



Phased Deployment of Network Access Control (NAC)

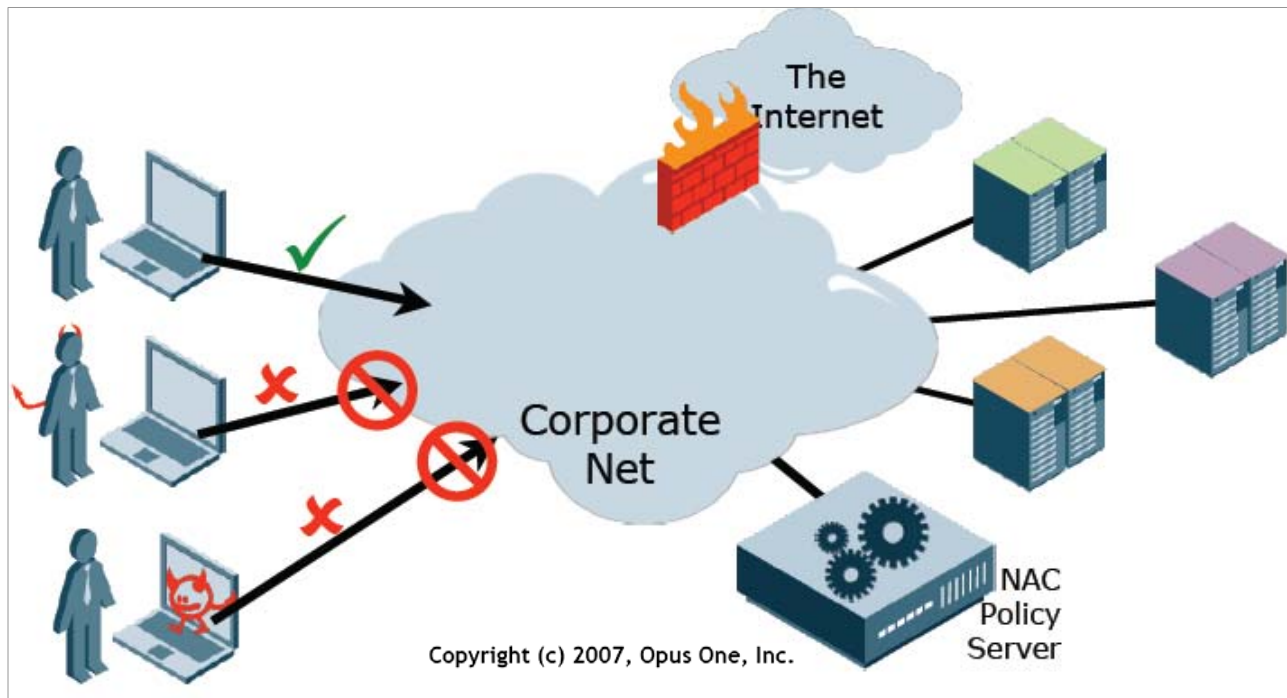
● Agenda

- What Is NAC?
- Phased Deployment Approaches
- Best Practices
- About Bradford Networks

● What is Network Access Control (NAC)?

What you can do on a network is a function of:

- Who you are
- What you're connecting with
- When, where and how you're connecting



● Real Problems that NAC Solves

Visibility

“I have thousands of employees accessing data from more than 40 locations. How do I keep track of them?”

Policy

“I need to provide varying levels of data access to different users based on title, role, location, and task.”



Security

“Worms and viruses have taken down a number of banking systems and compromised customer data. How do I ensure that every device accessing my network has the latest anti-virus, anti-spyware and security patches installed?”

Reporting

“Regulations require I audit and log network access and we do everything manually. How do I meet my reporting requirements?”

● What NAC Does

- Identifies users/devices accessing network
- Assesses security posture of devices
- Allows authorized users and devices on
- Blocks unauthorized users/devices
- Logs all activity for reporting / compliance
- Automates the entire process

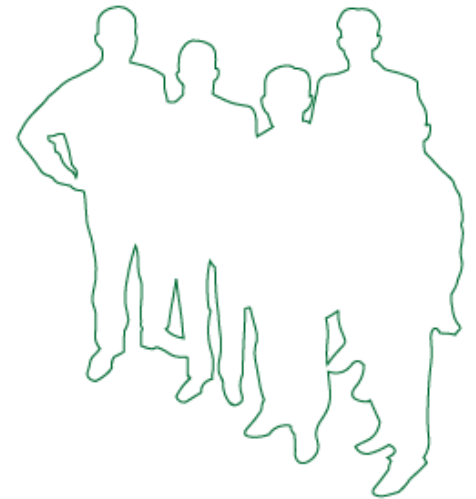
• What NAC Does

• Assess Identity

- Authenticate users (e.g., Username/Password)
- Authenticate host devices (e.g., MAC Address)
- Group users/devices by role

Goal

Tie access privileges to user-centric criteria so policies can “follow” users anywhere on the network



• What NAC Does

• Ensure Compliance

- Assess host devices for required or prohibited software
- Verify that only acceptable / approved applications are installed on host devices

Goal

Ensure host devices are “safe” and “clean” with only approved applications installed and running



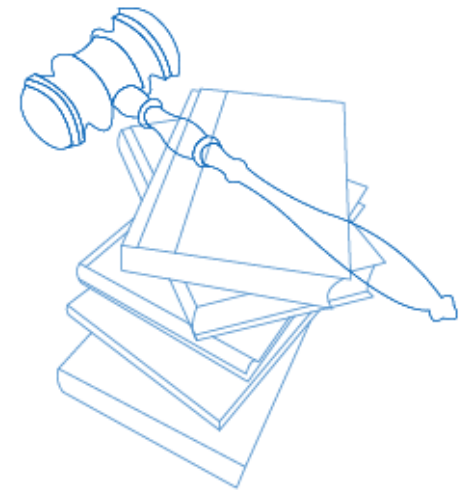
• What NAC Does

• Enforce Policy

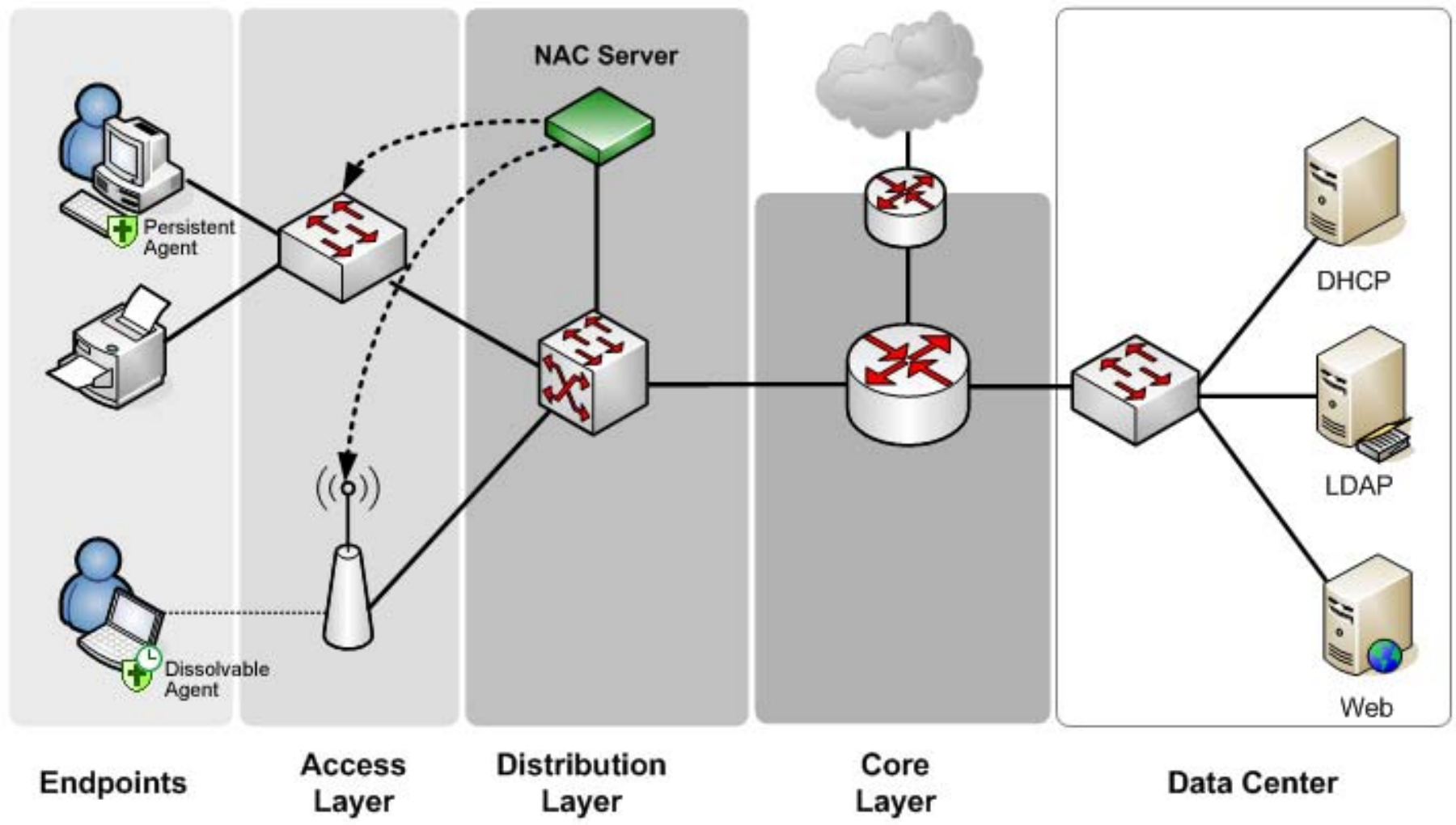
- Use identity and compliance data to control access
- Provide assisted or automated *remediation* services
- Control access before and after users log on

Goal

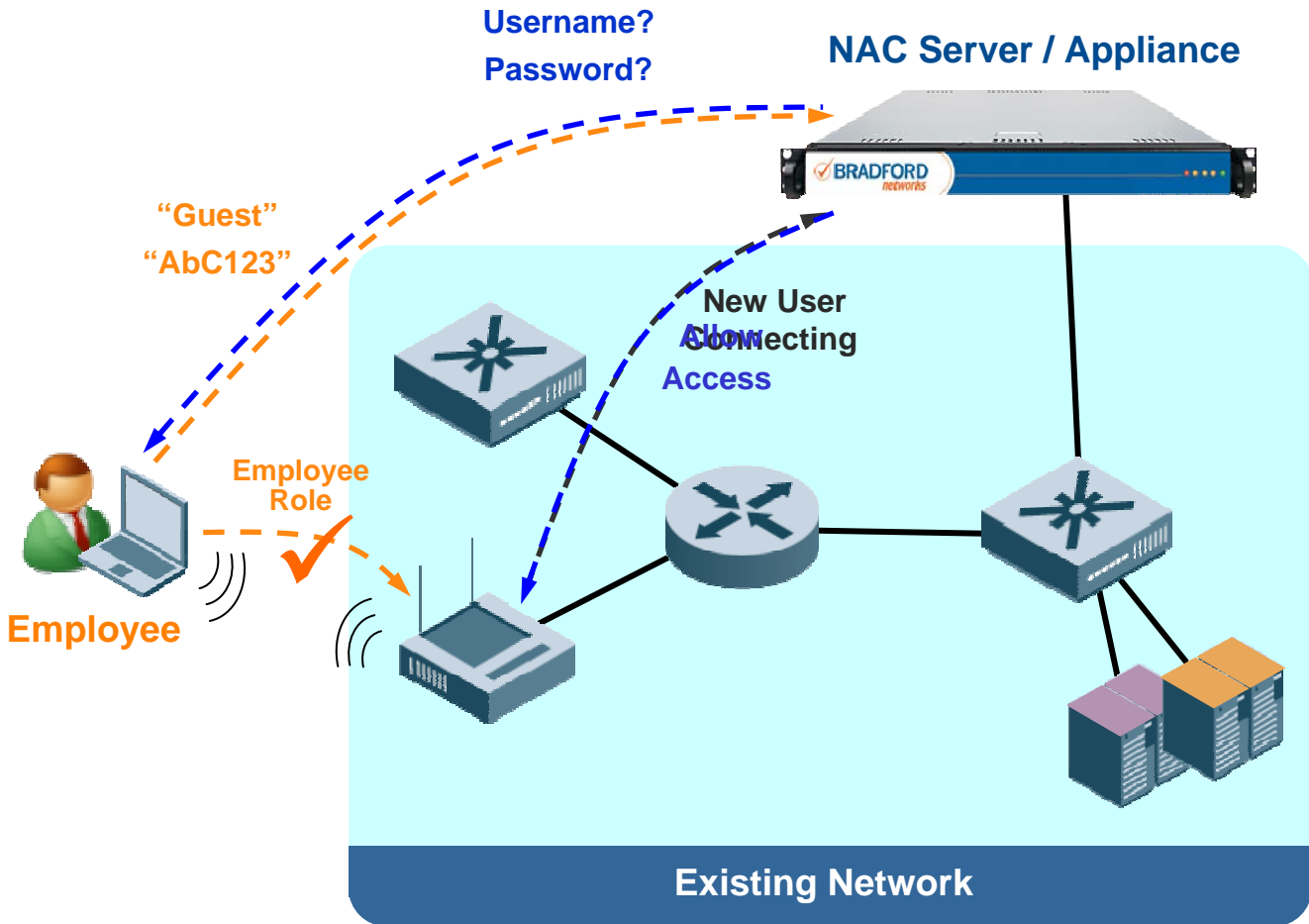
Automate access control to allow appropriate access by authorized users and compliant devices



● Elements of NAC Solutions



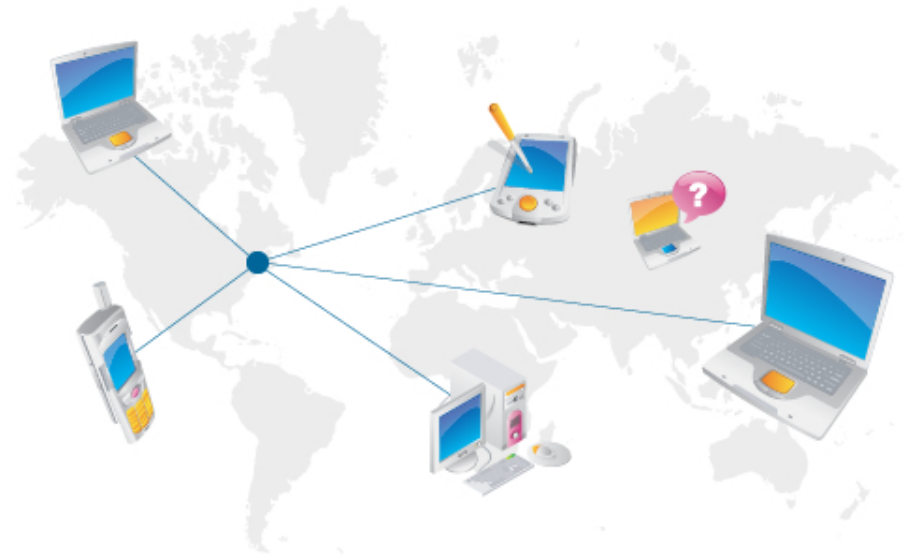
• How NAC Works: Authorized User



1. User connects
2. Login required
3. Laptop scanned
4. Check policies
5. Allow access
6. Activity logged

● Everyday IT Needs that NAC Addresses

- Register all devices
- Authenticate users
- Ensure endpoint devices are “clean” and “safe”
- Quickly identify and deal with policy violations
- Provide easy guest access
- Find and control users
- Secure wireless access
- Control bandwidth use
- Locate stolen computers
- Identify rogue servers
- Track and document activity on the network



• NAC Benefits

BUSINESS

- Security
- Productivity
- Regulatory Compliance
- Investment Protection

TECHNICAL / IT

- Visibility
- Control
- Easy of Use
- Flexibility / Scalability

● Business Considerations

- What problems will be addressed with NAC?
 - *What is the most immediate need?*
- Acceptable Use Policy
 - *Does the organization have one?*
- What are organizational / political implications?
- What level of financial investment is feasible?
- What is the timeframe for deployment?
- What are the expected benefits / ROI?
 - *How will benefits / ROI be measured?*

● Technical Considerations

- How can the existing infrastructure be leveraged?
- What authentication methods will be used?
- What is acceptable security posture for devices?
- What enforcement methods will be used?
- How will non-compliant users/devices be handled?
- What remediation methods will be used?
- How will NAC be rolled out?

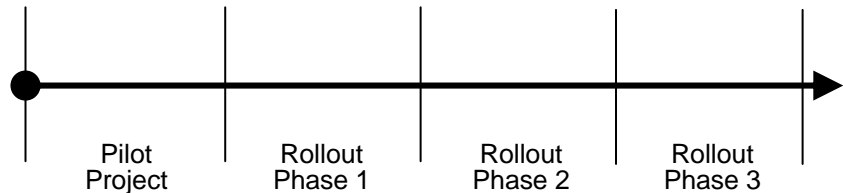
● NAC Deployment



- “All In” Approach
 - NOT recommended!

- Phased Approach
 - MUCH greater success

	11.03	12.03	1.04	2.04	3.04	4.04	5.04	6.04
Preparation and Planning								
Develop project proposal	■							
Approve project proposal		◆						
Recruit project team		■						
Development and Test								
Specify detail requirements			■					
Develop prototype			■	■				
Approve prototype				◆				
Develop beta version				■	■			
Test beta version					■	■		
Apply final corrections						■		
Approve final version							◆	
Implementation								
Train users						■	■	
Roll-out final version								◆



● Phased Deployment Approaches

- **“Monitor-Only” Mode**

- Identify/Authenticate users and devices
- Assess security posture of host device
- Monitor network access and log all activity
- No Enforcement
 - *Enforce access policies in later phases*

- **“Pilot Project”**

- Start Small, then expand in later phases
 - Building #1, Building #2, etc.
 - Department #1, Department #2, etc.
 - User Group #1, User Group #2, etc.

- **“Point Solutions” – Subsets of NAC**

Full Featured NAC Solution

User/Device Identity + Role-based Access
Endpoint Compliance/Posture Validation
Usage Policy Enforcement (Behavior-Based)

Guest and Contractors
Secure Access for
Unmanaged Users/Devices

What’s on the network
Device Identity / Profiling
Role-based Access

Who’s on the network
User Identity
Role-based Access

Behavior on the network
Behavior/Traffic Monitoring
Policy Enforcement

● Guest/Contractor Scenario

Organization: Financial Services Firm

Problem: Need to allow network access for visiting users, business partners, and contractors working on-site without sacrificing network security

Goal: Identify and control guest and contractor users (and other visitors)

• User Visibility Scenario

Organization: Manufacturing Company

Problem: Need to automatically identify and track shift workers connecting to network using shared-access PC's and give role-based network access

Goal: Identify and control all users

● Device Profile Scenario

Organization: Healthcare Services / Hospital

Problem: Need a way to automatically identify devices connecting to the network and set appropriate network access based on the type of device

Goal: Identify and control all devices

● Behavior Monitoring Scenario

Organization: College / University

Problem: Existing devices such as IDS/IPS identify threats / vulnerabilities on the network, but...

Need a way to automatically stop threatening / inappropriate behavior at the point of access to the network

Goal: Control behavior at point of access

● Best Practices Summary

- Plan, Plan, Plan
 - Define clear goals/objectives and metrics for success
- Engage all stakeholders early and often
- Address the most critical business problem(s) first
- Apply deployment strategy that fits best
 - “Monitor-Only” – no policy enforcement
 - “Pilot Project” – start small, then expand
 - “Point Solution” – subset of full NAC
- Choose NAC solution for short and long term needs

• **Bradford Networks At-A-Glance**

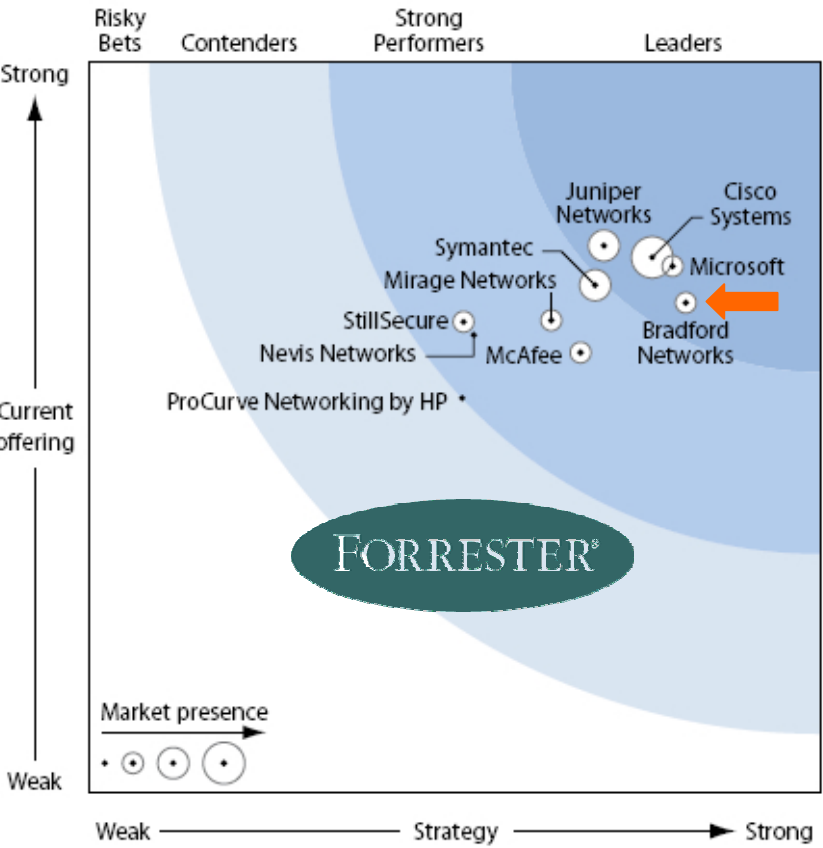
- **Founded in 1999**
- **Headquartered in Concord, NH USA**
- **Focus On Secure Network Access Control Solutions**
- **Shipping Products Since 2002**
- **Over 500 Customers Worldwide Today**
- **Over 1 Million Network Users Secured**
- **Venture-Backed to Accelerate Growth**
- **Record Growth in Last Two Fiscal Years**
- **Customer-Focused**
- **Broad Industry Recognition**

Awards and Recognition

- Innovation
- Strategy and Vision
- Technology Leadership
- Customer Satisfaction



2008 NAC Studies: Forrester and Gartner



Gartner	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
3Com (TippingPoint)			X		
Aruba Networks			X		
Bradford Networks				X	
Check Point Software Technologies			X		
Cisco				X	
ConSentry Networks				X	
ForeScout			X		
Impulse Point		X			
InfoExpress			X		
Insightix		X			
Juniper Networks				X	
McAfee			X		
Mirage Networks			X		
Nevis Networks			X		
Sophos				X	
StillSecure				X	
Symantec				X	

- **Bradford's Comprehensive NAC Solution**



NAC Group Test

"A feature set that can do just about anything"



Bradford Enterprise Products

NAC Director™ Full Featured Network Access Control (NAC) Solution

- Identity management + role-based access
- Endpoint compliance validation
- Usage policy enforcement (behavior-based)
- ALL capabilities described below

GCS

Guest/Contractor Services

Sponsored guest and contractor access with tracking / auditing

DPC

Device Profile and Control

Automated device identification and classification with role-based access

UVC

User Visibility and Control

Authentication and role-based access with or without 802.1X

BMC

Behavior Monitoring and Control

Behavior monitoring with ability to mitigate issues at network edge

Additional Information

www.bradfordnetworks.com

Overview

NAC Director™ Guest/Contractor Services (GCS)



PROBLEM
Business partners need greater access to resources on secure devices.

SOLUTION
Contractors can often authenticate on regular staff computing assets to internal systems for extended periods of time.


BENEFITS
Greater productivity for visiting users and external partners, the IT organization, and the enterprise as a whole.

FEATURES
Role-based access
Maximum user authentication, device registration, and assessment for guests users on wireless and wired networks, and enforce role-based access policies.

BRADFORD NETWORKS

Overview

NAC Director™ User Visibility and Control (UVC)



PROBLEM
Who is on the enterprise network?
Organizations require real-time knowledge of all users accessing the network as well as granular control over the resources users have access to.

SOLUTION
Automatic user identification and authorization to access only appropriate network resources.

BENEFITS
Greater productivity and security for users, IT and the enterprise as a whole.

FEATURES
Real-Time, Enterprise-Wide Visibility
Maintains knowledge of all users on the network, including user identity, user role, location, and time.

BRADFORD NETWORKS

Overview

NAC Director™ Device Profile and Control (DPC)



PROBLEM
What is on the enterprise network?
Organizations require real-time knowledge of all endpoint devices on the network as well as granular control over the resources those devices have access to.

SOLUTION
Automatic device identification, profiling, and authorization to access only appropriate network resources.


BENEFITS
Enterprise-wide visibility and control over all endpoint devices attached to the network.

FEATURES
Device Profiling
Without multiple device profiling parameters and technologies via administration-defined templates to classify devices and automate control actions by device type.

BRADFORD NETWORKS

Overview

NAC Director™ Behavior Monitoring and Control (BMC)



PROBLEM
Standardize behavior monitoring and threat detection to reduce risk and provide security at the network edge where users and endpoints connect.

SOLUTION
Add identity awareness and ability to mitigate security issues at the network edge.

BENEFITS
Enterprise Security Policy Enforcement
Policy enforcement at the edge of the network, provides maximum security.

FEATURES
Real-Time Prediction
Provides real-time control over all IP-enabled devices on the network.

BRADFORD NETWORKS



THANK YOU