USE CASE

BRADFORD NETWORKS

Network Sentry

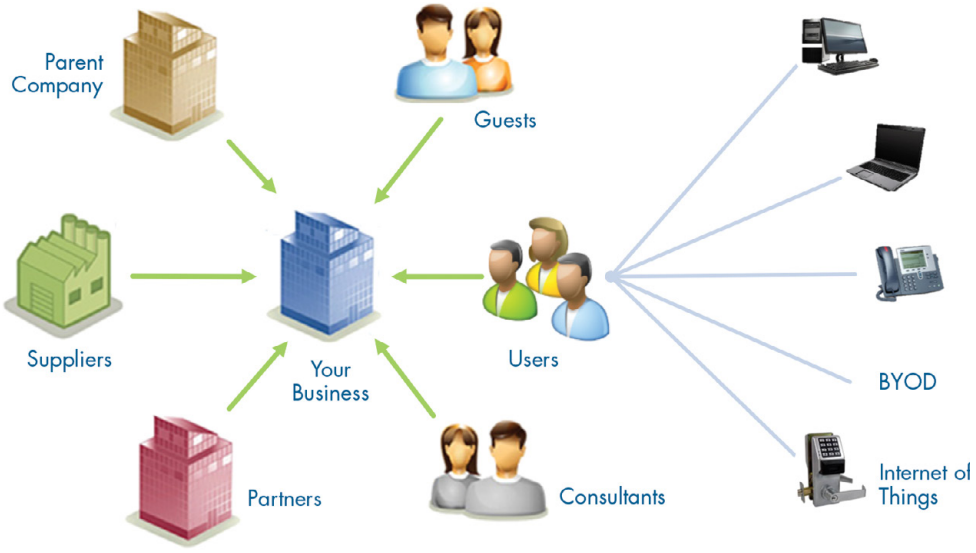
ROLE-BASED DYNAMIC NETWORK ACCESS

Network Sentry features a policy-based network access control engine that enhances security by enabling network segmentation to control access to network segments with sensitive information. Using role-based dynamic network access, Network Sentry identifies, validates and controls every wired, wireless or VPN network connection before access is granted.

With vulnerable endpoints and unsuspecting users being the primary attack vector for cyber criminals, it is critical to allow only users with well-protected devices to gain access to sensitive corporate assets. As the number of IP-enabled devices skyrockets with the Internet of Things (IoT), it's imperative for an organization's security team to comprehend and mitigate risks resulting from a growing "attack surface" across the network.

Using a centralized and highly scalable architecture, Network Sentry leverages the built-in commands of network switches, routers and access points to establish a Live Inventory of Network Connections and enforce control over network access. It seamlessly integrates with authentication technologies such as 802.1X, RADIUS, and Active Directory to automatically determine if a device is corporate issued or employee owned, and the appropriate level of network access for the user of that device.

The flexibility of the architecture enables the solution to be deployed as a hardware appliance, a virtual appliance, or a cloud service — ensuring that Network Sentry adapts to the unique needs of any network environment.



» Dynamic and ever-expanding attack surface

KEY BENEFITS

- » Identify every switch, router, wireless controller and access point on the network
- » Gain complete visibility and control over users and devices accessing wired and wireless network
- » Assess the risk of every endpoint including desktops, mobile and IoT devices
- » Provision role-based policy to enable secure network access
- » Enable network segmentation to secure sensitive data
- » Automate onboarding process for large volumes of company-issued and personally-owned devices
- » Improve overall network security posture, compliance and asset protection

DEPLOYMENT OPTIONS

- » Hardware appliance
- » Virtual appliance: VMware ESXi, Microsoft Hyper-V
- » Cloud Service

Network Sentry's comprehensive discovery process automatically identifies and profiles all network devices and users rather than requiring an access control solution for each network segment. Unlike network access control products from networking and wireless vendors, Network Sentry provides a view across all brands of network equipment and connecting devices — thereby eliminating risky network blind spots.

Gain Unprecedented Network Visibility

Fundamental to the security of a constantly changing network is an understanding of its makeup: Switches, Routers, Wireless Controllers and Access Points as well as VPN concentrators. Network Sentry provides a real-time view into dynamic network infrastructure so that risky changes are detected and prevented. Network Sentry provides centralized administration and reporting from a single console and visibility of all network devices, users and endpoints across all locations without deployment of hardware at each site.

Identify and Classify Every Endpoint on the Network

With the growth in BYOD and the IoT, managing device types and ownership is a significant challenge when securing a network. Network Sentry automatically discovers and profiles endpoints, classifying them by type and determining if the device is corporate-issued or employee-owned. The user is also identified and the appropriate role-based network access policies are implemented within Network Sentry to protect critical data and sensitive assets while ensuring compliance with internal, industry and government regulations and mandates.

Access Risk of Every Endpoint on the Network

Ensuring the integrity of wired and wireless devices before they connect to your network minimizes the risk of vulnerability and the spread of exploits and malware. Network Sentry validates the endpoint's configuration as it attempts to join the network. If the configuration is found to be non-compliant, the connection is prevented or the device is forced to an isolated or limited-access VLAN. Users are warned that their device must be remediated. This can be done automatically through integration with a vulnerability assessment, patch management system or by following manual instructions delivered to the user's device. Access is granted once corrective measures are successfully undertaken.

Enable Network Segmentation to Secure Sensitive Data

A flat network makes it trivial for hackers and malicious users to roam freely across the network. Use dynamic role-based network access control to logically create network segments to group applications and like data together to limit access by specific group while enhancing network security.

Automate and Simplify Network Access for Guests

Network Sentry streamlines the secure registration process of guest users. When appropriate, users can self-register their own devices — laptops, tablets or smartphones — shifting the workload away from IT staff. Or, the simplified task of onboarding guests can also be delegated to designated network administrators.

Automate Onboarding Process

BYOD and guest-network environments using 802.1X can leverage Network Sentry's EasyConnect feature to simplify the onboarding process by dynamically configuring security settings on Windows, Mac OS X, iOS and Android devices. In the event that a device initially connects to an open (unsecured) wireless SSID, Network Sentry automatically configures its security settings by seamlessly moving the connection to a secure SSID.

Simulate Control Policies Before Going Live

Network Sentry enables "what-if" scenarios when defining network access policies. By test-driving the policies, administrators can evaluate the impact of making changes before implementing them. This capability helps to avoid a policy that is too restrictive or too open without causing unnecessary connectivity issues and adversely impacting users and their devices.

Improve Overall Network Security Posture, Compliance and Asset Protection

Network Sentry empowers extensive management and control functionality. Features built into the existing infrastructure can be leveraged to secure the network. Control features are accessed via a highly customizable, easy-to-use web-based administrative dashboard. Users or devices on the network are easily located and identified with a few mouse clicks. Potential threats are contained by isolating suspect users and vulnerable devices, or by enforcing a range of containment actions.

BRADFORD NETWORKS

374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web vwww.bradfordnetworks.com

Bradford Networks offers the best solution to enable secure network access for corporate issued and personal mobile devices. The company's flexible Bradford Networks platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Bradford Networks provides a view across all brands of network equipment and connecting devices eliminating the network blind spots that can introduce risk. Widely recognized by industry analysts including Gartner, Forrester and ESG, Bradford Networks has received SC Magazine's Best Buy and Best NAC product awards; TechTarget Security 7 Award; CRN 5 Star Partner Program Award; and eSchool Week Reader's Choice Award.