

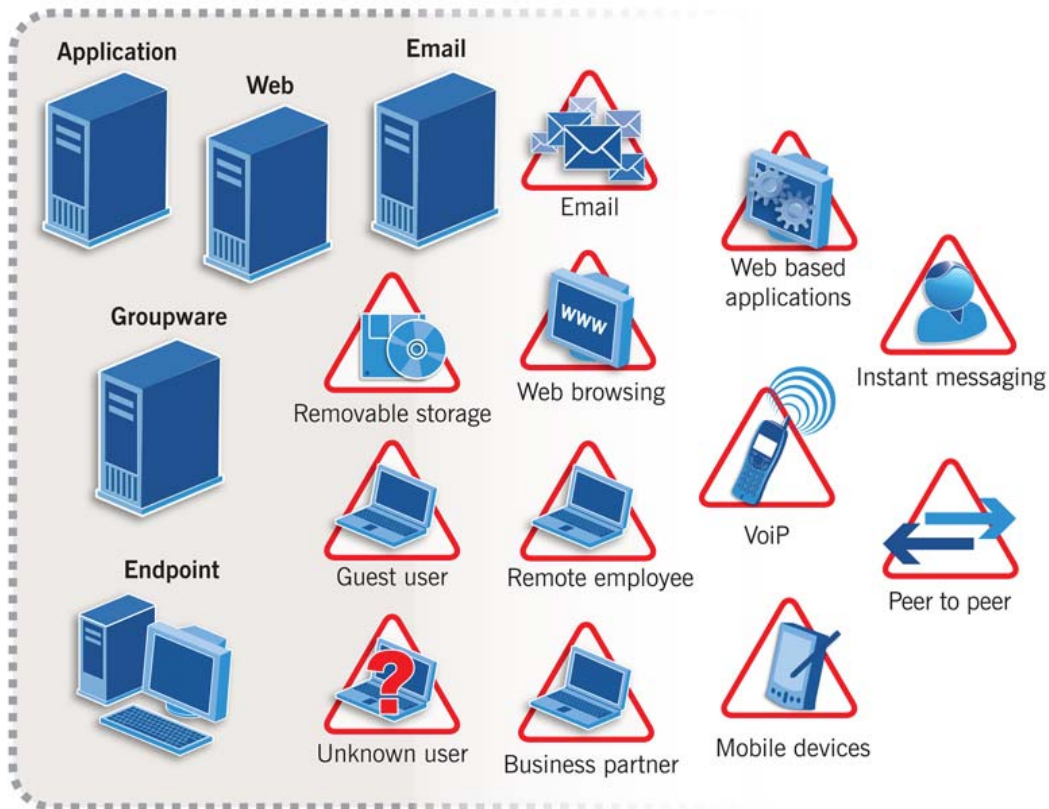


NAC - It's really about the endpoint

Richard Jacobs

April 2008

Today's dissolving perimeter



- Increased mobility
- Flexible working
- Non-managed users

Rapidly evolving threat landscape

Then

Noisy and random threats

Disruptive, IT systems crash

Growing volume, spread on email

Now

Silent &
targeted

Theft &
damage

Accelerating &
web-based

IT challenges

Deploying ever increasing number of security solutions

Controlling network access and compliance

Doing more with static budgets

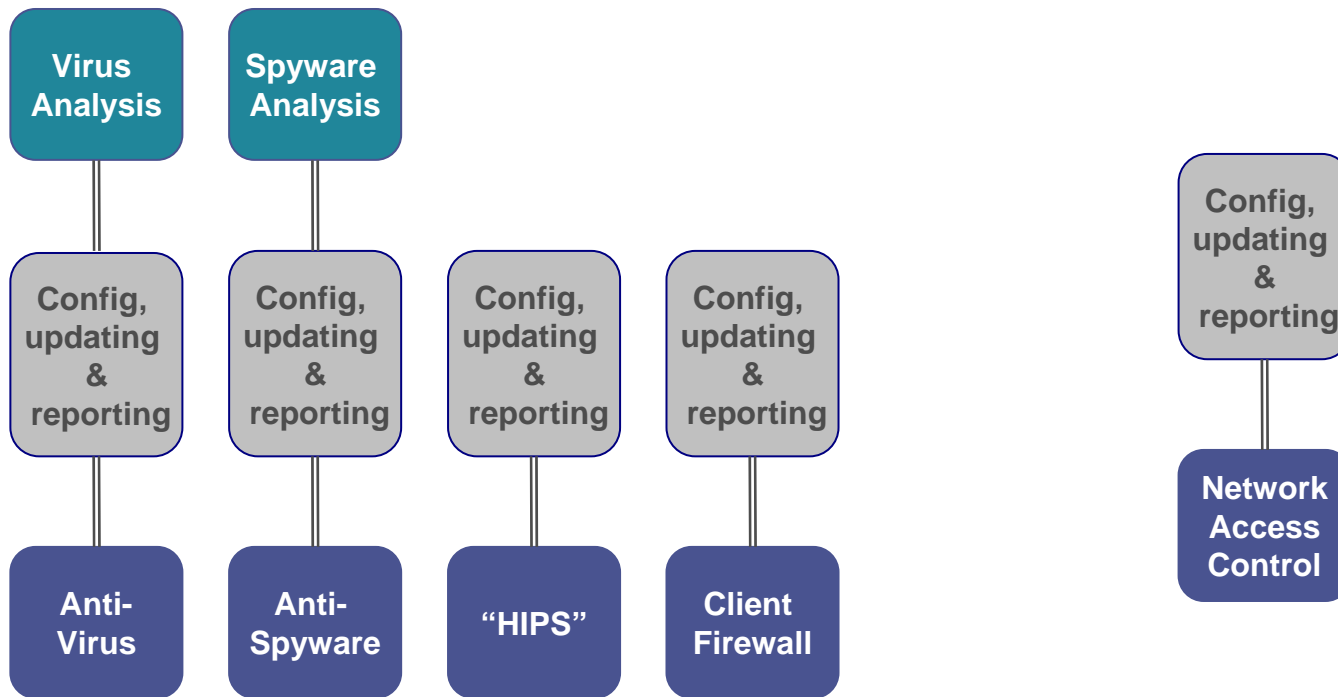
Security slows computers, network, web and email

Reliable support when required

Still getting infected



Fragmented response to growing threats



Restricted protection, confused responsibilities & increased costs

What is Network Access Control?

- Everybody claiming NAC solutions
 - Network infrastructure providers
 - Niche appliance vendors
 - Endpoint software vendors
- But what's the problem?
 - NAC ≠ Enforcement
 - NAC = Enablement
 - Through risk reduction
 - And reducing IT costs/pain

Network Access Control policies

- All connecting PCs must have all critical patches installed
- Anti-virus must be enabled & have been updated in last 24hrs
- All laptops must have personal firewalls enabled
- All contractors' PCs must comply with the corporate standard
- Unknown computers may only access the internet
- All laptops must be encrypted & backup to the network daily
- Brokers must submit reports within 3 days of month end

NAC use scenarios



KNOWN USER
MANAGED ENDPOINT

Employees

Company
owned assets

- ✓ Ensure security and productivity
- ✓ Enable access
- ✓ Automatically correct configuration drift



KNOWN USER
UNMANAGED ENDPOINT

Partners

Non-company
owned assets

- ✓ Ensure security
- ✓ Restrict access
- ✓ Enable self help on non-compliance



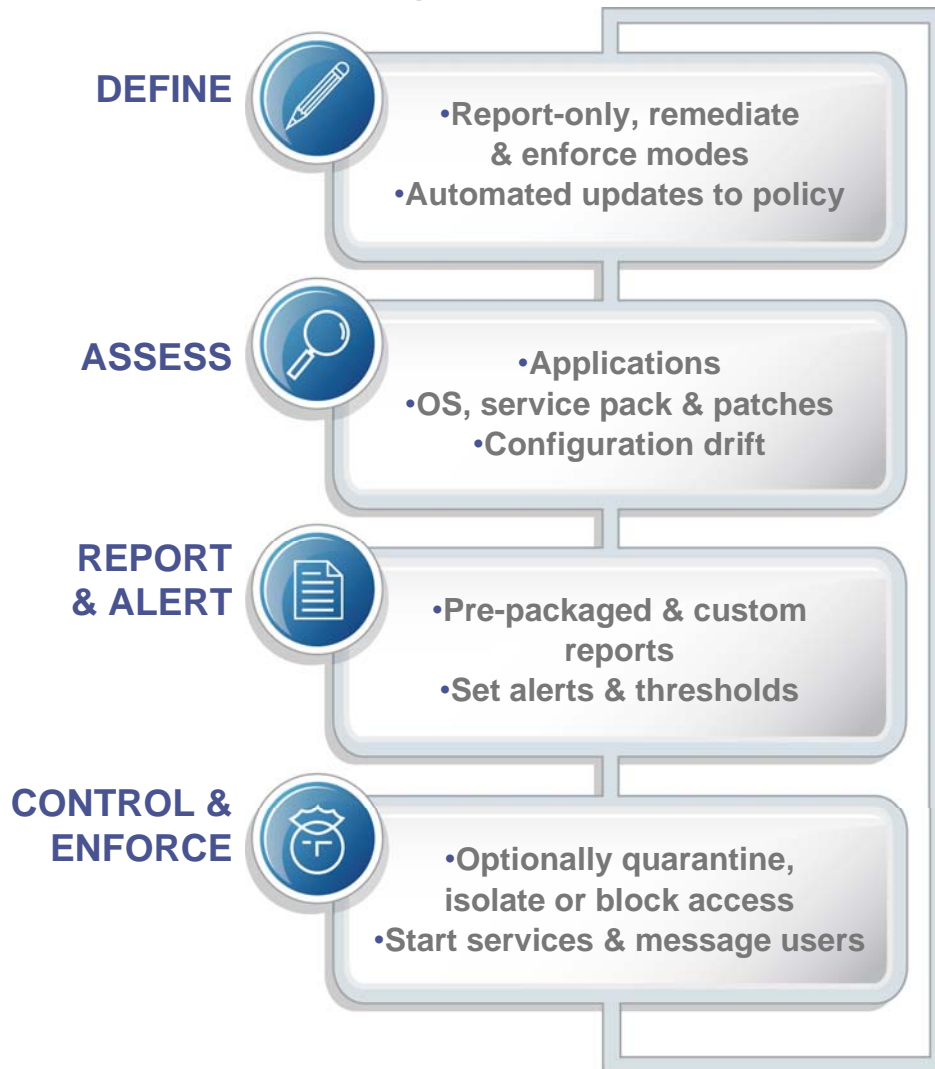
UNKNOWN USER
UNMANAGED ENDPOINT

Guests

Non-company
owned assets

- ✓ Ensure authorization
- ✓ Isolate traffic
- ✓ Block access if not authorized

NAC life-cycle



- ✓ Define policy & actions by user group
 - ✓ Protection, vulnerability, productivity
-

- ✓ Pre- and post-connect
 - ✓ Managed and unmanaged
-

- ✓ Compliance, application and session
 - ✓ Real-time and historical
-

- ✓ Control access
- ✓ Automated and assisted fix
- ✓ Enforce assessment

Network Access Control assessment

- Contextual assessment
 - On the corporate LAN
 - On the road
 - At home
- Employees, contractors & guests
- Wherever & whenever users are working

NAC reporting & alerting

- Real-time alerting
- Compliance auditing
 - How many corporate PCs are not patched?
 - Which users have disabled the personal firewall?
 - How many unknown PCs are connecting to the network?

NAC Case Study



Goal: Zero Vulnerabilities

- Approach:

- Policy/Baseline: SOPHOS
- Access Control: DHCP

- Critical Success Factors

- Tested Usage Cases (employee PC, visitor PC, "bad guy")
- Focus first on audit, not enforcement

- Before NAC:

- 4.4 Vulnerabilities per PC
- 70% of systems patched within 30 days

- After NAC (report only):

- 1.4 Vulnerabilities per PC (trending down)
- 99% of systems patched within 7 days

NAC control

- Remediation
 - User notification
 - Self-service or automated
- Application level control
 - By EXE and IP address
- User based
 - CEO
 - Sales department
 - Call center
 - Contractor
 - Guest

NAC enforcement

- Ensure that all PCs are assessed
- Prevent connection of unassessed PCs
- Set rules for other assets
 - E.g. Wifi access points

What is Network Access Control?

- NAC is managing endpoint/user policy compliance
 - Endpoint IT responsibility
 - Definition of policy
 - Continuous assessment
 - Reporting and alerting
 - Control and remediation
 - Converging with endpoint security
 - Corporate and unknown users and systems
- Enforced through the network
 - Partner with Network IT team
 - Use existing infrastructure



NAC - It's really about the endpoint

Richard Jacobs

April 2008