StillSecure®

Closed loop endpoint compliance – an innovative, standards based approach

A case study - NMCI

Tom Lerach – Head of IA, HP DoD
Rajat Bhargava – StillSecure

October 2009

Agenda – endpoint compliance with NMCI

- Introduction to NMCI
- The IA challenge
- Next generation approach: closed loop endpoint compliance
- NAC Implementation battle Plan
- Current and future state
- Q & A

NMCI Network Access Control Status

HP Enterprise Services

NMCI Overview

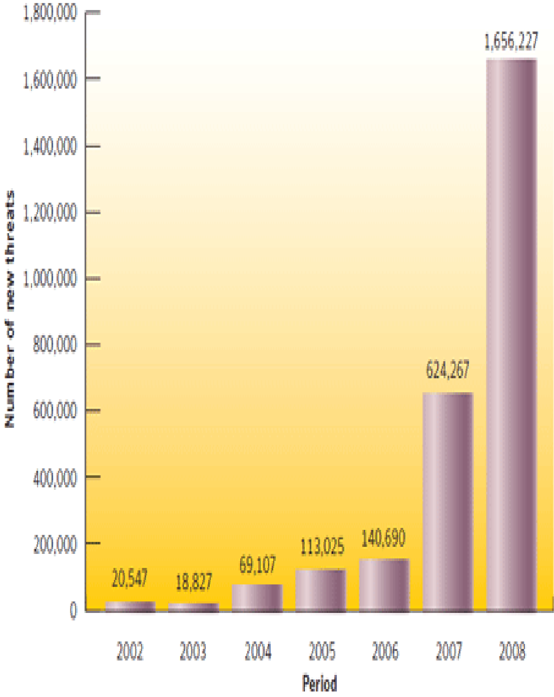
The Navy Marine Corps Intranet (NMCI) is the world's largest purpose-built IP network:

- Standardized software, hardware, and infrastructure for more 700,000 Sailors, Marines and civilians at 620 locations.
- Four Network Operations Centers (NOCs)
- Approximately 375,000 seats
- More than 19,000 BlackBerry devices
- Approximately 2,000 wireless PC cards
- More than 100 million e-mail messages per month
- 3.4 terabytes of data throughput (1/3 the volume of the Library of Congress) per day

NMCI is much more than just a big network

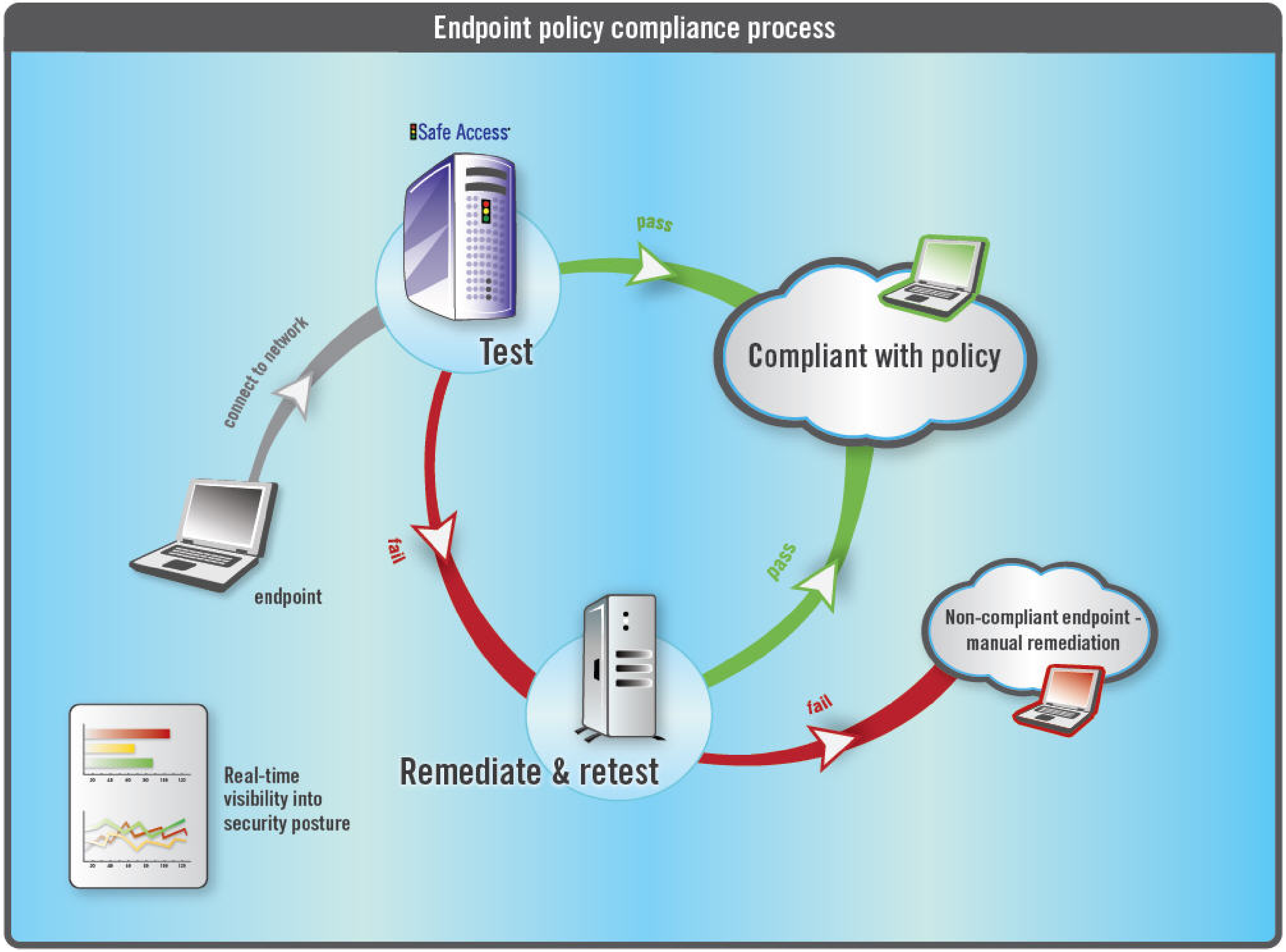
C2 Concerns – the “New Normal”

- Cyber war continues to escalate →
- DOD required IA posture continues to be elevated, going deeper into the infrastructure (bios, chip sets), wider in scope to other services (W2.0, social networking)
- Key area of action is Vulnerability Management, and the configuration control on networked devices.

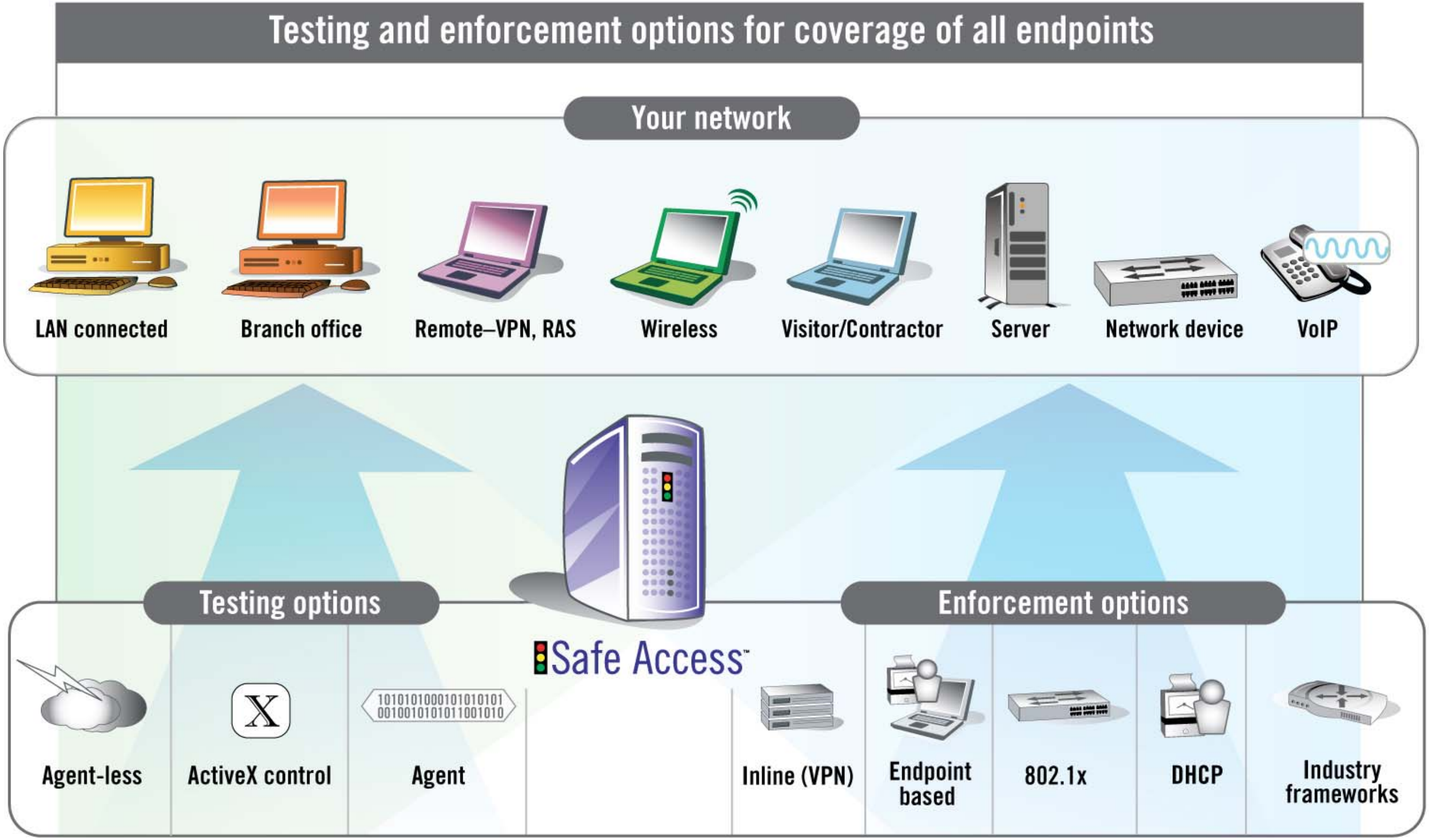


- NMCI has hardened the edge, has hardened the Boundary 1 – 4. How do we stop things before they get on the network, stop motion???
- One key initiative for us: Network Access Control (NAC)

Closed loop endpoint compliance process


Endpoint policy compliance process
Safe Access
Test
pass
Compliant with policy
connect to network
endpoint
fail
pass
Remediate & retest
Non-compliant endpoint - manual remediation
fail
Real-time visibility into security posture

Flex testing + flex enforcement = full coverage in your network



SCAP – the great equalizer?

- **SCAP efforts to standardize compliance**
  - NAC vs. vulnerability scanners vs. endpoint solutions – standards eliminate tool differences
  - Results can be compared and normalized

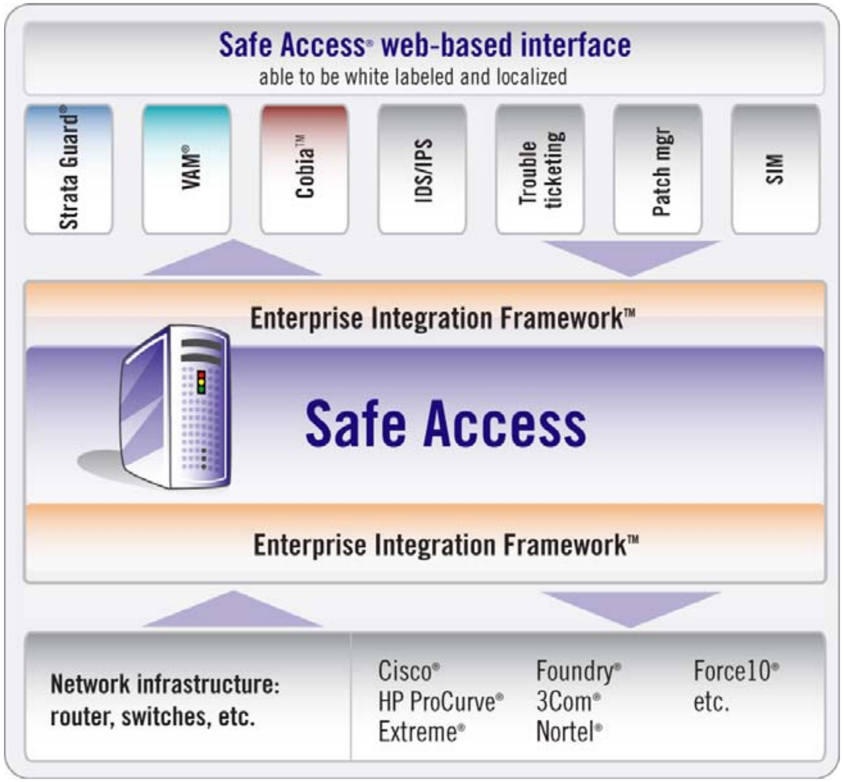
- **Standardization of checks**
  - Which checks are required / not required
  - Which ones are critical and how will they be tested
  - Depth of testing – misconfigurations, malware, etc.
  - Checks created / validated by government – control quality of tests

- **StillSecure vision: SCAP compliant scan on connect will be model**
  - “Vulnerability scanners” will ultimately give way to scan on connect technology
  - Test devices at point of entry and at time of greatest risk to the network
  - Immediately remedy issues prior to potential for widespread outbreak
  - Point in time testing and validation will go by the wayside
  - Depth of testing will continue to increase – more issues, more control, more risk mitigation

- **StillSecure Safe Access SCAP support in process**
  - FDCC and XCCDF support
  - Authenticated scanner
  - Purpose built scan engine to be extended to include SCAP support

Open and standards based

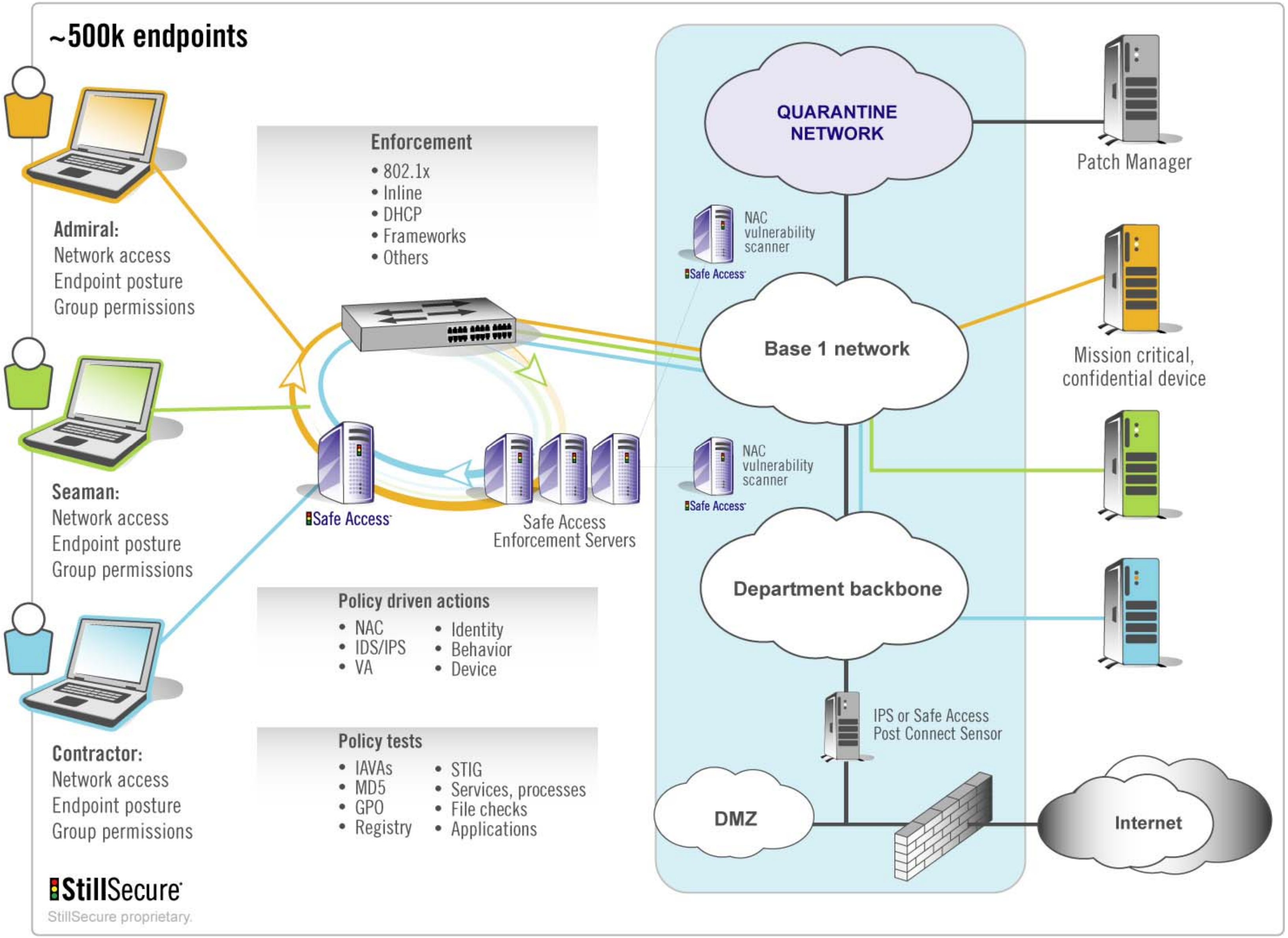
- **Enterprise Integration Framework (EIF): A published open architecture**
  - Allows third-party systems to control Safe Access testing and quarantining functions
  - Enables Safe Access to import/export endpoint security data with other IT systems


Safe Access® web-based interface
able to be white labeled and localized
Strata Guard®
VAM®
Cobia™
IDS/IPS
Trouble ticketing
Patch mgr
SIM
Enterprise Integration Framework™
Safe Access
Enterprise Integration Framework™
Network infrastructure: router, switches, etc.
Cisco®
HP ProCurve®
Extreme®
Foundry®
3Com®
Nortel®
Force10®
etc.

- **EIF benefits:**
  - Leverages Safe Access quarantining and testing capabilities
  - Leverages capabilities of other security-related systems
  - Improves security, productivity, and efficiency with the IT environment

- **Standards focused**
  - Common Criteria
  - FIPS 140-2 Level 1 and 2
  - SCAP in process – XCCDF / FDCC support

NMCI Safe Access deployment architecture



~500k endpoints

Admiral:
Network access
Endpoint posture
Group permissions

Seaman:
Network access
Endpoint posture
Group permissions

Contractor:
Network access
Endpoint posture
Group permissions

Enforcement
- 802.1x
- Inline
- DHCP
- Frameworks
- Others

Policy driven actions
- NAC
- IDS/IPS
- VA
- Identity
- Behavior
- Device

Policy tests
- IAVAs
- MD5
- GPO
- Registry
- STIG
- Services, processes
- File checks
- Applications

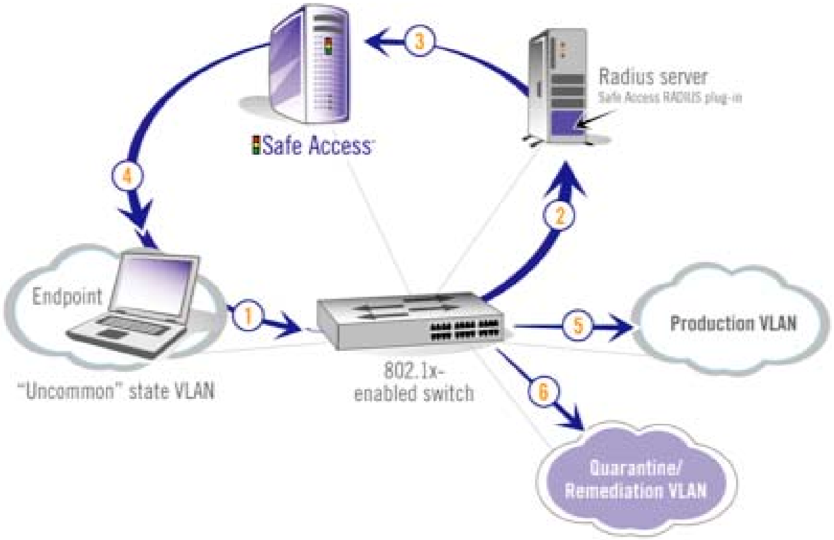
Safe Access
Safe Access Enforcement Servers
QUARANTINE NETWORK
Patch Manager
NAC vulnerability scanner
Safe Access
Base 1 network
Mission critical, confidential device
NAC vulnerability scanner
Safe Access
Department backbone
IPS or Safe Access Post Connect Sensor
DMZ
Internet

StillSecure
StillSecure proprietary.

NAC Battle Plan

- NMCI is deploying an enterprise NAC solution consisting of:
  - 802.1x authentication with machine based certificates
  - Posture assessment w/Remediation
  - Layer 2 network access assignment
- Solution is based on DISA White Paper ***Network Access Control_Security At a Glance***
  - Draft version V1.R0.1 with enhancements.
  - An overview of the 802.1x enforcement mode flow is below.
- Two key phases - passive and then active NAC

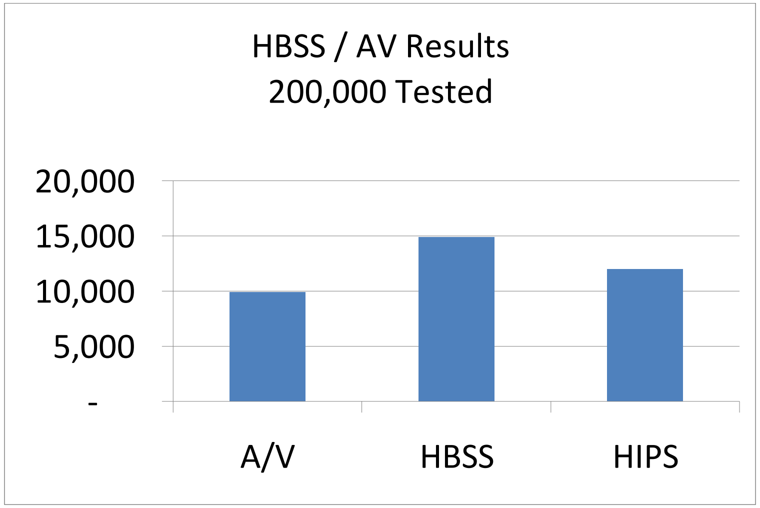
Two key phases – enterprise deployment of passive NAC with scanning/alarming enabled – Complete.
Pilot, then deployment of active NAC with quarantining (in process this year, py2010)

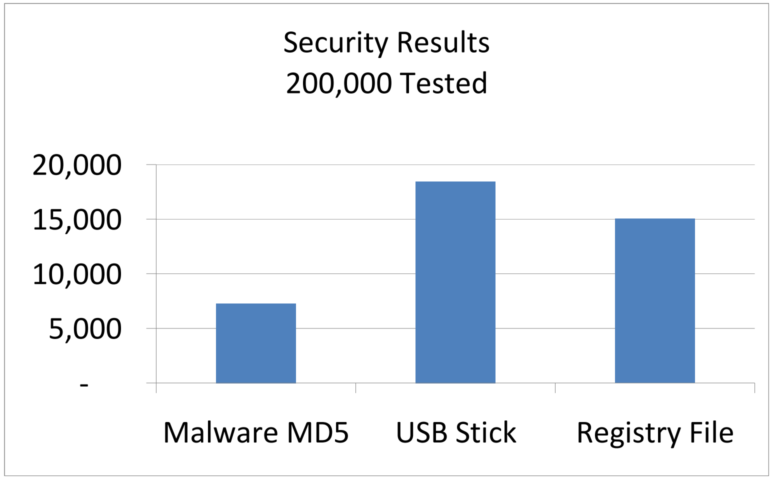


NMCI IA NAC

Current State – passive NAC (all data is notional)

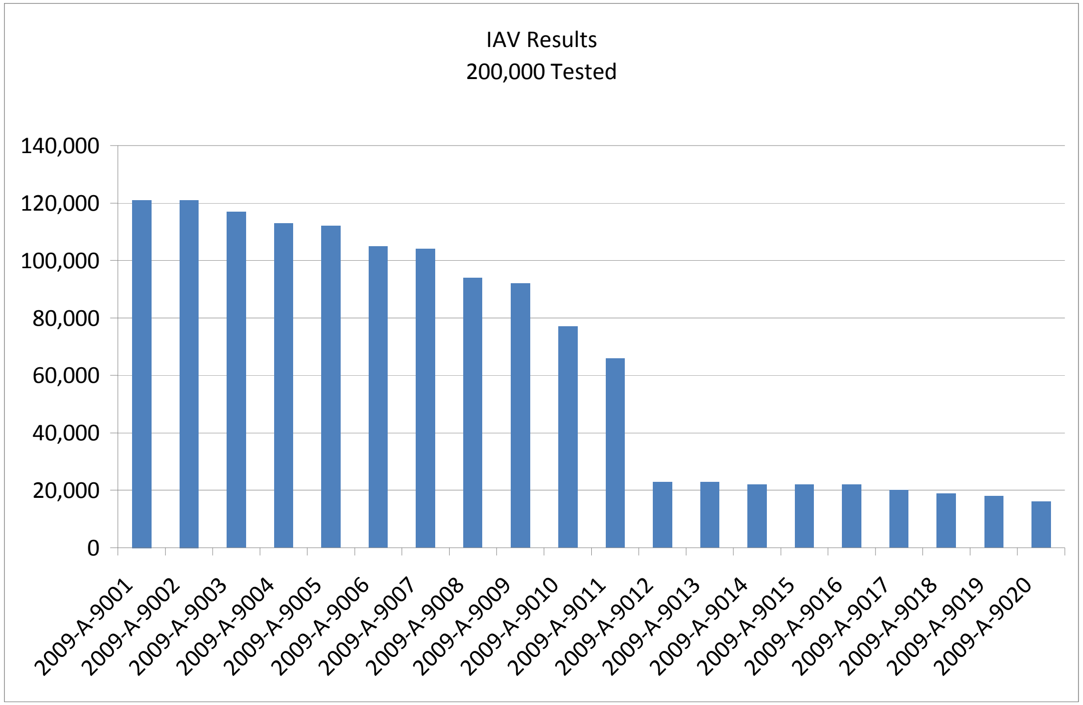
- SafeAccess NAC solution is employed for on-connect scanning
  - IAV Compliance
  - Security Application Compliance
    - Host Based Security Suite (HBSS) and sub-modules
    - Workstation Anti-Virus
  - Targeted malicious files
    - MD5
    - Filename/File Extension
    - Registry Settings
- NAC reports:
  - Negative findings for compliance
    - Forwarded for mitigation
  - Positive findings for targeted and malicious scans
    - Input to SIM for correlation and investigation





Current State – IAV (all data is notional)

- IAV Compliance
  - Scans for all applicable JTF-GNO reported IA Vulnerabilites
    - IAV Alerts (A), Bulletins (B), Technical (T)
    - Consistent with SCCVI (eEye Retina) Output
  - Provides multiple output formats for mitigation and tracking
    - Calculates and trends vulnerabilities per machine
    - Input into Security Information Manager (SIM) for correlation



Next phase, Active NAC Objectives

- In FY10, the effort within NMCI will be a pilot deployment with the following objectives:
  - Provide a managed device authentication function to authenticate managed devices using the IEEE 802.1X Port Based Network Access Control specification.
  - Provide a non-managed device authentication function to authenticate non-managed devices (i.e., printers ,etc) using MAC authentication.
  - Provide logically separated VLAN’s for repositing endpoints as part of the network admission process. The network admission function will support the “movement” of endpoint devices among the VLAN’s during the various phases of access negotiation.
  - Provide a network admission function management console that will allow authorized network operators to define and manage network access policy rules.
  - Provide a notification and metric reporting function for endpoint devices, i.e. non-compliant systems quarantined for remediation, etc.
  - Provide a mechanism whereby a user can self-initiate a policy assessment of his or her endpoint device to facilitate obtaining the latest patches and software updates on an NMCI workstation in order to avoid a disruption of service.
- An After Action write-up will be provided to the NMCI Program Office to facilitate analysis of the impact of this capability has on the day to day mission of the Navy.

Future Implementation

- **Managed Device Authentication**
- Endpoints and access switches will be 802.1x enabled
  - Today NMCI is Certificate Authority and all NMCI workstations are issued machine certificates; leveraged in solutions today on NMCI (WLAN, RRAS).
  - Considering leveraging native .1x capability within the Windows OS for client.
- **Unmanaged Device Authentication**
- If endpoint does not have a supplicant, we will be authenticating through MAC
- Authentication Bypass (MAB).
  - Feature supported within current switch fabric
  - Have the switch vendor (Cisco) perform code rec for enterprise
- **STIG Compliance**
- Solution will seek to comply with current outlined STIG ID’s.
  - *(NET-NAC-002: CAT II) The IAO/NSO will ensure the network access control policy*
  - *limits access in the Policy Assessment VLAN to the policy assessment server only.*
  - *Would request to combine Assessment and Remediation to minimize the time of “movement” and get systems to Production more quickly.*
  - *(NET-NAC-004: CAT II) The IAO/NSO will ensure the network access control policy contains all non-authenticated network access requests in an un-authorized VLAN that has access to no devices or networks.*
  - *Considerations for option to support non-auth systems to be reposited to Guest VLAN*
- **Add’l Challenges**
- “Whitelisting” – Policy for government accepted non-compliant hosts (traveling VIP’s that have limited access to remediation systems, etc.
- Support for multiple authentication directories (certification stores).
  - Ability to authenticate NMCI, OneNet, IT-21, DoD, etc.

Questions?

Thank you!

Contact information:

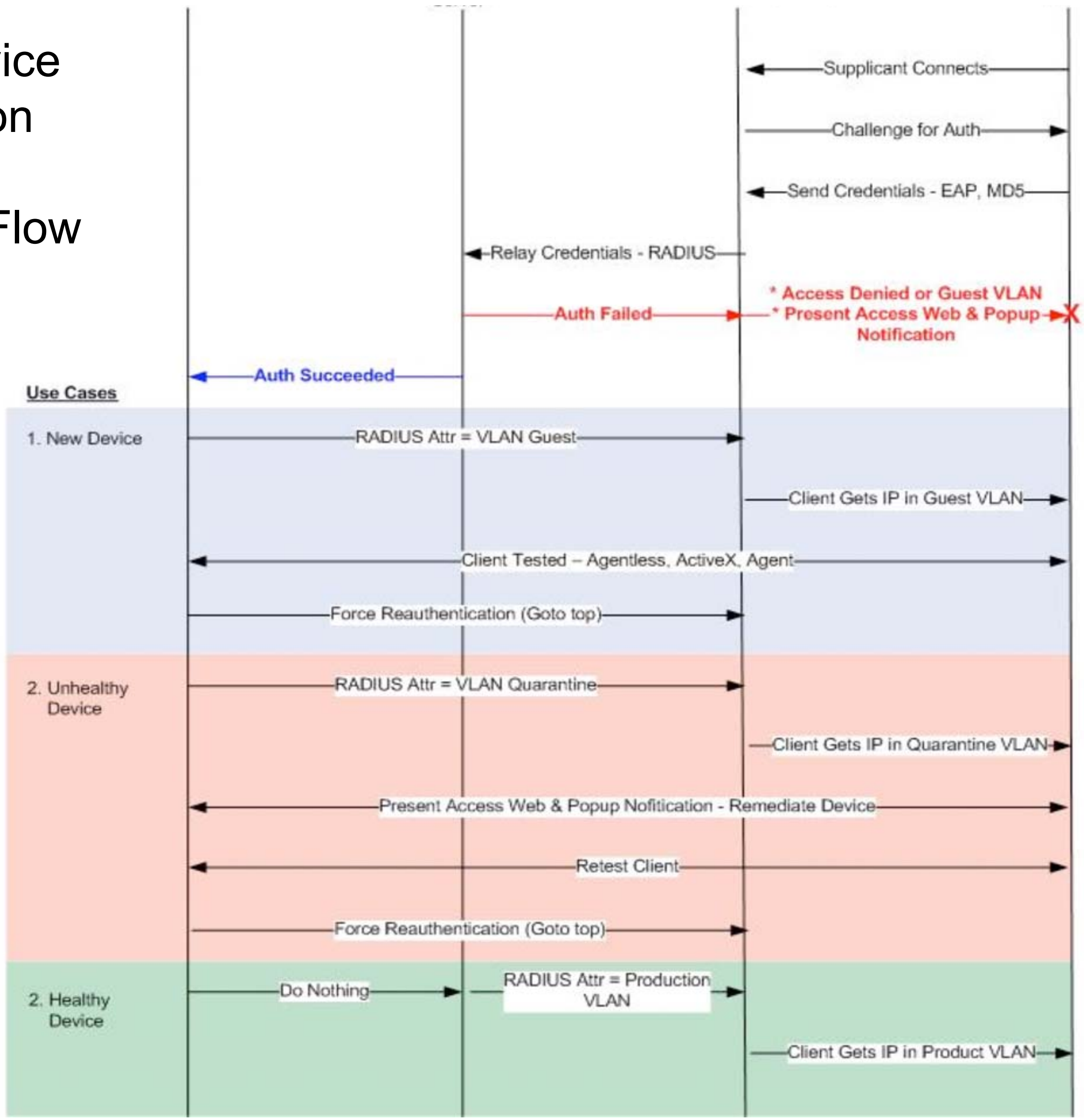
Tom Lerach
Head of IA, HP DoD

Rajat Bhargava
President & CEO, StillSecure

Backup Slides

Managed Device Authentication

NAC Process Flow



Supplicant Connects

Challenge for Auth

Send Credentials - EAP, MD5

Relay Credentials - RADIUS

Auth Failed

* Access Denied or Guest VLAN
* Present Access Web & Popup Notification

Auth Succeeded

Use Cases

1. New Device

RADIUS Attr = VLAN Guest

Client Gets IP in Guest VLAN

Client Tested – Agentless, ActiveX, Agent

Force Reauthentication (Goto top)

2. Unhealthy Device

RADIUS Attr = VLAN Quarantine

Client Gets IP in Quarantine VLAN

Present Access Web & Popup Nofitication - Remediate Device

Retest Client

Force Reauthentication (Goto top)

2. Healthy Device

Do Nothing

RADIUS Attr = Production VLAN

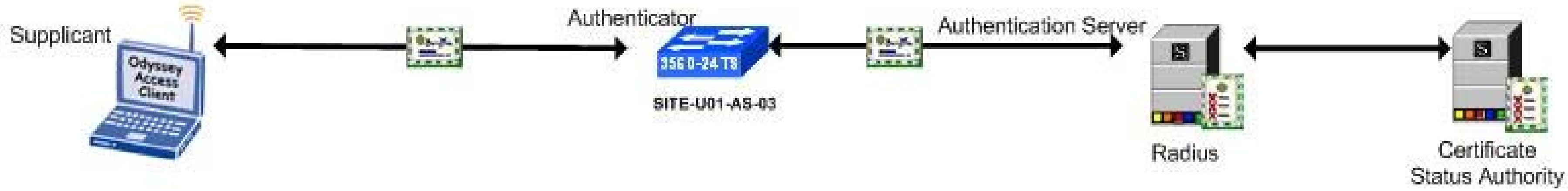
Client Gets IP in Product VLAN

Safe Access supports all key 802.1X functionality outlined in the DISA white paper to provide authentication of devices at Layer 2, before devices receive an IP Address. 802.1X enabled switches or other access points, challenge connecting devices for authentication information which is securely relayed to RADIUS authentication servers for authentication before an IP Address has been assigned. This prevents endpoint devices from posing any significant risk to the network.

Authentication options include:

- unique User ID/Password
- AD domain User/Pass
- AD device membership (machine certificates)
- MAC Address authentication

Machine authentication with NMCI certificates will use EAP-TLS, as shown below. Safe Access directs devices that pass or fail authentication to specific VLANs for special handling and restriction or remediation.



Managed Device Authentication

•Endpoints use 802.1x supplicant
•All switch ports are 802.1x enabled
After successful authentication, endpoint is placed in an assessment VLAN with ACL limiting access to:

- DHCP server
- SafeAccess Server
- Remediation services (Remedy, Radia, HBSS, SAV, etc.)

If endpoint fails compliance test, SafeAccess will tag endpoint as unhealthy and force an 802.1x re-auth. After successful authentication, endpoint is placed in the remediation VLAN with ACL limiting access to:

- DHCP Server
- SafeAccess Server
- Remediation services (Remedy, Radia, HBSS, SAV, etc.)

Upon successful remediation, SafeAccess will retest endpoint, tag it as healthy and force an 802.1x re-auth. After successful authentication, endpoint is placed in the production VLAN.

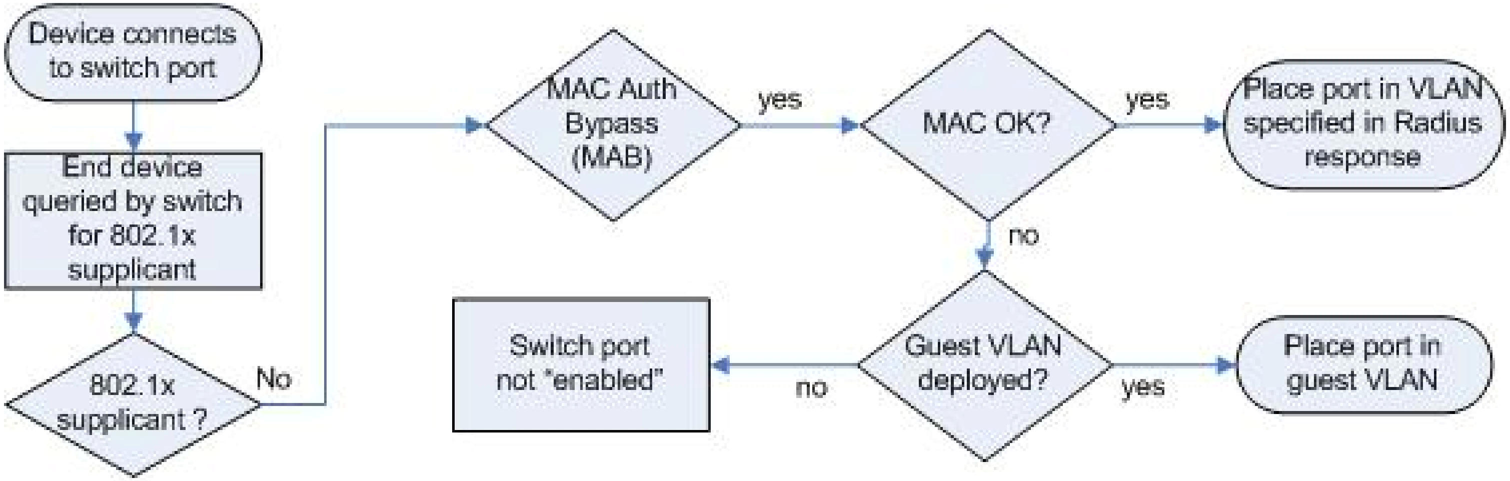
If endpoint passes compliance test, SafeAccess will tag endpoint as healthy and force an 802.1x re-auth. After successful authentication, endpoint is placed in the production VLAN.

Unmanaged Device Authentication

If endpoint does not have a supplicant, it will be authenticated through supported feature of Cisco access layer switches, MAC Authentication Bypass (MAB).

- If device passes MAB authentication (e.g. a printer, CLIN 27), SafeAccess will place in VLAN specified by RADIUS server.
- If device fails MAB authentication, it will be placed in a restricted VLAN (802.1x guest VLAN, configurable per port) or the port will change back to the unauthorized state (802.1x un-auth state).

Below is a process flow for an unmanaged device.


Device connects to switch port
End device queried by switch for 802.1x supplicant
802.1x supplicant ?
No
MAC Auth Bypass (MAB)
yes
MAC OK?
yes
Place port in VLAN specified in Radius response
no
Guest VLAN deployed?
yes
Place port in guest VLAN
no
Switch port not "enabled"

HP Enterprise Services

PROPRIETARY STATEMENT

Contract No. N00024-00-D-6000
Electronic Data Systems Corporation
13600 EDS Drive, Herndon, Virginia 20171

Technology for better business outcomes

HP
13600 EDS Drive
Herndon VA 20171