NETWORK ACCESS CONTROL FOR GOVERNMENT

DETECTING AND PROTECTING DATA COLLECTION

Trustwave Enterprise Network Access Control (NAC) enables granular control over network access and delivers continuous monitoring of government networks. In addition, Trustwave NAC helps to prevent the spread of malware and other threats from the inside of the network out that can harm the infrastructure and leave government agencies vulnerable to attack and data loss. Safeguarding access to government networks is essential to protecting the data collection and retention process—a necessary component to maintain a high level of service to constituents.

THE TRUSTWAVE NAC DIFFERENCE

A network-agnostic solution, Trustwave Enterprise **NAC requires no agent software** and automatically performs risk assessments on all managed *and* unmanaged points **regardless of IP device type or operating system (OS)**. When an endpoint is determined to be out of network admissions policy, the Trustwave NAC appliance virtually steps in to quarantine and isolate the endpoint from the network.

Trustwave recently won the *SC Magazine* 2013 award for Best NAC (Network Access Control) product and has achieved Common Criteria validation with EAL 2+ level of certification, providing critical advantages, including:

- Full life cycle protection for all endpoints, managed and unmanaged
- Agentless network access control combined with zero-day threat prevention and automated policy enforcement
- Network intelligence that provides a unified view of endpoint activity, delivering powerful analysis support and situational awareness of your network's history and usage

Together, these features deliver comprehensive endpoint control, offering security checks throughout the life cycle of a device's network access. Trustwave NAC policy enforcement is composed of three support components: Identity, Compliance and Behavior.

Identity

- Tracks user behavior
- Enforces policy based on user access profiles or role-based user groups
- Integrates seamlessly with existing credential stores and identity management systems

Compliance

- Continuously monitors health and compliance status of every endpoint on the network
- Tracks all compliance data with comprehensive, Web 2.0-style management and reporting to aid with FISMA compliance
- Flexible, tiered enforcement

Behavior

- Analyzes every packet from every device
- Provides zero-day threat detection
- Includes L2-L7 behavioral policy enforcement

Trustwave NAC detects and continuously evaluates all entrants to the target network based on acceptance criteria for pre-admission and continuous monitoring post-admission.

The Trustwave unique and comprehensive NAC solution portfolio includes the most flexible deployment options in the industry offered to government:

Trustwave Enterprise NAC

A highly scalable, full-cycle NAC solution that is uniquely designed for large government networks.

- Management of thousands of endpoints
- Centralized, Web-based user interface with unified configuration and reporting support to aid with FISMA compliance
- Deployed virtually inline, compatible with any network infrastructure

For smaller networks, Trustwave offers a lightweight, full-function, standalone NAC option.

Trustwave Managed NAC

Our leading Managed Security Service operation offers the Trustwave full-function NAC as a fully managed service.

- Includes same features and functions as Trustwave Enterprise NAC
- Maintains NAC sensor integrity and health
- Provides reduced cost with no capital expense for agencies with limited funding

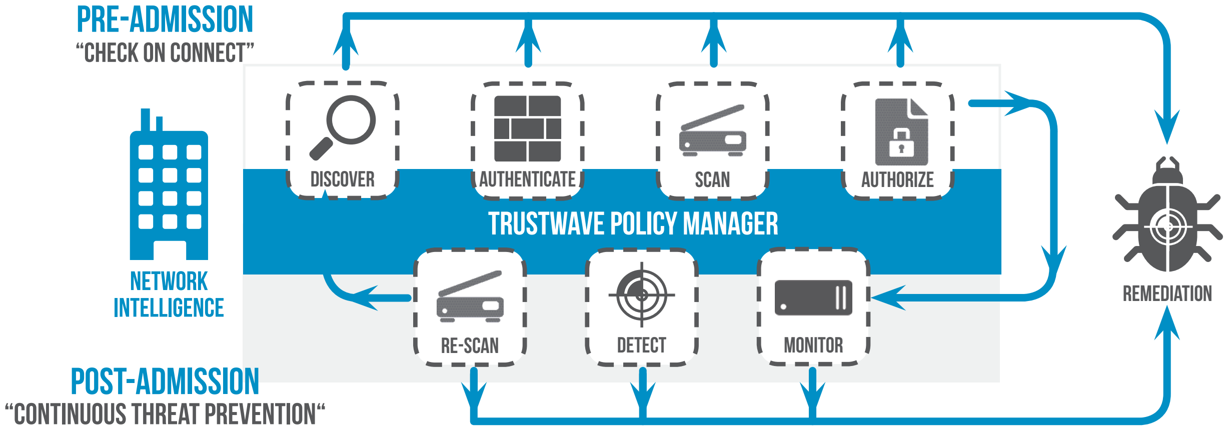
Plug-n-Play NAC

Offered as an add-on software module with Trustwave Managed UTM service for smaller, distributed enterprises, Plug-n-Play NAC automatically detects and optionally blocks rogue devices and network services.

- Enables real-time device comparison with authorized asset lists.
- Provides detection of rogue devices including routers.
- Delivers automatic updates of firewall rules for policy enforcement aligned with FISMA compliance requirements.

NAC COMPARISONS

TYPE OF NAC ISSUES	ENTERPRISE NAC	MANAGED NAC	PLUG-N-PLAY NAC
Deployment Mode	Out of Band	Out of Band	Inline
Quarantine Mechanism	ARP Management	ARP Management	Firewall
Management Responsibility	Customer	Trustwave	Trustwave
Device Authentication & Rogue Detection	●	●	●
Rogue Gateway Detection	●	●	●
OS Detection	●	●	●
Service Port Detection	●	●	●
Compliance Scanning (FW, AV,AS, Patch)	●	●	
Active Directory Integration	●	●	



EMBRACE BYOD

Trustwave NAC puts control of managing Bring Your Own Device (BYOD) back into the hands of IT administrators to ensure a secure, productive, and compliant computing environment. BYOD also creates challenges including managing non-standard, heterogeneous devices, personal and potentially rogue applications, and the potential of introducing malware into government networks. Embracing a BYOD culture offers government agencies numerous benefits including:

- Increased employee satisfaction and productivity
- Lowering overall total cost of ownership (TCO) of mobile devices

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com.