



NAC Director™



Out-of-Band Network Access Control for Wireless, Wired and VPN Networks

- Control guest/contractor access
- Assess OS patch, anti-virus, anti-spyware, and prohibited applications status
- Automatically remediate at-risk devices
- Secure wireless networks
- Track network access and usage
- Support regulatory compliance

NAC Director's comprehensive access control capabilities, administrative flexibility, and easy to use interface was far ahead of all the products we evaluated. Its advanced out-of-band architecture let us integrate it quickly with our high performance, highly redundant network. NAC Director is a superior NAC solution."

NaviMedix
Bob Chin
Co-founder and EVP

Business in the 21st century requires accessing, organizing, and disseminating information across the enterprise quicker and more cost effectively than the competition. The economic factors forcing this change – global competition, customer expectations, and regulatory mandates – are also forcing the enterprise to evolve into a virtual, interconnected value chain of partners, suppliers, distributors, and customers. This ability to efficiently share and integrate data across the value chain raises the importance of the underlying enterprise network.

As CIOs work to deliver access anytime, anywhere to members of the extended value chain, their networks become increasingly vulnerable to attack by serious hackers and recreational rogues as well as employees and unmanaged users. The only way to protect the integrity of the enterprise network is to architect and implement a comprehensive network access control solution.

Bradford Networks' innovative NAC Director product family delivers the three key elements of effective network access control – identity management, endpoint compliance, and usage policy enforcement – as an integrated, appliance-based solution. NAC Director's out-of-band architecture leverages the existing network infrastructure to deliver automated security services without costly equipment upgrades or performance bottlenecks.

NAC Director automatically identifies authorized users and registered devices and verifies device compliance before granting network access. If the user's system is non-compliant, NAC Director provides self-remediation options so the user can update their system themselves.

NAC Director then continuously enforces security policies, records detailed historical network activity, and generates reports for security threat analysis and regulatory compliance.



IDENTITY MANAGEMENT

NAC Director provides registration, authentication, and role-based access options for precise identity management. Registration identifies and tracks a device and user by MAC address and user ID. Authentication incorporates user name and password information utilizing 802.1X with supplicants or 802.1X-like functionality through a captive portal. NAC Director also integrates with authentication systems and directory technologies such as RADIUS, Active Directory, LDAP, and Sun ONE solutions.

NAC Director creates an advanced 7 point identity profile linking the user name, user role, device name, MAC address, IP address, physical network access point, and access time for each user. This gives administrators the ability to effectively locate, monitor, control, and resolve threats down to the exact point of access for each user and device on the network.

NAC Director's unique "GetOut/StayOut" feature lets network managers quickly locate suspicious users or devices, turn off the port they're connected to, and then flag all associated MAC addresses so they cannot reconnect to other wired, wireless, or VPN ports. Mapping user identity to network identity, no matter how many different machines, MAC addresses or IP addresses are used, prevents users from changing their network identities in order to bypass network access controls.

ENDPOINT COMPLIANCE

NAC Director validates that PCs, laptops, handhelds, and other devices on the network meet the minimum required security standards to keep the network safe and secure. NAC Director performs registry-based assessments on each endpoint device prior to the device being allowed on the production network.

Endpoint assessment is performed using persistent or dissolvable software agents. The persistent agent is installed on the endpoint device for continuous monitoring, while the dissolvable agent is a run-once executable that is suitable for guest or contractor laptops or other devices not owned and managed by the enterprise.

Persistent and dissolvable agents check and verify the following:

- Operating system type, patch levels, and hotfixes
- Anti-virus applications, engine, and definition version levels
- Anti-spyware applications, engine, and definition version levels
- Prohibited/required applications
- File presence/status
- Process activity
- Endpoint drivers

Devices that fail one or more policy checks can be placed in a secure quarantine VLAN where users can self-remediate without the need for help-desk intervention. In addition, NAC Director allows remote validation of devices, further enhancing security and reducing IT staff cycles by allowing users to validate their devices prior to arriving on location.

USAGE POLICY ENFORCEMENT

Many organizations have acceptable use policies for their networks to create secure and reliable operations with high performance and availability levels. These policies are often mandated by regulations such as SOX, HIPAA, PCI, and FISMA. NAC Director provides administrators with the tools and flexibility needed to effectively create and enforce applicable policies. Whether NAC Director is tracking unwanted activities like excessive bandwidth usage, malicious acts, denial of service attacks, or discovering rogue servers and devices, administrators can quickly identify threats, isolate risks, and take corrective action.

When the corrective action is user or device isolation, NAC Director supports four isolation methods (802.1X, MAC-based RADIUS authentication, DHCP, and VLAN steering via SNMP/CLI) while providing a consistent user experience. In isolation, devices are automatically prevented from connecting to both wired and wireless ports.

NAC Director also integrates with a wide range of in-line, deep packet inspection solutions such as intrusion detection/prevention systems, firewalls, web content filters, and traffic shapers to identify and act on threats as they occur. Alarms and traps from deep packet devices trigger NAC Director to initiate appropriate notification, problem isolation, and corrective actions immediately at the offender's point of network access.

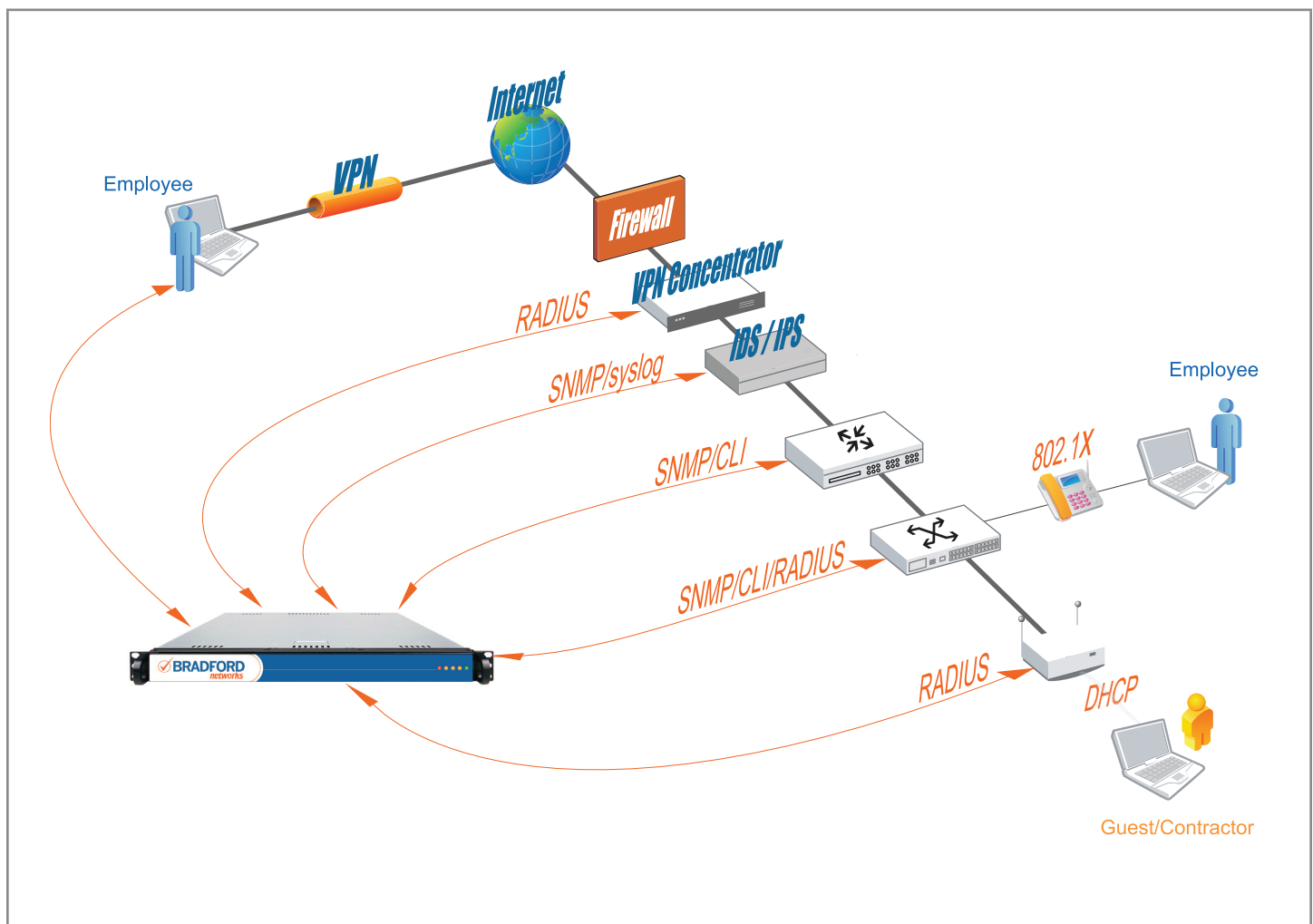
HISTORICAL TRACKING AND REPORTING

NAC Director records and archives comprehensive profile and activity data for every user and device that accesses the network, including connections logs, scan results, and much more. This critical data lets security and network managers analyze user activity patterns, identify emerging trends, and document individual user actions for policy enforcement and regulatory compliance reporting requirements. Standard reports include registrations, registration failures, scan results, and connection logs and can be scheduled or created on an ad-hoc basis. If custom reports are needed, a data definition language (DDL) for the reporting database has been published by Bradford Networks to make the data accessible to external reporting tools like Crystal Reports.

OUT-OF-BAND ARCHITECTURE LEVERAGES EXISTING NETWORK

NAC Director's out-of-band architecture utilizes network configurations from switches, wireless access points, and other infrastructure equipment to create a logical representation of the network. This includes extensive automated network device discovery using a protocol-independent process (SNMP, CLI over SSH, CLI over Telnet) to access each device in the network and identify its unique security features, such as Alcatel's group mobility, or Cisco's private isolated VLANs. NAC Director then correlates network infrastructure data with user identity information to enforce policies.

When policy violations occur, NAC Director executes corrective action via CLI, SNMP, or RADIUS commands to the corresponding network equipment to address the threat at the point of network access.



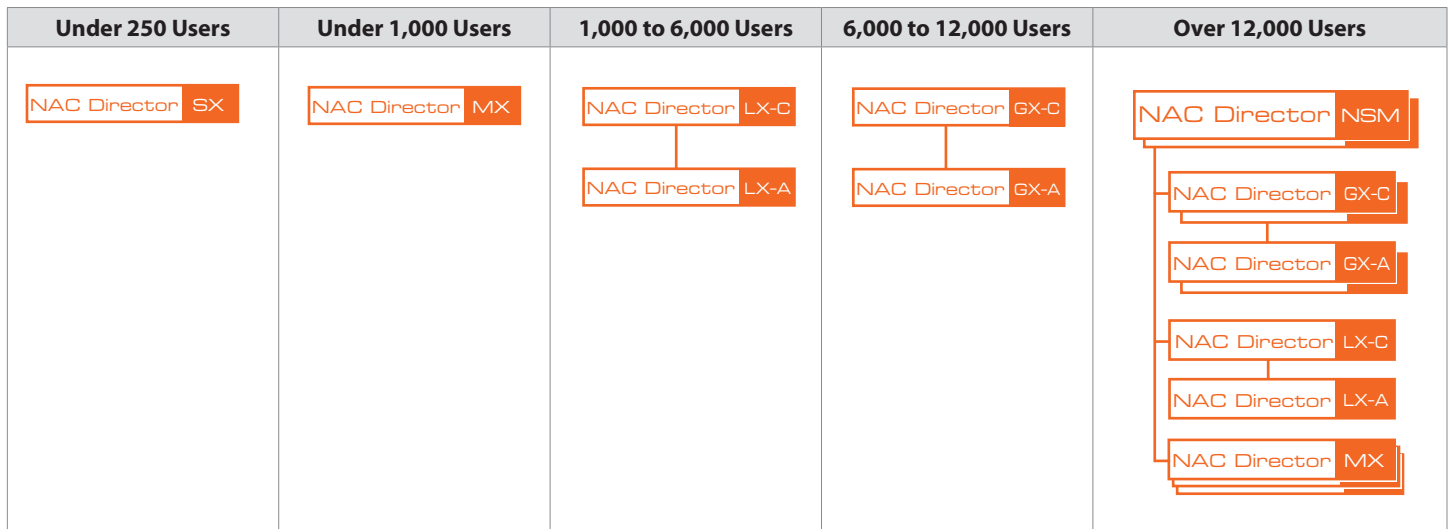
UNMATCHED VENDOR INTEROPERABILITY

Bradford Networks is unmatched in the industry in its support of network and security infrastructure equipment, operating systems, and security applications. NAC Director integrates rapidly with existing networks leveraging the unique features and properties of each network element to enhance and extend security services in the network.

Network Infrastructure	3Com, Alcatel, Allied Telesis, Apple, Aruba, APC, Avaya, Cisco, Dell, Digital Networks, Enterasys, Extreme, Fortinet, Foundry Networks, HP, Juniper, Meru Networks, NetScreen, Nortel, Proxim, Signamax, SMC, Trapeze Networks	
Security Infrastructure	Enterasys Dragon, Fortinet, Internet Security Systems, Lancope, McAfee IntruShield, NitroSecurity, Packeteer, SourceFire, Stonesoft, TippingPoint, TrendMicro	
Authentication & Directory Services	RADIUS	Microsoft IAS, Cisco ACS, Juniper Funk, OSC Radiator, Free RADIUS
	LDAP	Microsoft Active Directory, Novell eDirectory, Sun ONE, OpenLDAP
Operating Systems	Microsoft	Windows 98, Me, 2000 Professional, 2000 Advanced Server, XP Home, XP Professional, XP 64-Bit edition, Server 2003, Vista
	Mac OS X	10.1 Puma, 10.2 Jaguar, 10.3 Panther, 10.4 Tiger, 10.5 Leopard
	Linux	Various distributions of x86 and x86_64 architectures
Endpoint Security Applications	Anti-virus	Avast, Avira, Bullguard, CA, Dr. Web, ESET, F-Prot, F-Secure, G Data, Grisoft AVG, Kaspersky, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Symantec, Trend Micro, ZoneAlarm
	Anti-spyware	Enigma, Kaspersky, Javacool, Lavasoft, McAfee, Norton, PC Tools, Sophos, Spyware Bot, Sunbelt, Trend-Micro, Webroot SpySweeper

NAC DIRECTOR APPLIANCE FAMILY

NAC Director’s highly scalable architecture cost-effectively secures enterprises ranging from one hundred to hundreds of thousands of network users and includes high availability options for mission critical environments. Utilizing high performance, server-based appliances, NAC Director allows customers to upgrade within the product family via cost-effective software upgrades.



ABOUT BRADFORD NETWORKS

Bradford Networks develops advanced network access control solutions for wireless, wired and VPN networks. Bradford’s award-winning, out-of-band appliances leverage existing network infrastructure to automatically enforce NAC policy at the network edge making networks more secure and efficient. Privately held, Bradford Networks is located in Concord, NH.