



# Top 10 Reasons Why Customers Choose Cisco NAC

Brochure

## 1. Addresses customer challenges

Cisco Network Admission Control (NAC) solutions help customers meet real-world business and security challenges such as guest access, unmanaged assets, unauthorized access, posture assessment and remediation, governance, compliance (for example, HIPAA for healthcare customers and PCI for retail customers), and security policy enforcement.

## 2. Reduces complexity with effective and integrated services

Cisco delivers multiple NAC services, including guest, profiling, posture, remediation, and governance services. The Cisco NAC Manager centralizes the ruleset updates service. The Cisco NAC Server integrates the guest, profiling collection, and posture assessment services in a single platform. The [Cisco NAC Profiler](#) provides visibility, intelligence, and automation to simplify NAC deployments and reduce ongoing NAC operational costs.

## 3. Works with existing network and is optimized for an upgraded network

Cisco NAC works seamlessly with the existing network, enabling customers to deploy a NAC solution without having to modify or upgrade the existing network. Cisco NAC is optimized for an upgraded network, using the infrastructure, identity, and service layers as customers go through their natural refresh cycles. Customer can apply any of the NAC services provided by the award winning NAC Manager and NAC Server over an infrastructure controlled via out-of-band SNMP or RADIUS (802.1x).

## 4. Supports third-party solutions and applications

Customers are seeking a fully integrated solution that supports their existing third-party solutions and applications. Cisco NAC integrates with a wide range of endpoint security applications, and supports built-in policies for more than 350 applications from leading antivirus and other security and management software solution providers. Cisco NAC also delivers interoperability with Microsoft solutions such as Active Directory and Vista, and provides value-added NAC services for the upcoming Microsoft Network Access Protection (NAP).

## 5. Supports all environments

Customers can deploy Cisco NAC anywhere in their infrastructure. Cisco NAC supports all business environments: main campus, branch offices, remote access, wireless, and guest access. With Cisco NAC, IT and security staff can enforce security policies on both managed or unmanaged assets. Cisco NAC supports numerous operating systems, including Windows, Macintosh, and Linux. By providing the Cisco NAC profiling service, Cisco NAC can also manage non-authenticating devices (such as IP phones and printers) automatically, saving IT organizations precious headcount to identity, document, and track these devices.

## 6. Flexible deployment options

Understanding that every customer is unique, Cisco provides many NAC deployment options, such as Layer 2 and Layer 3; centralized or distributed; in-band or out-of-band; SNMP or RADIUS; standalone server appliance or modular server ([a module in the Cisco integrated services router](#)). These flexible options help customers deploy Cisco NAC solutions based on their specific environment and business needs.

## 7. Ease of use and grows with your business

Cisco NAC is easy to deploy and manage, offering features such as single-sign-on (SSO) and silent remediation to greatly reduce the impact to end users. Cisco NAC is also scalable. Customers can start Cisco NAC where they need it the most (for example, guest access, wireless, VPN, or branch offices), and extend NAC deployment to other areas of their business over time. Cisco NAC can be deployed with an installed base as small as 50 users and as large as tens of thousands users.

## 8. A component of the Cisco Self-Defending Network

The best security posture is achieved with a layered security defense. Cisco NAC is one of the foundational components of the Cisco Self-Defending Network. With Cisco NAC, security enforcement is enabled across network access devices, providing collaborative security with other Cisco Self-Defending Network components such as Cisco Security Agent, Cisco Adaptive Security Appliances, and Cisco wireless security products.

## 9. Protects existing investments

Cisco is committed to helping customers protect their security investments. Cisco's convergence plan brings together appliance- and framework-based NAC technology, taking full consideration of customers' business priorities, security challenges, infrastructure needs, and operational requirements. In the converged Cisco NAC solution, Cisco NAC Appliance components become the foundation for NAC services while the Cisco infrastructure components provide the pillars for access authentication and network enforcement.

## 10. Proven track record of innovation

Cisco makes NAC a reality for customers by delivering a solution that is simple, deployable, manageable, and effective, with innovative features and services that meet customers' real-world needs. Cisco NAC continues to evolve, providing innovative identity, posture, profiling, and governance services. More than 2000 customers have chosen Cisco NAC over other competing point solutions.