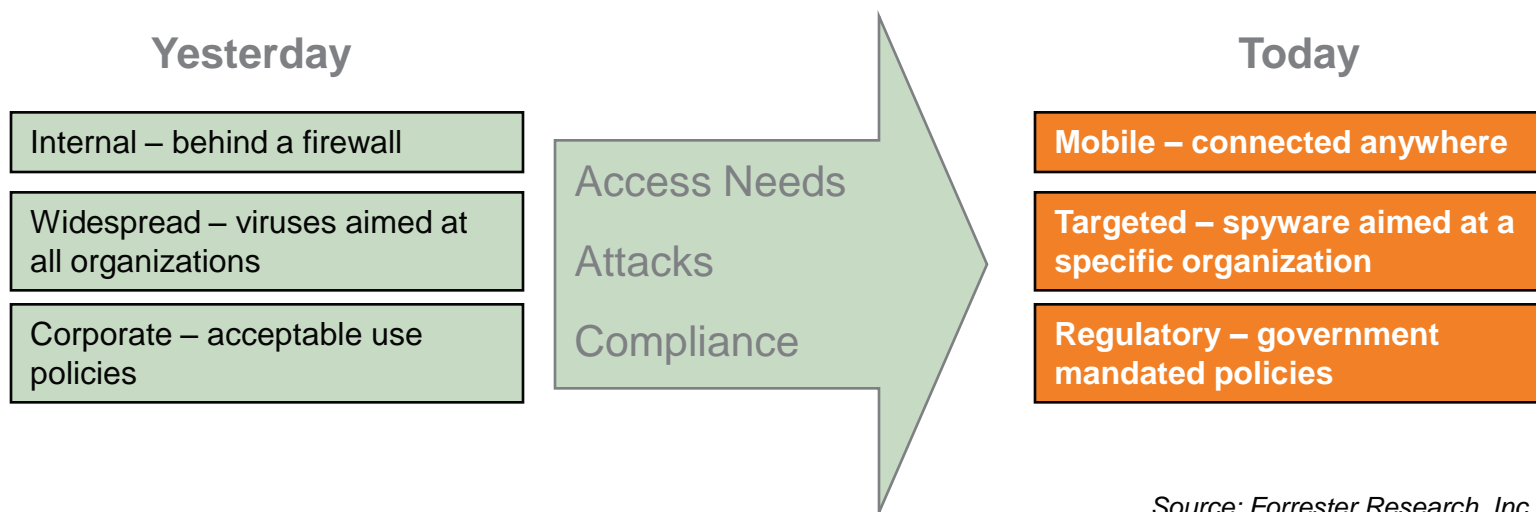
“Five technology functions accepted and expected as part of NAC:

- 1) Pre-connect host posture assessment
- 2) Host quarantine and remediation
- 3) Network access control based on user identity
- 4) Network resource control based on identity and policy
- 5) Post-connect - Ongoing threat analysis and containment”



--Joel Conover, Current Analysis

Changing Security Needs



Source: Forrester Research, Inc.

The Dissolving network perimeter

Pre-connect vs. Post-connect NAC



- Pre-connect:
 - Checks for endpoint “safety”:
 - Is anti-virus installed, running and up-to-date?
 - Is anti-spyware installed, running and up-to-date?
 - Is the OS patched?
 - Are required processes running?
 - Are banished processes not running?
 - Takes action based on the above results
 - Allows connection – user is prompted for authentication
 - Deny connection (drop or block)
 - Quarantine for remediation (isolate and redirect)
 - **Per-user vs. VLAN approaches**
- Post-connect:
 - Access control policy enforcement based on **identity** (AAA/LDAP) or profile (e.g. guest)
 - Continuous endpoint “safety” checks
 - Persistent user activity and security event monitoring to validate above
 - Identify active, real-time threats on the network (policy violations or exposure to malicious code)



Identity-Aware Networks



- Who's on your network?
- Where the going?
- What are they doing?
- Where they came from?
- Can you control their behavior?
- **Would you like to?**

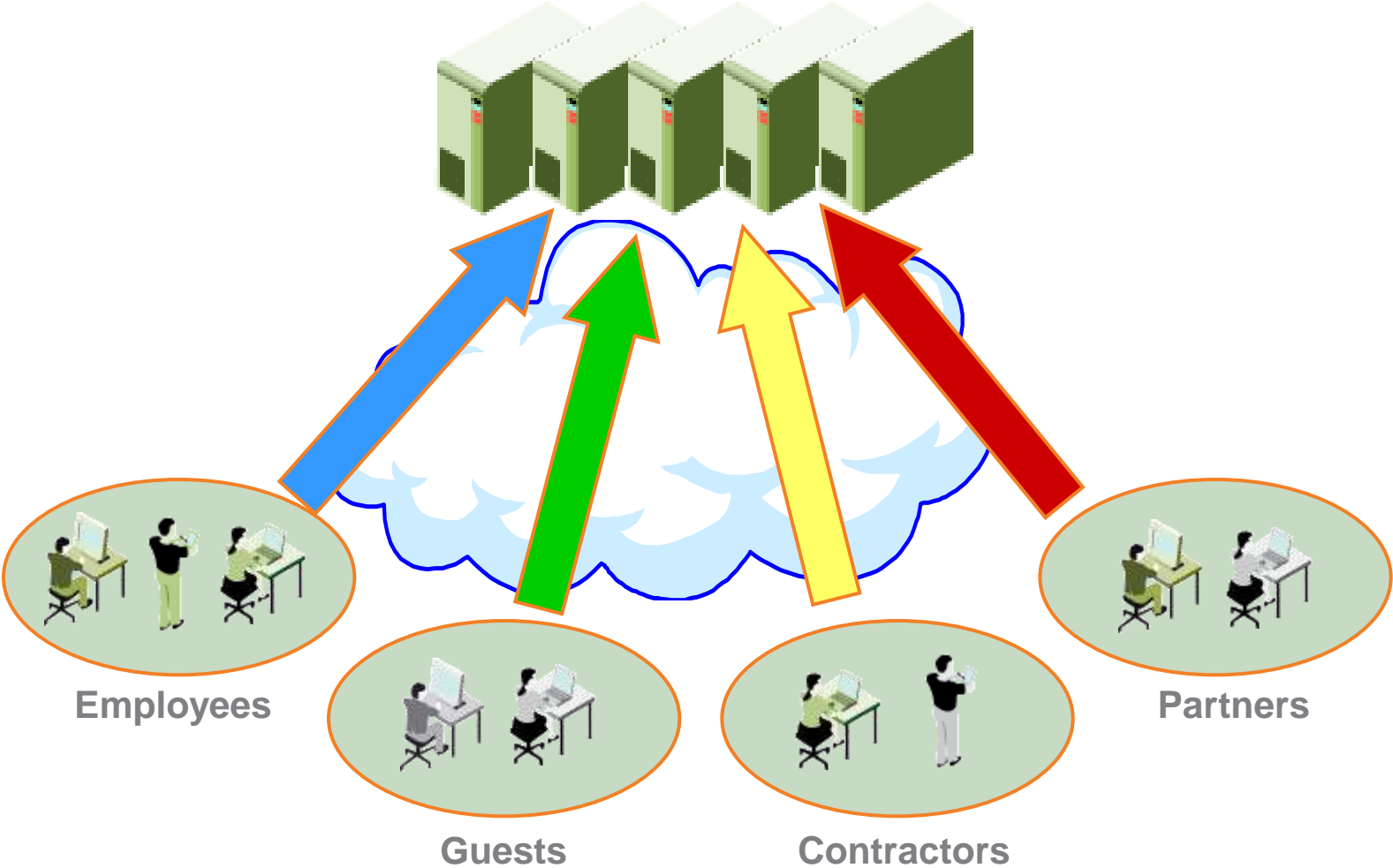
Who, What, Where & When?

Get Their User Names, Not Just Their Addresses

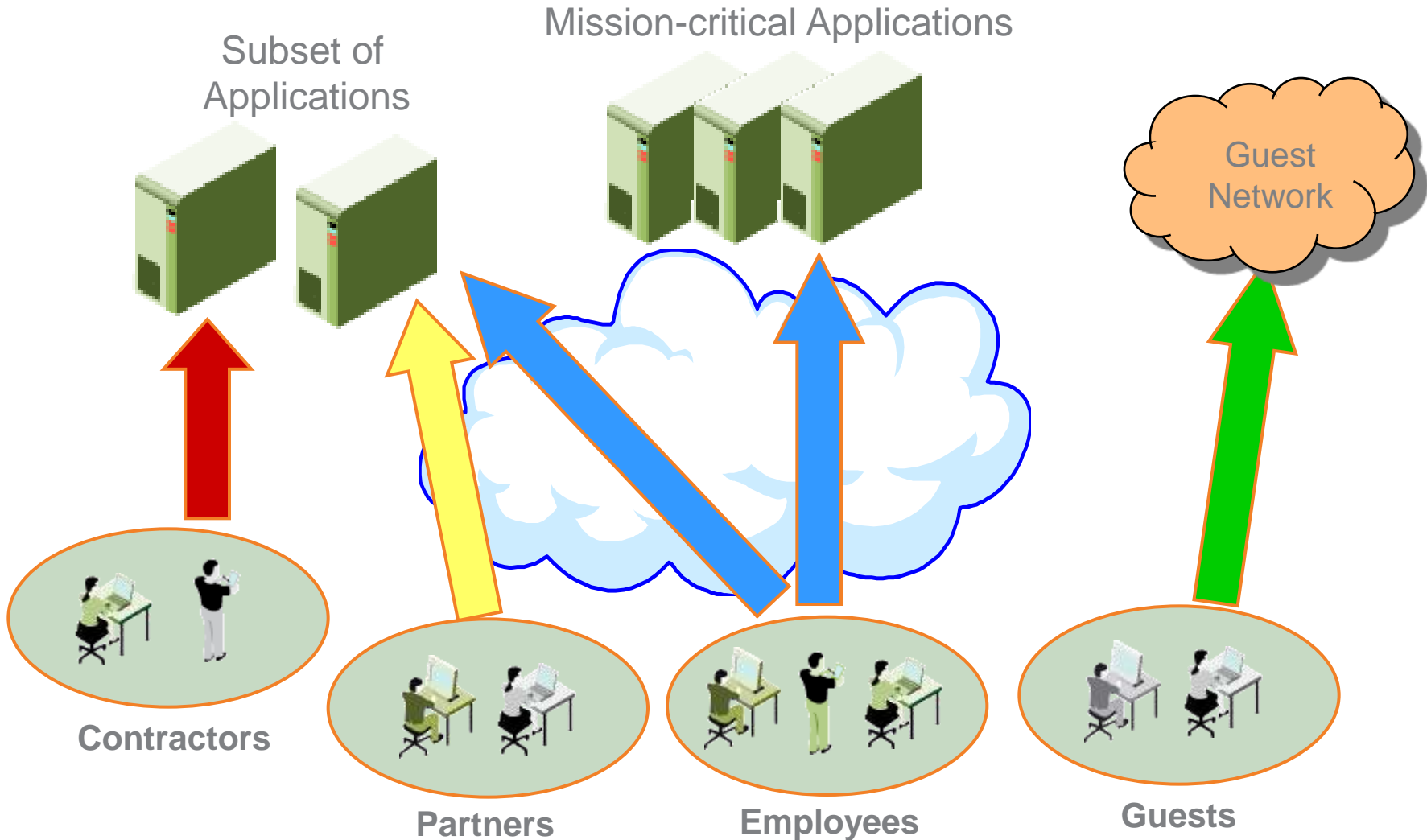
Enterprise Networks Are Anonymous



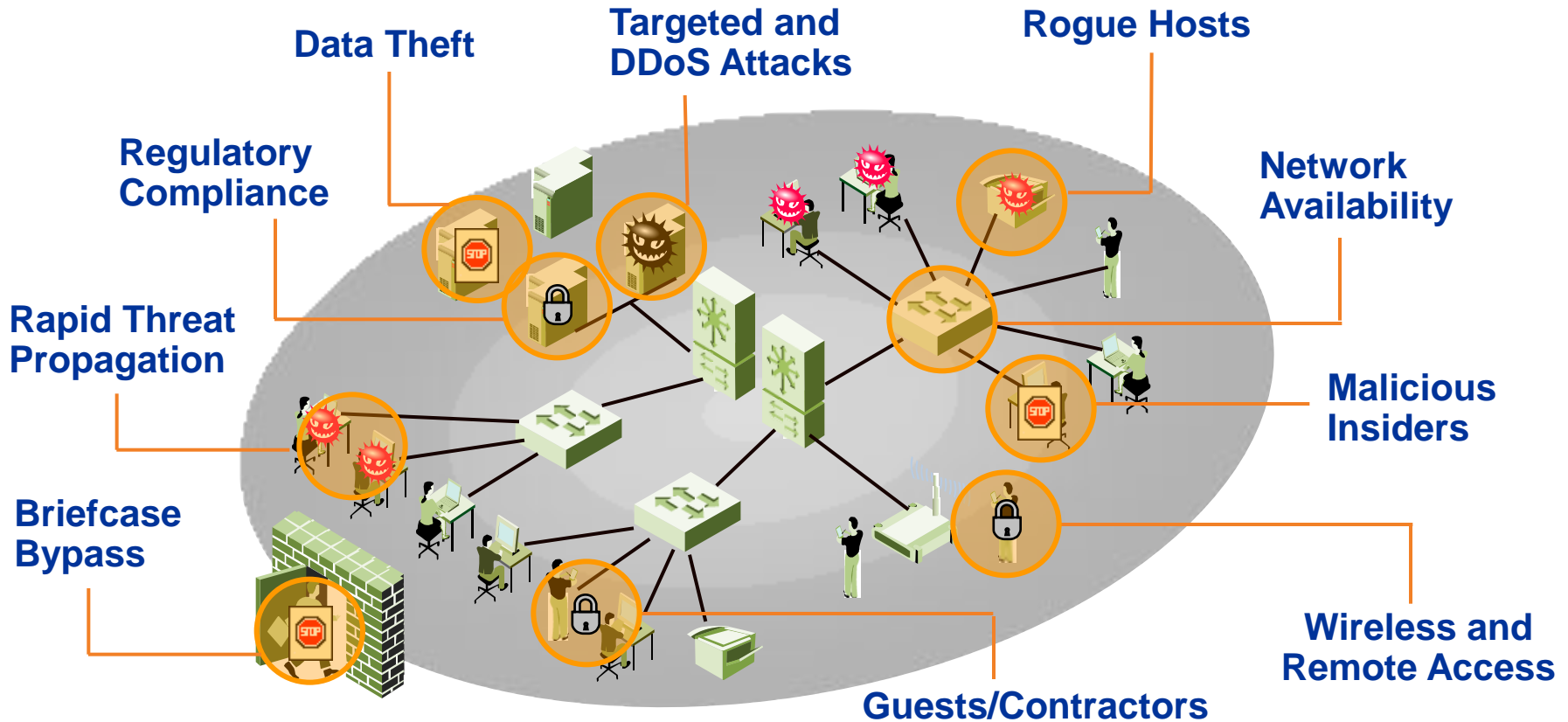
Mission-critical Applications and Servers



The Identity-Aware Network



LAN Security Is Required



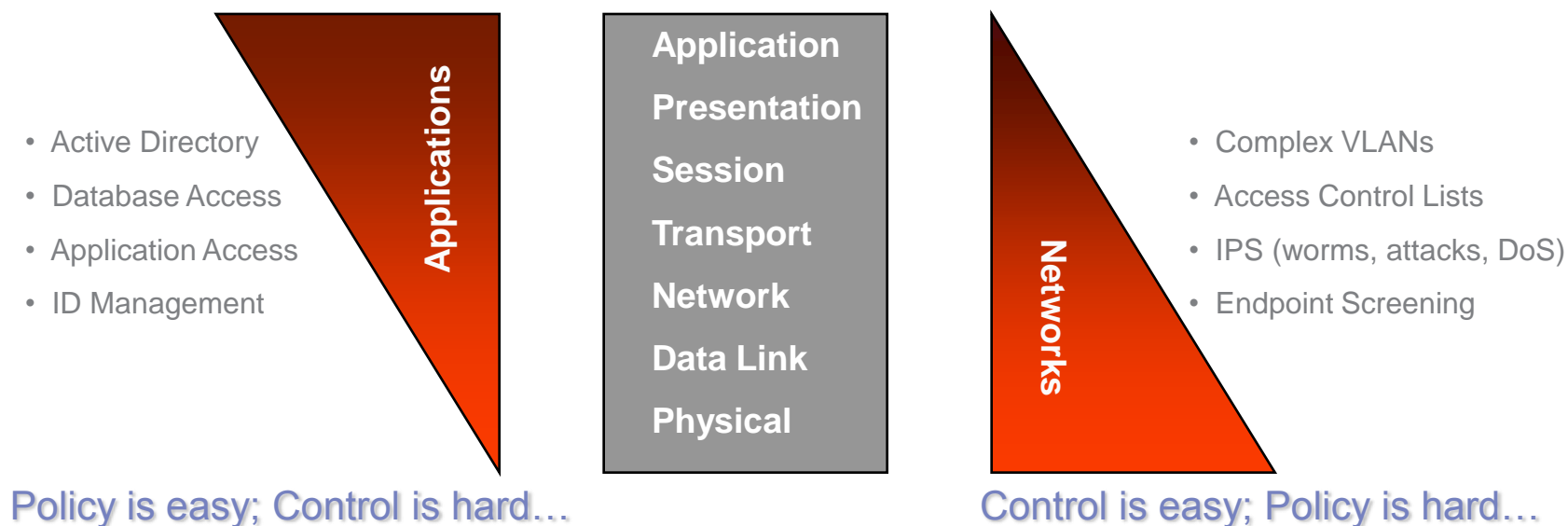
Business Has Changed The Way We Use The Network

The LAN Is The New DMZ

The Best of Both Worlds



Historically Different Approaches...



The Best of Both Worlds



Application Policy + Network Control Identity Driven LAN Security

- Active Directory
- Database Access
- Application Access
- ID Management

Applications

Application
Presentation
Session
Transport
Network
Data Link
Physical

- Complex VLANs
- Coarse ACL
- IPS (works, attacks, DoS)
- Endpoint Screening

Networks

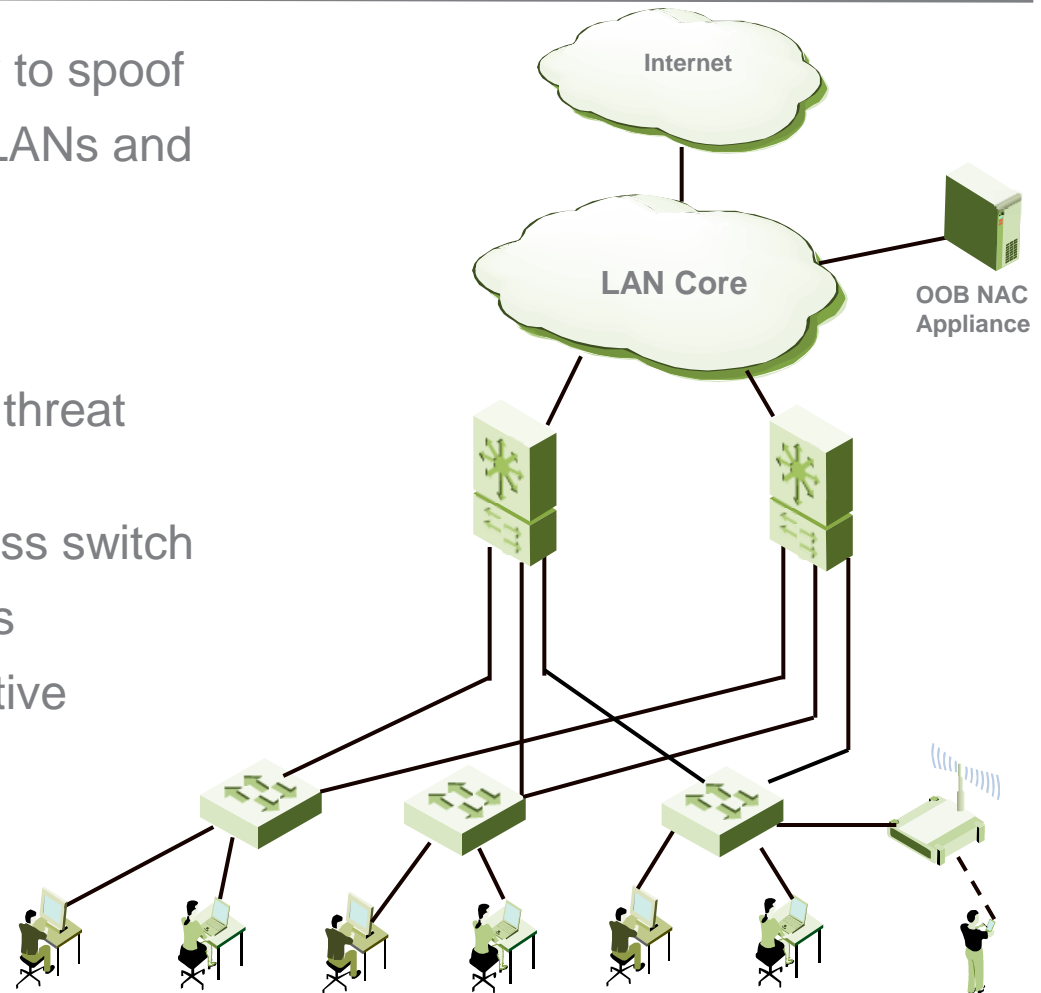
Policy is easy; Control is hard...

Control is easy; Policy is hard...

Out-of-Band Architecture: Appropriate for Pre-Connect, Monitor-Only

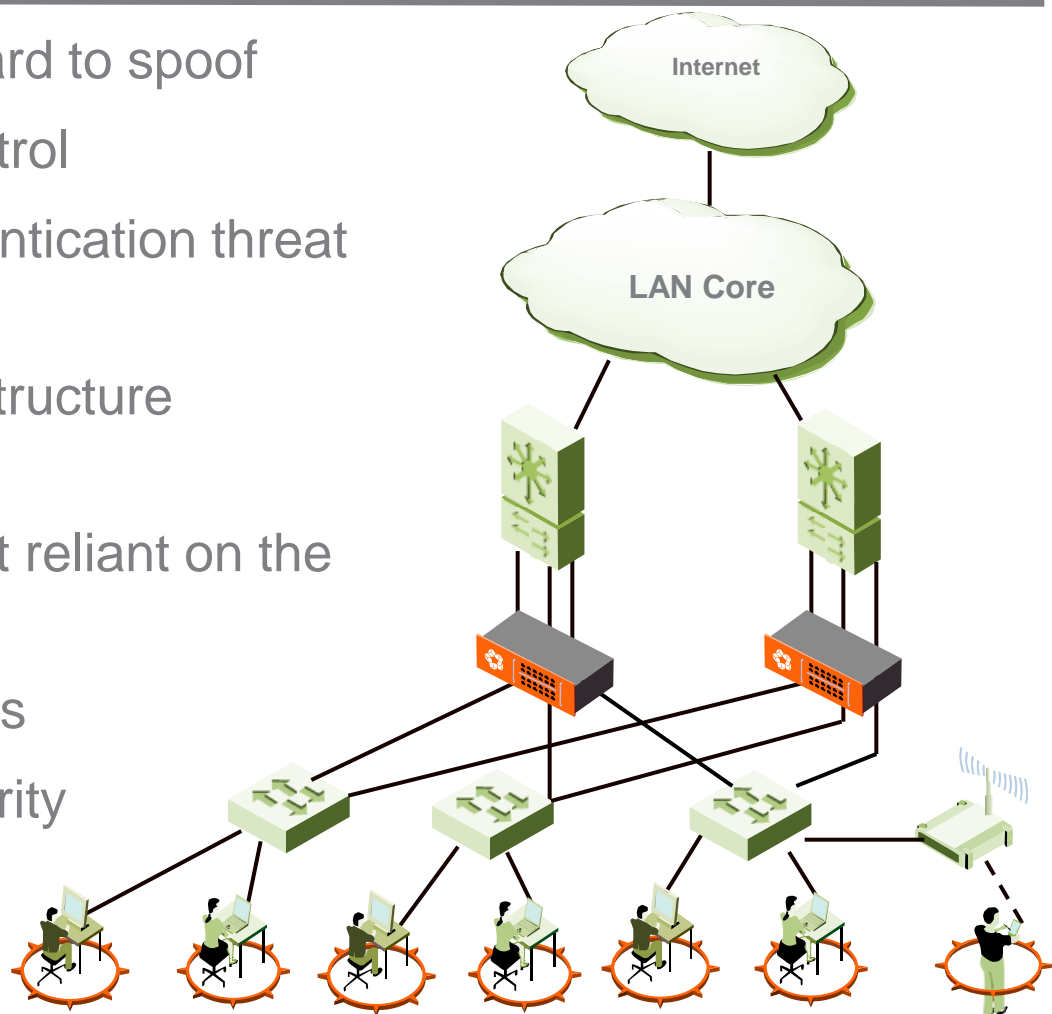


- Sits high in the network – easy to spoof
- Access Control depends on VLANs and ACLs
 - Lacks user awareness
 - Not scalable
- Little or no post authentication threat detection
- Enforcement depends on access switch
- No application layer awareness
- Monitor-only rather than proactive enforcement and protection



Inline Architecture: Designed for Pre- and Post-Connect NAC

- Sits close to the threat – hard to spoof
- Identity-based Access Control
- Comprehensive post authentication threat detection
- Protects the network infrastructure (e.g. DoS protection)
- Immediate quarantine – not reliant on the switch
- Application layer awareness
- Purpose built for LAN security



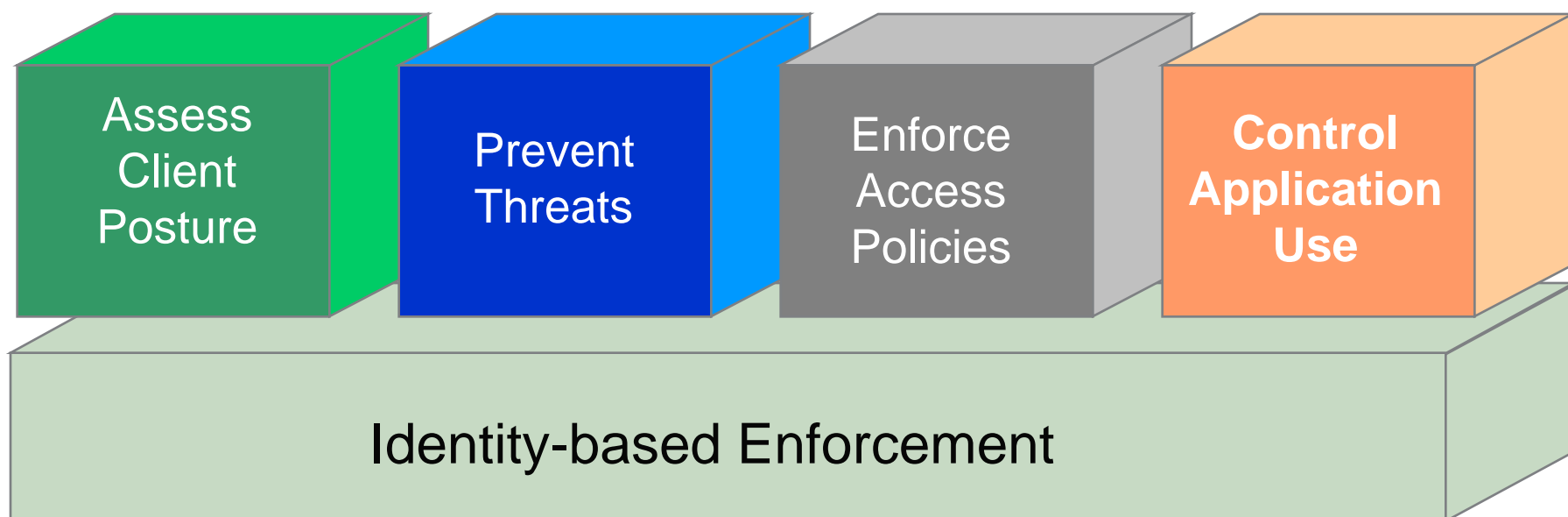
Inline Architecture: Operational Considerations



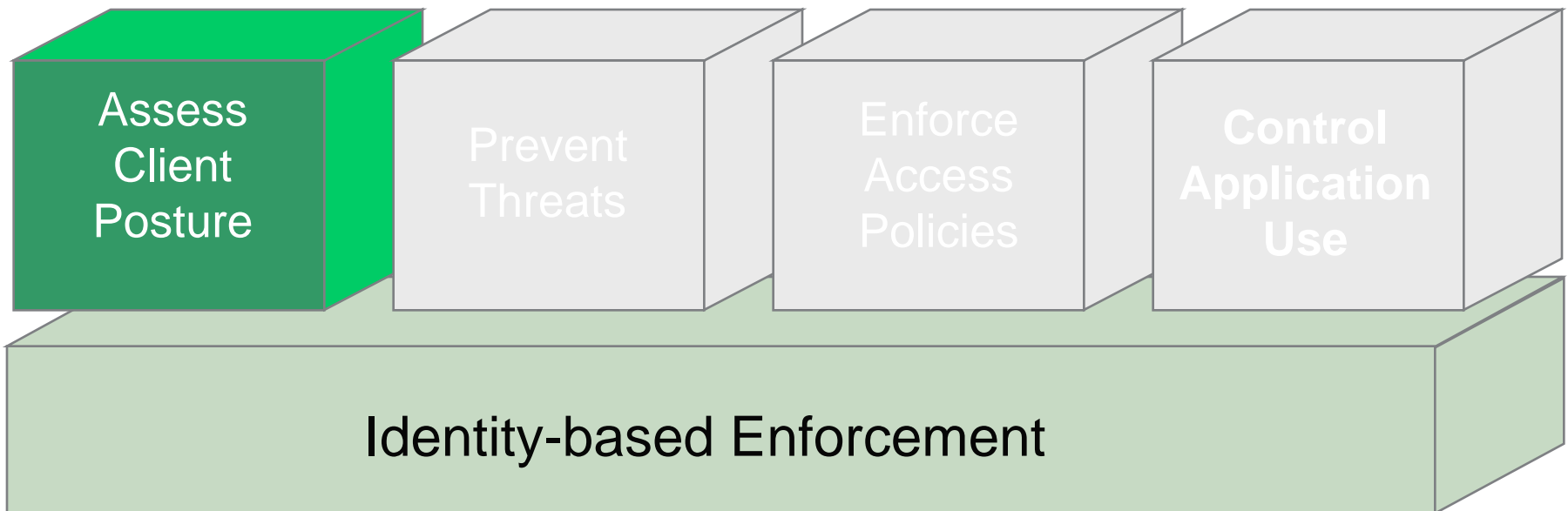
- Redundancy: Fail over, Fail open, Fail through
- In-depth security functionality incurs performance requirements
 - Highly scalable, massively parallel computing resources
 - Can't be done with standard PC processor architecture
 - Latency is not tolerated in the LAN
- Integrated policy decision and enforcement
 - Single place for troubleshooting
 - No reliance upon or bias for third party switching technologies
- Support for existing VLAN architecture
 - No redesign required
 - If problem with appliance – simply unplug and bypass

More appropriate for enterprises that require comprehensive security controls and continuous access control policy enforcement.

An Integrated Policy Approach



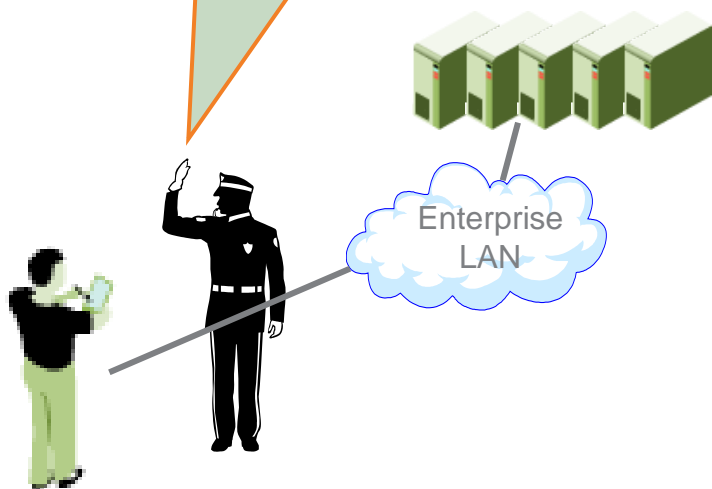
Client Posture Assessment



Network Admission Control

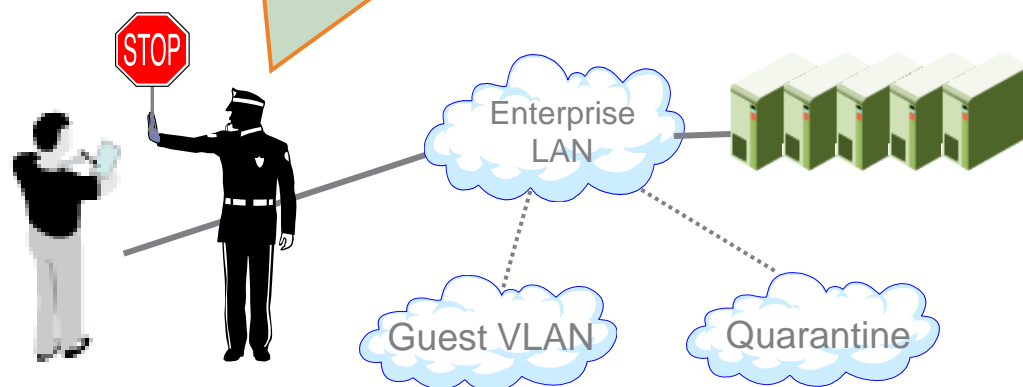
Without NAC

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

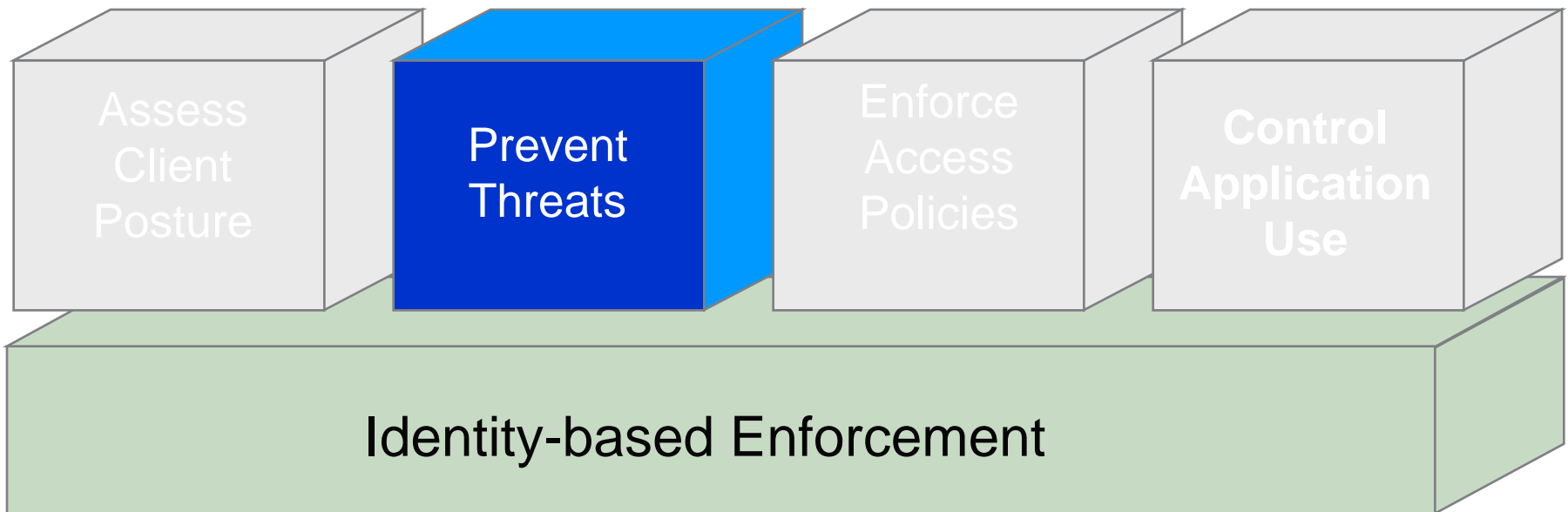


With NAC

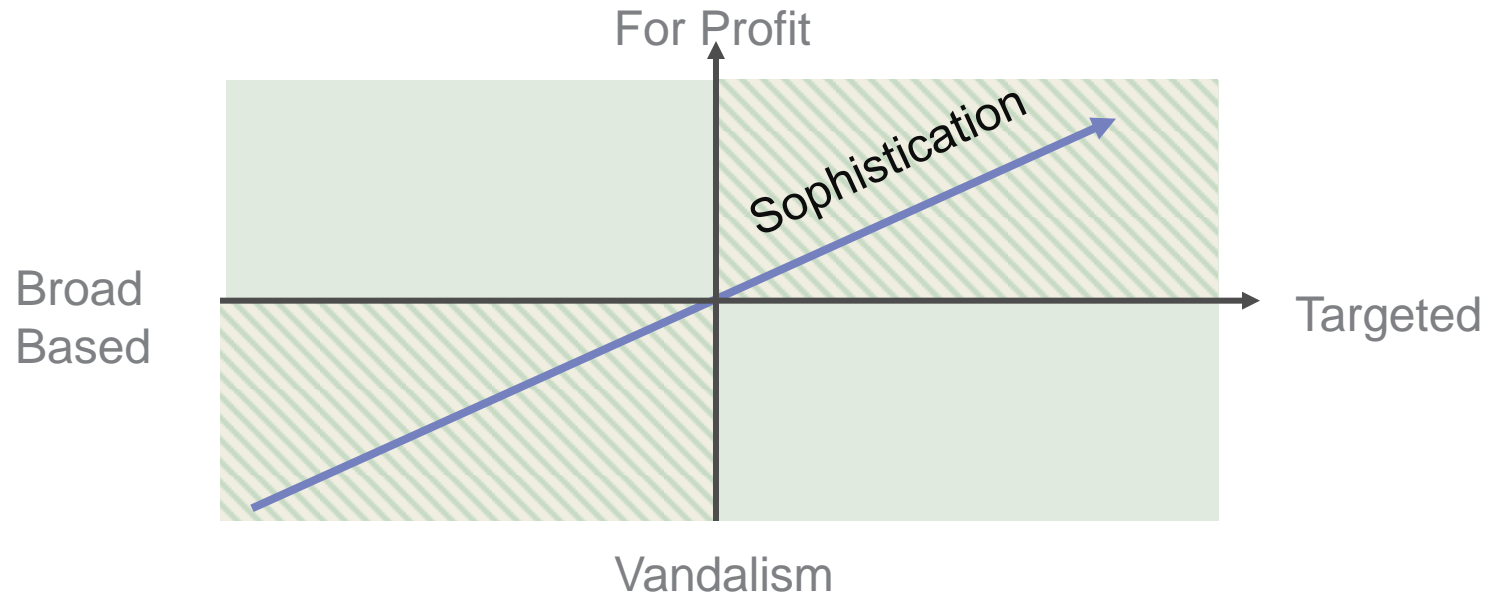
1. Who are you? Are you in our directory?
2. Are you running current anti-virus, anti-spyware?
3. What OS? Is it patched?
4. Are you running all required processes?
5. Are you not running any banned processes?



Threat Prevention



Enterprise Malware Trends



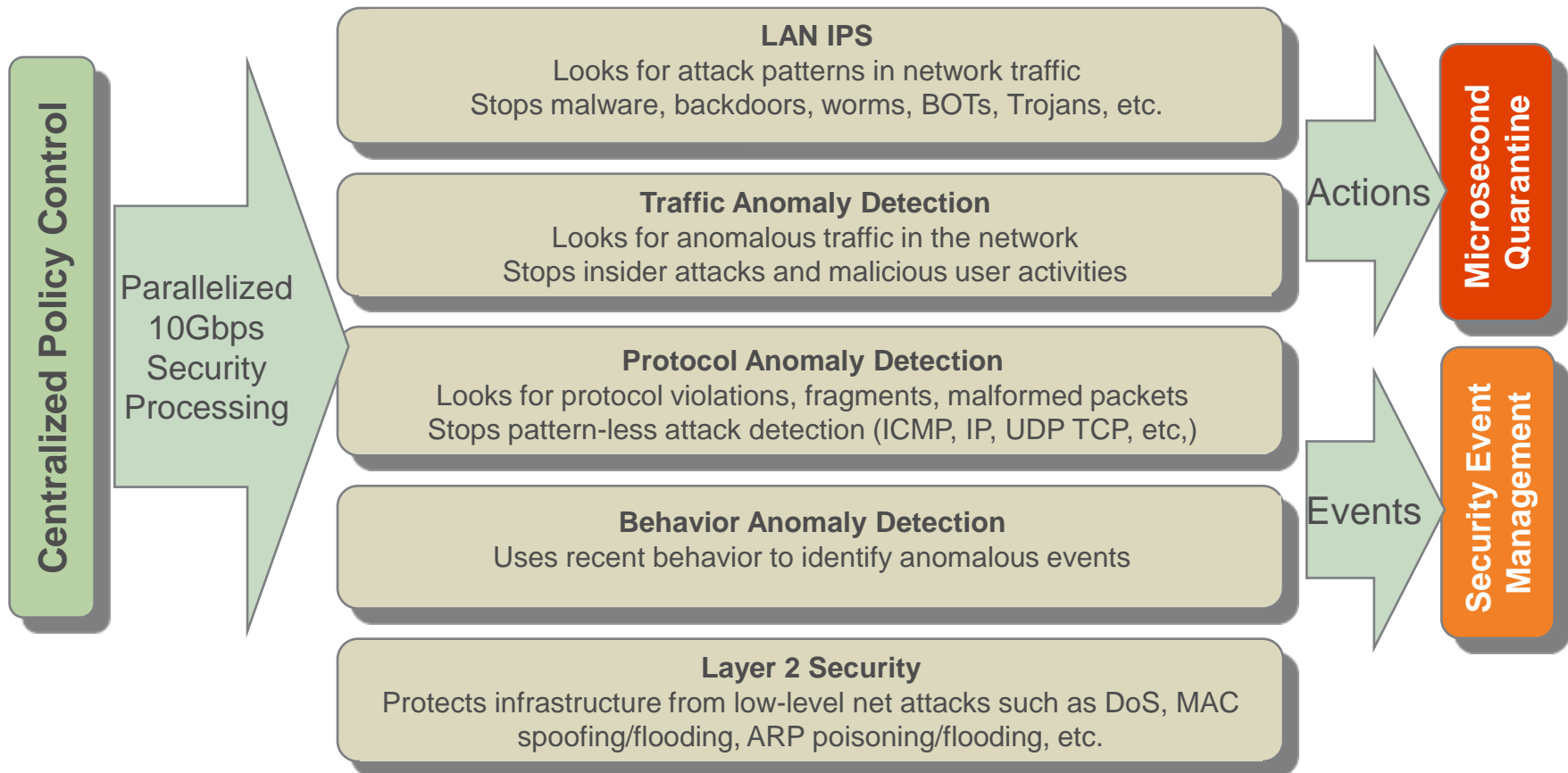
By year-end 75% of enterprises "will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses"

Source: Gartner Group

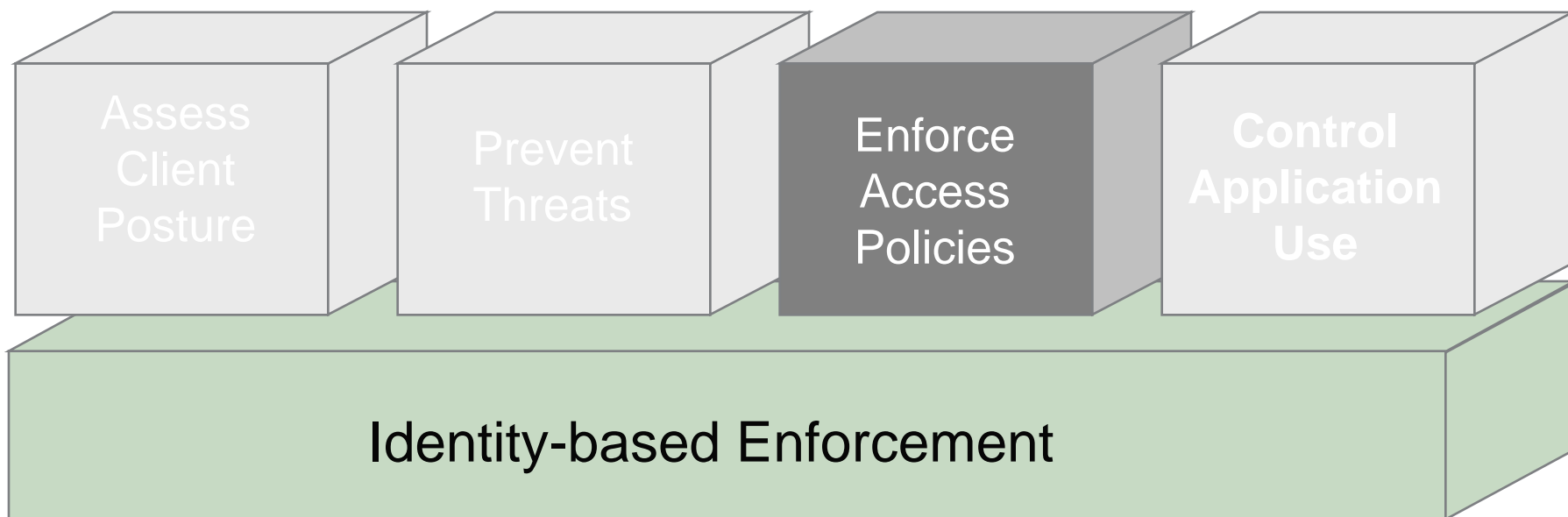
Of 4.5 million URLs analyzed, 450,000 - one in 10 - were "successfully launching drive-by-downloads of malware binaries."

Source: Google Research

Integrated Threat Containment

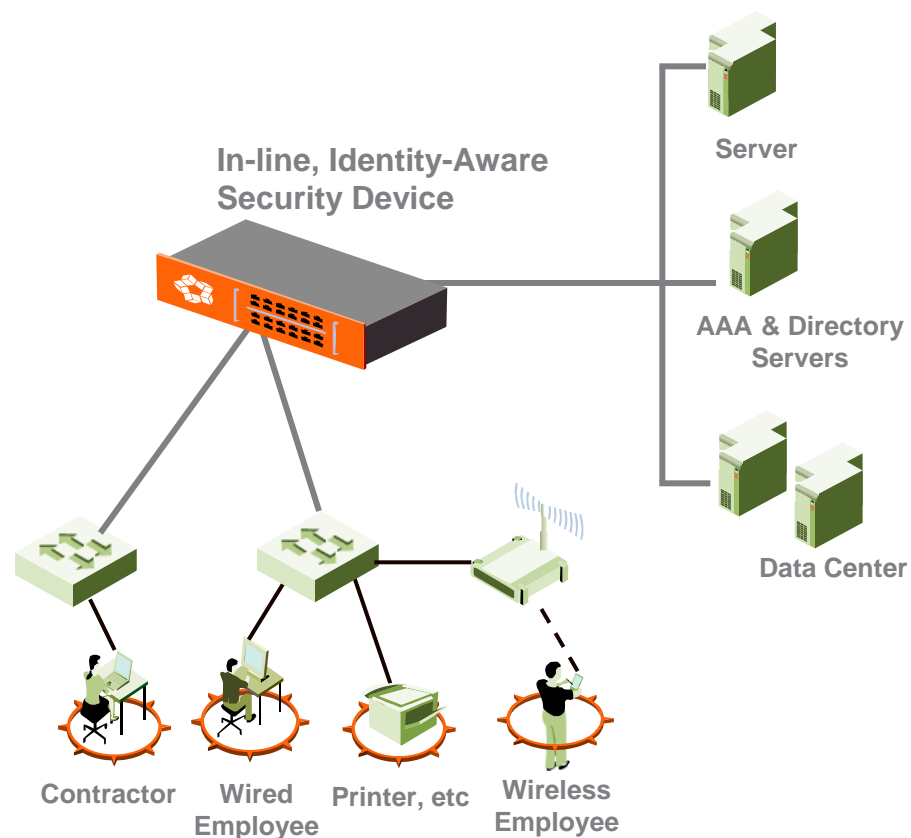


Identity Based Access Control

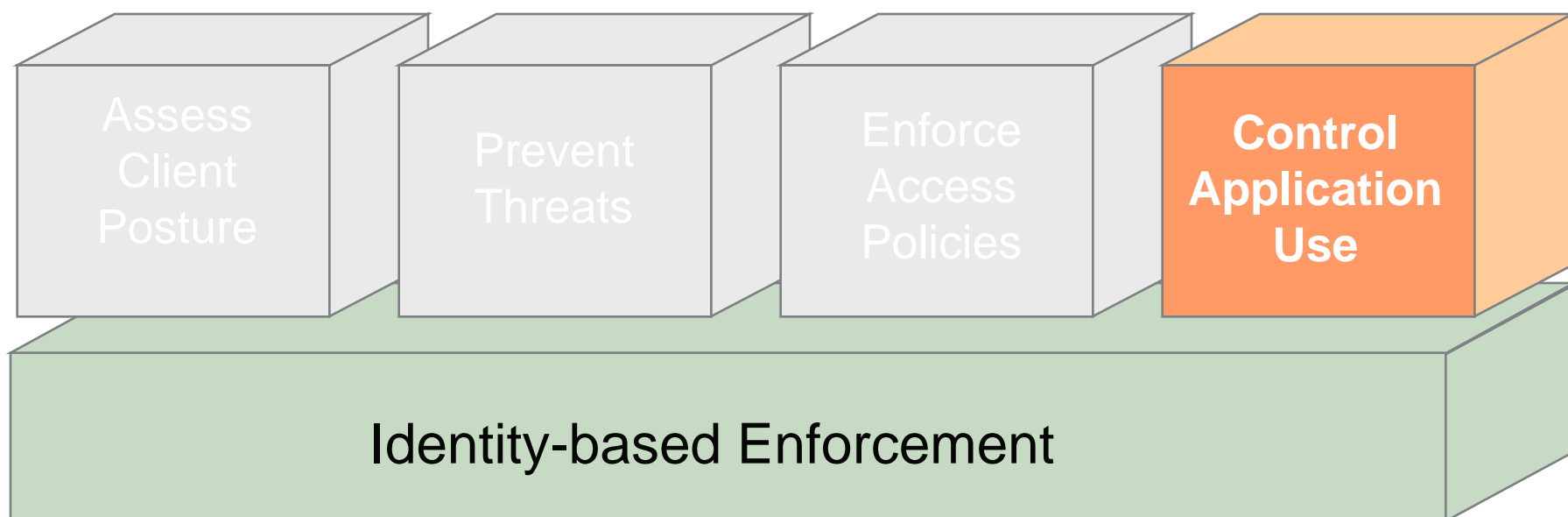


Identity-Based Access Control

- Associates each network session with a specific user ID
- Employs role-based access policies based on AAA groups
- 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

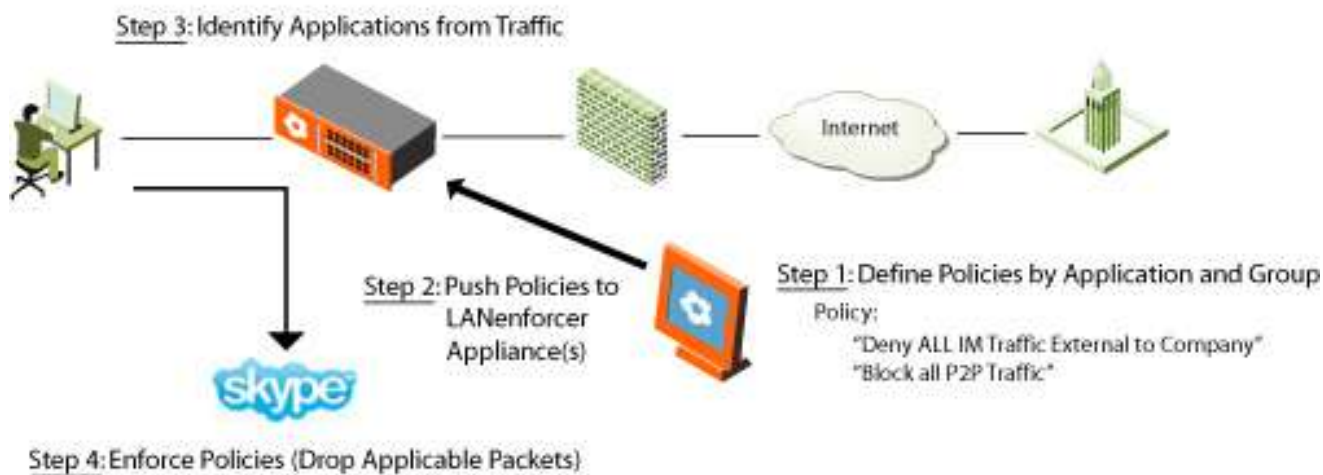


Application Use Controls

Peer-to-Peer (P2P) Applications



Instant Messaging (IM) Applications

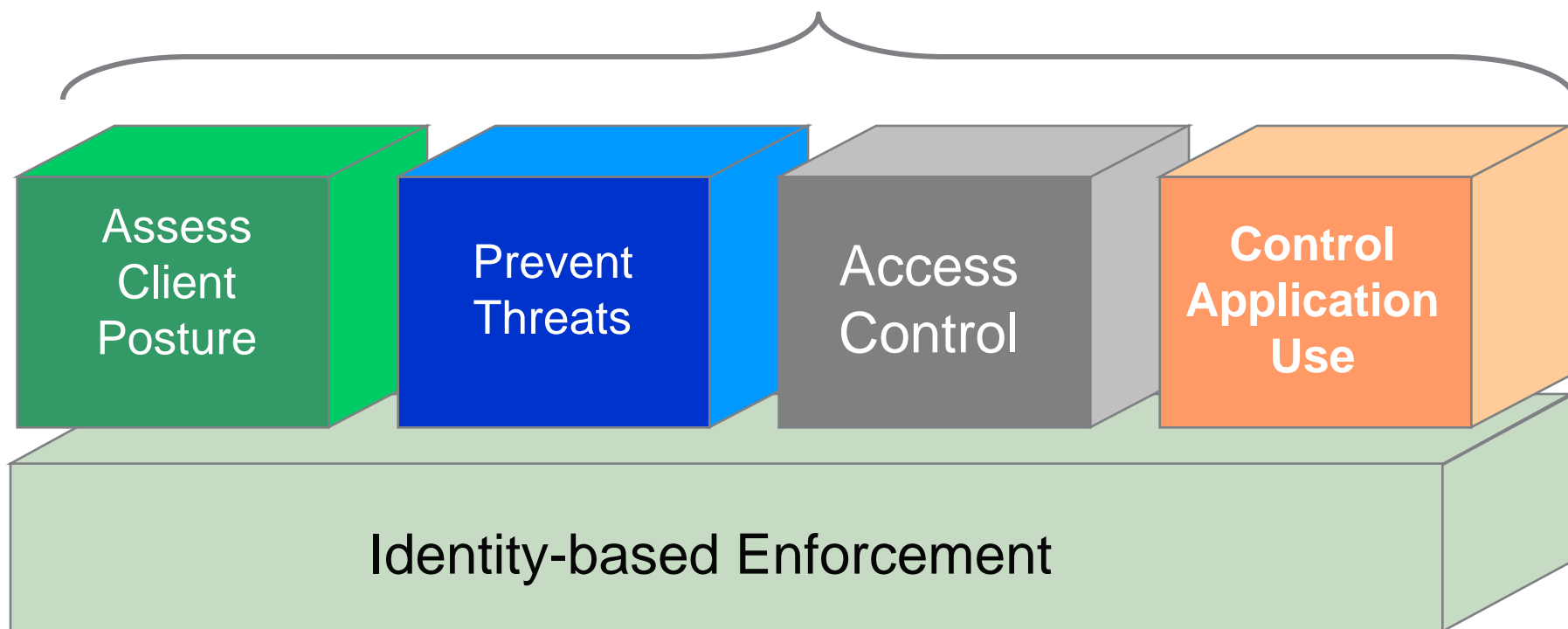


Appropriate use policies linked to user identity

LAN Security Done Right



Identity-driven LAN Security



Implementing Identity-driven LAN Security



- Key Considerations:

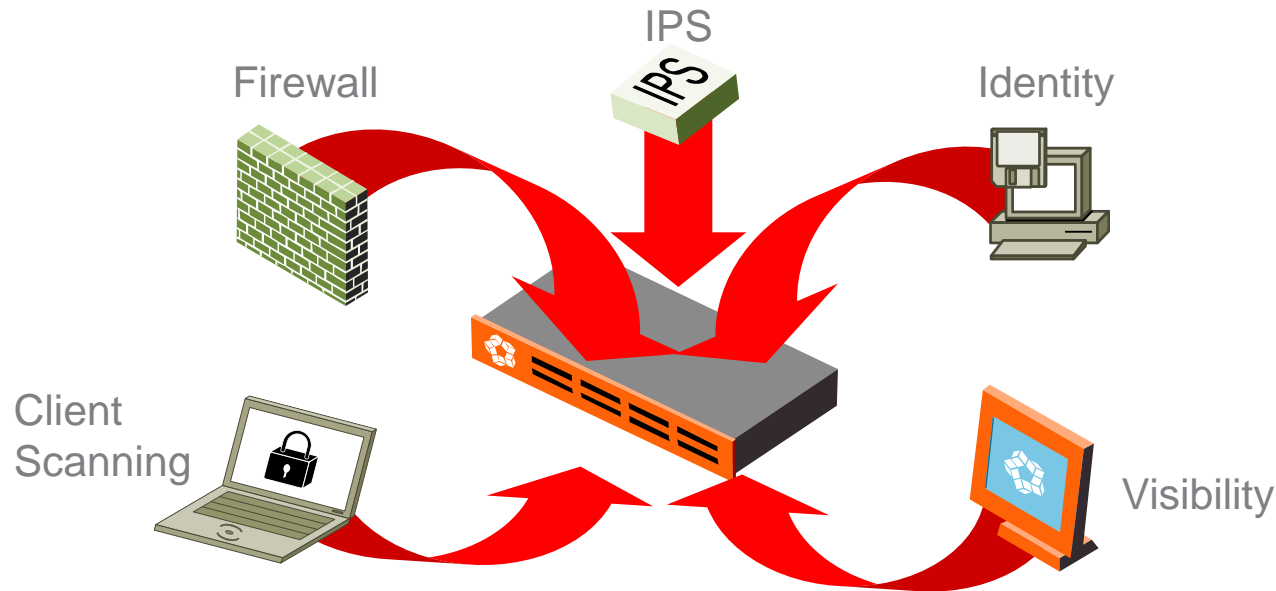
- Define primary and secondary goals
 - Securing guest access?
 - Checking endpoint compliance?
 - Enforcing employee access policies?
 - Monitoring user activity?
- Cost and complexity of initial deployment and maintenance overtime
- Redundancy requirements
- Impact on end-users – level of transparency
- Scalability and growth plan
- Phased implementation is recommended

- Architectural options:

- Agent-based
- Agent-less
- Inline appliances
- Out-of-band appliances
- Secure Switches



Nevis: Secure, Fast, Comprehensive



- ✓ Pre and Post Connect Security
- ✓ Deterministic Performance
- ✓ Transparent to Users
- ✓ Drops malicious packets
- ✓ Nevis Labs research service
- ✓ Existing Policy Store Integration
- ✓ Easily Deployed
- ✓ Application Intelligence

The Nevis Product Line



- LANenforcer 1048
Secure LAN Switch
- LANenforcer 2024
LANenforcer 2124
LAN Security Appliance
- LANSight
Management Appliance



Thank You!



NEVIS NETWORKS

John Ginsberg
Sr. Security Engineer
(212) 865-0813
jginsberg@nevisnetworks.com