The self-defending network
a resilient network

By
Steen Pedersen
Ementor, Denmark

The self-defending network - a resilient network

- What is required of our internal networks?
  - Available, robust, fast and secure
  - No virus or worms active inside our network
  - All systems on our network are compliant to our policy with antivirus, patches, configuration etc.
- Protect our network from unsecure devices
  - Possibility to block, disconnect or quarantine unsecure devices

Resilient infrastructure

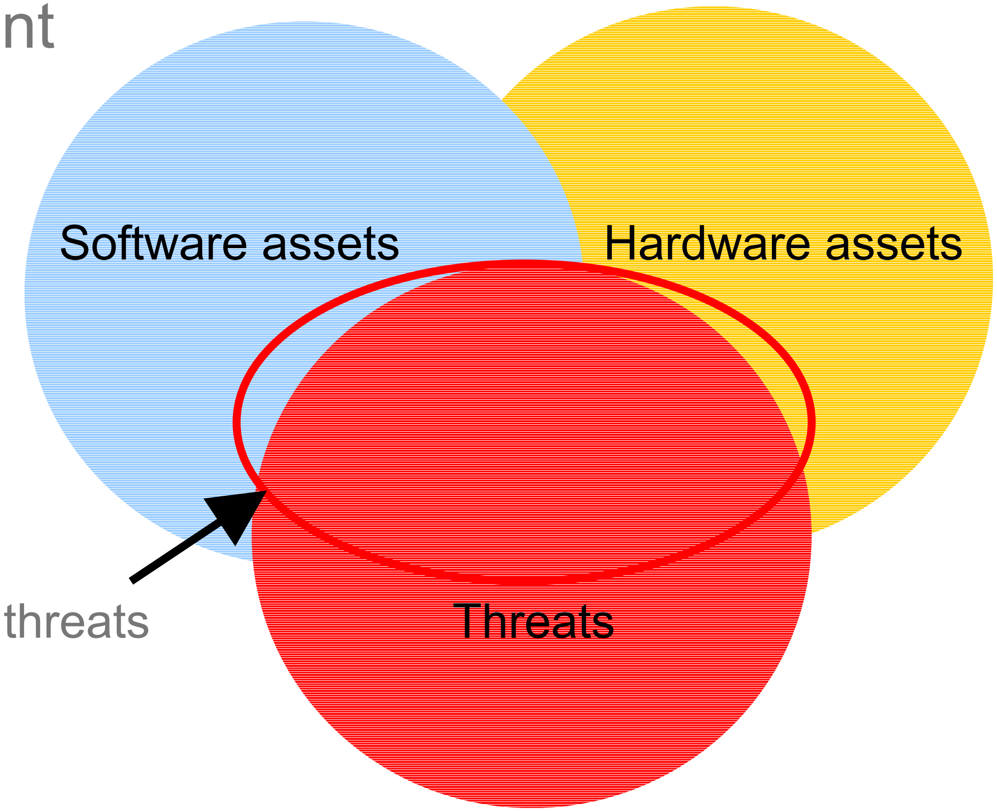
- Know your infrastructure
- Know the threats

- Focus on the critical section of the infrastructure first
  - Step by step implement methods to protect the infrastructure

- We all face challenges managing our infrastructures. Disruptions to availability can be caused by any number of factors

Software and hardware asset management

A key component



The real security threats

DHCP - Dynamic Host Configuration Protocol

- DHCP – A key component to the problems
- What is DHCP?
- DHCP's purpose is to enable individual computers on an IP network to extract their configurations from a server
- The overall purpose of this is to reduce the work necessary to administer IP addresses a large network

“Manage the un-managed”

- CIA - Confidentiality, Integrity & Availability
  - The main concern is often availability

- Within a distributed network, knowing which devices to trust is a major issue

- It does not help having the best updated AV, client firewall and Host IDS if we do not verify that all systems are running with them – Auditing is the key

Defensive vs. Offensive Security

- Defensive Security
  - Putting out “fires” as they occur
  - This model is the most common
- Offensive Security
  - Reduce the chances of “fires” starting
  - Enhance the response time to a “fire”
  - Prepare for “fire” – minimizing problems when they occurs
  - Learn from incidents and adjust

Technologies and solutions

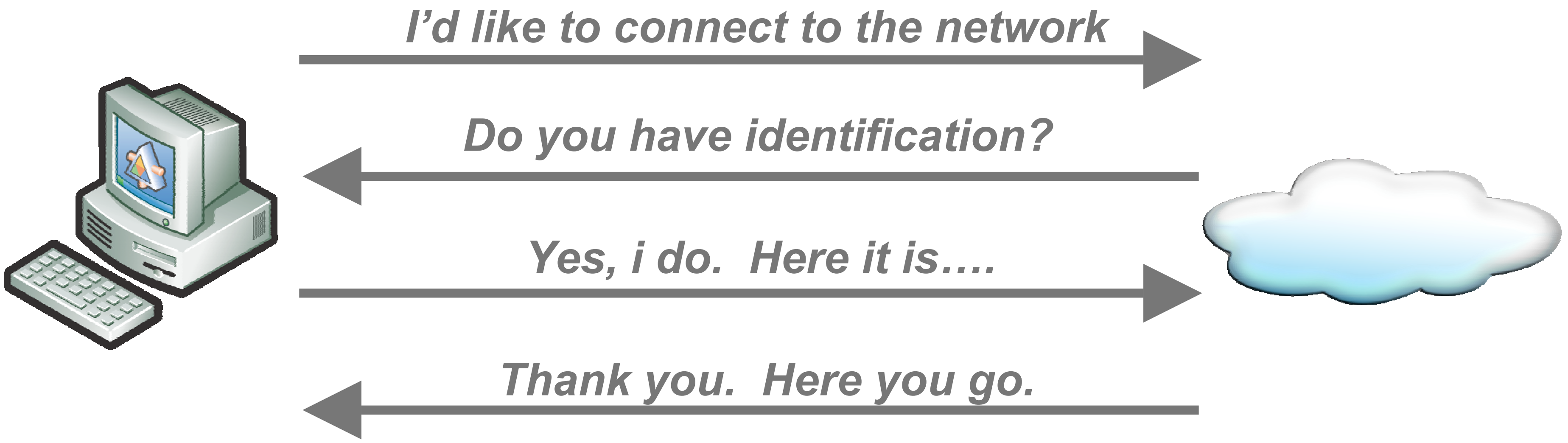
- Cisco
  - NAC – Network Admission Control
- Microsoft
  - NAP – Network Access Protection
- McAfee
  - MTC – McAfee Trusted Connection
  - Rogue System detection

Cisco – NAC – Network Admission Control

- Cisco’s vision of the Self-Defending Network
  - Cisco’s Secure Connectivity
  - Threat Defence
  - Trust and Identity Management

- NAC is the first deliverable initiative in the Cisco vision of Self-Defending Network

Typical Identity Trust Model on the Network



I’d like to connect to the network

Do you have identification?

Yes, i do. Here it is….

Thank you. Here you go.

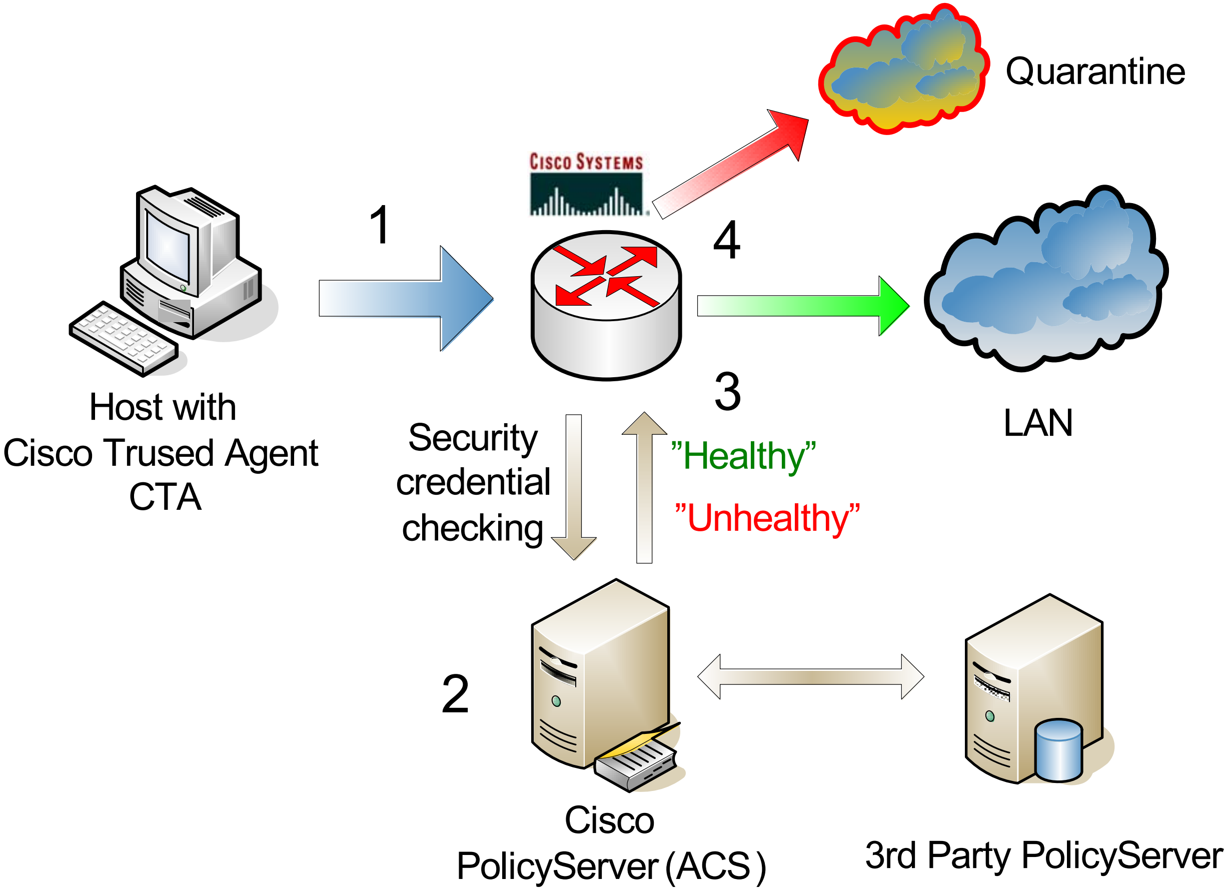
Questions from the host:

- How secure is this network?
- How secure are the other hosts connected?
- Are there any virus on the network?

Questions from the Network:

- How secure is this host?
- Is it safe for the network to have accepted this host?
- What if this host starts to send virus?

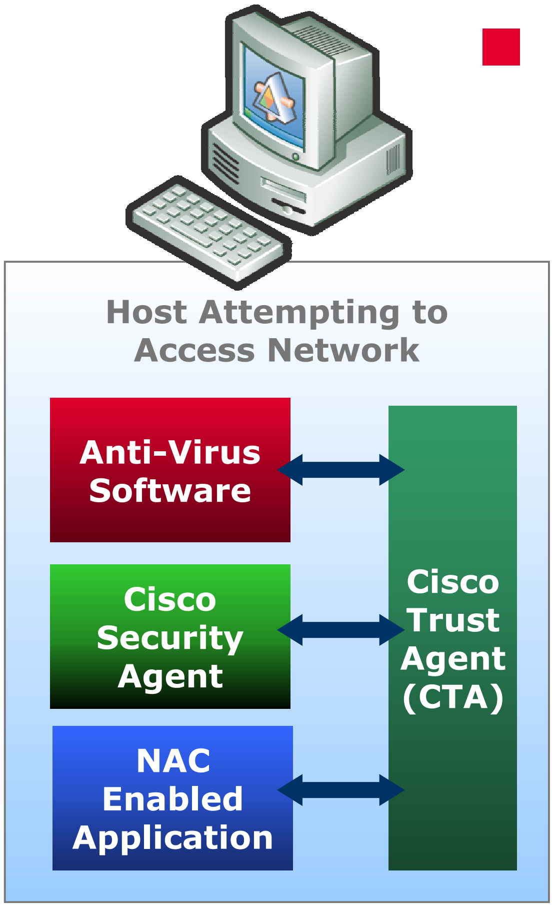
How Cisco NAC Works



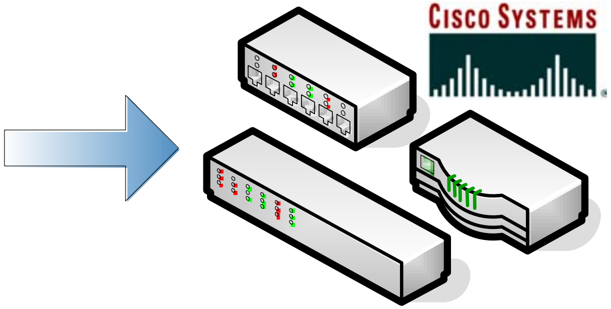
1. Request access
2. Check security
3. Status returned
4. Access control

How Cisco NAC Works

- Cisco Trust Agent talks with several components



NAC devices



Routers, Switches, Wireless Access Points

Cisco NAC – Pros:

- Integrated into the network device infrastructure
- Un-managed systems can be blocked from the network or placed in a quarantine segment/VLAN
- Non-compliant systems can be placed in a quarantine segment/VLAN of the network
- Works nearly real-time
- Extended with host based intrusion prevention makes it reactive to unknown threats

Cisco NAC – Cons:

- Requires Cisco network devices
- Not supported on all Cisco network devices
- Only integration with Cisco's host intrusion prevention
- Not full support for all antivirus products
- Costly to implement and only Windows OS support

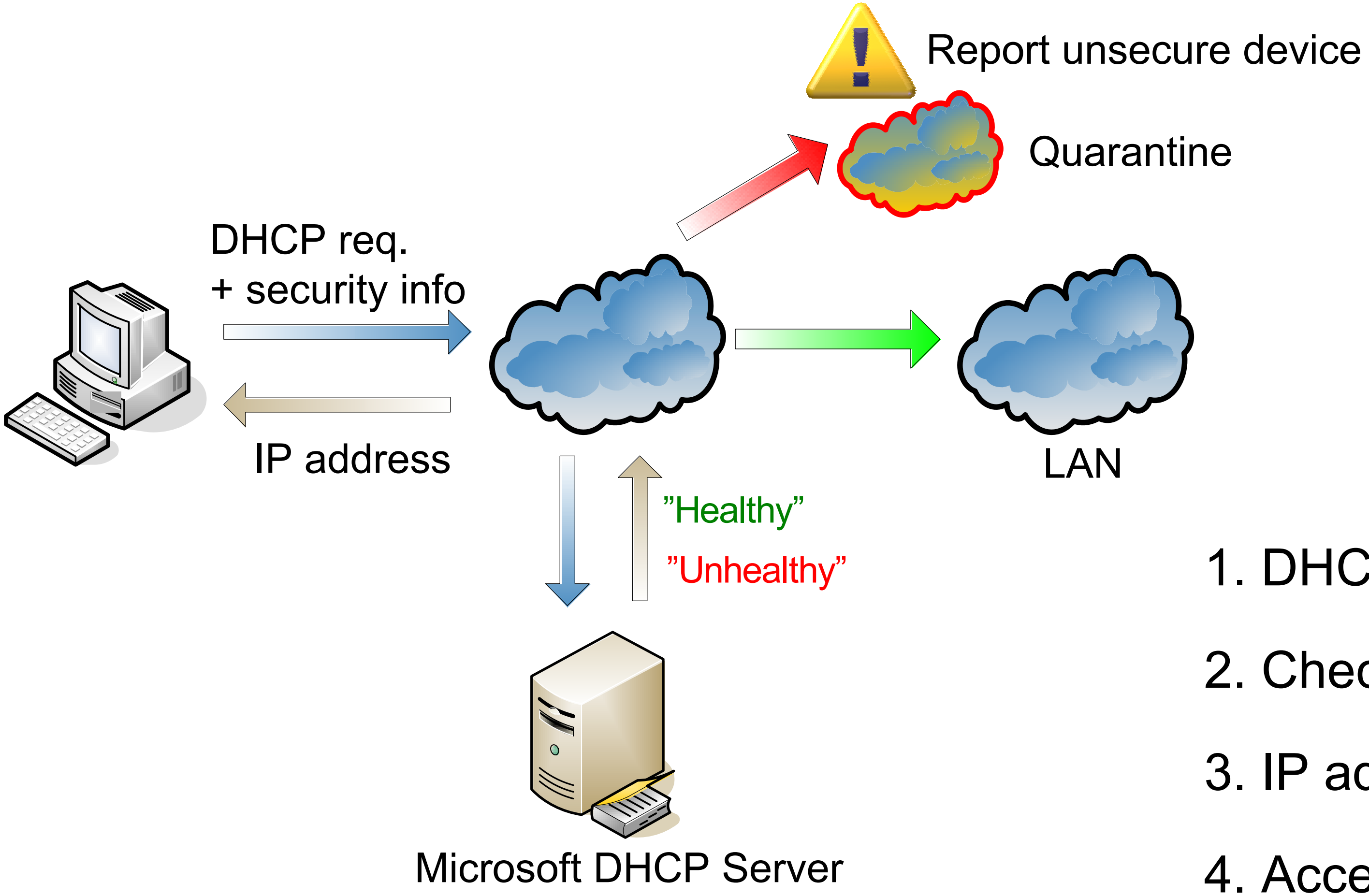
Microsoft – Network Access Protection – NAP

- New architecture to restrict the access of computers until their health can be verified
- The first version of NAP uses the DHCP-server service
- Inspect, assess, ensure compliance policy and remediate where possible on all Windows-based systems attempting to access the network
- The initial release of NAP will be delivered in the “Longhorn” release of Windows Server

Microsoft – Network Access Protection – NAP

- NAP is supported by Windows XP Service Pack 2 and Windows 2003 Server Service Pack 1
  - Other Windows OS's are being considered
- Should not be mistaken for Network Access Quarantine Control which ship with Windows Server 2003
  - based on client inspection with customer-written script to perform compliance checks for remote access connections like VPN and RAS

How does NAP works



1. DHCP Request
2. Check security
3. IP adr returned
4. Access

Microsoft ISA 2004 functions

- Available now
- VPN quarantining when the client is not compliant with the security policies
- Done with scripts

Microsoft NAP – Pros:

- No requirements for the network devices
- Relativly simple to implement
- Integrated into the Microsoft OS
  - No agents required

Microsoft NAP – Cons:

- Only support for Windows XP SP 2 and Windows server 2003 SP 1
- NAP is not released yet
- An infected system which is compliant to the security policy can still connect to the network
- If the compliance validation is only performed on DHCP request and renewal a non compliant system can be on the network for some time
- Problem if using static IP address

McAfee Trusted Connection – MTC

- A “soft” solution implemented by Rogue System Detection within ePolicy Orchestrator version 3.5 (August 2004)
- Automatically detecting un-managed systems on the network
  - One step to a more secure network

How does McAfee Trusted Connection work

- McAfee ePolicy Orchestrator (ePO) which manages McAfee products like VirusScan, McAfee Desktop Firewall ex. is the center of the solution
  - Uses agents for administration
  - The agent report MAC addresses of the system being administrated – and stored in an SQL database

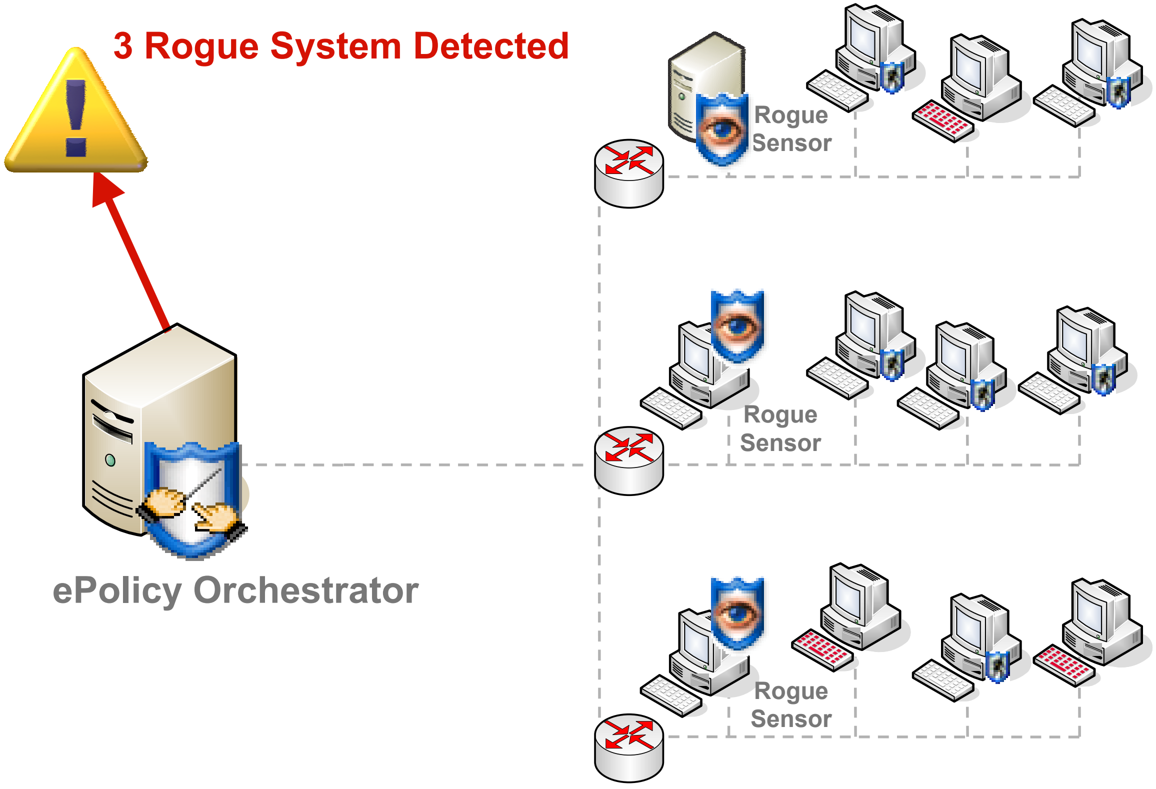
- Rogue sensors are deployed on each subnet
  - Listening for broadcasts
  - Reports the MAC addresses active on the net back to ePO

How does McAfee Trusted Connection work

- Un-managed system can now automatically be reported and remediation or exclusion can now be performed

- Need a “learning” period before it is effective
  - All solutions in this presentation needs a “learning” period

How does McAfee Trusted Connection work



McAfee Trusted Connection – Pros:

- No requirements for the network equipment
  - Host supported - Windows, Linux and Mac
- Relative simple to implement
- Support compliancy check on Windows
- Tested solution - has been released since August 2004
- Free if you already have ePO 3.5 or above implemented

McAfee Trusted Connection – Cons:

- Reporting only
  - Some automatic action/response can configured
- An infected system which has the ePO agent running can still connect to the network without any rogue system being reported
- No integration with Host IDS

A generic and simple solution

- Implement an automatic antivirus compliancy test on the network
- It can work if the antivirus software opens a management port on the hosts
- A port scanning tool can verify if the host runs Windows and has the antivirus management port open
  - If not = report the system as un-managed Windows systems

Intel Active Management Technology – AMT

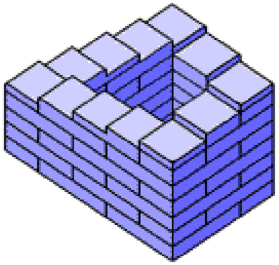
- A relative new technology for hardware and software asset management
- Embedded in the hardware
- Runs without any agents on the client
- Works even if the operation system does not work or is not running

Steps to implement Self-Defending Network

- Defining a security policy and verifying the compliancy

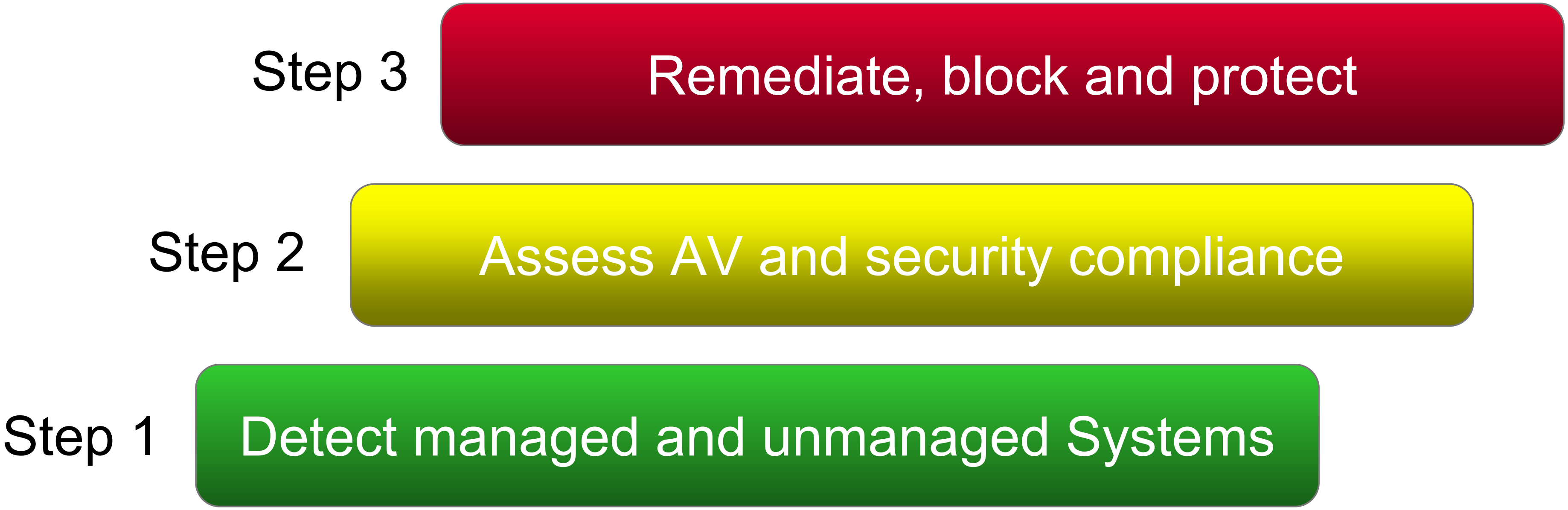
- Initial phase is primarily focused on anti-virus compliance
  - Bigger scope like security patches, unauthorized applications and other security applications

- The ultimate resilient Self-Defending Network can be a goal
  - Each and every step will improve security



3 Steps to a Self-Defending Network

- The 3 big steps into a more secure network



Step 3 Remediate, block and protect

Step 2 Assess AV and security compliance

Step 1 Detect managed and unmanaged Systems

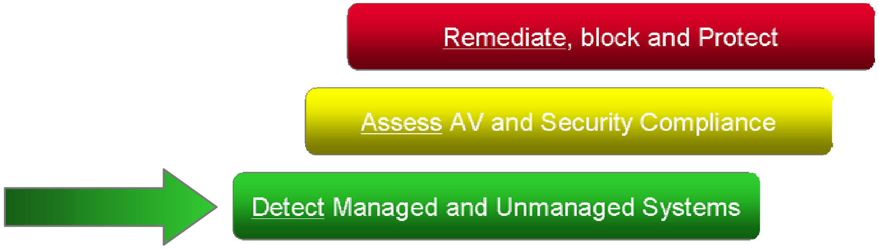
Steps to a Self-Defending Network

All the systems **connected** to the network are managed

- Report un-managed systems

All the systems **connecting** to the network are managed

- Report un-managed systems when they connect


Remediate, block and Protect

Assess AV and Security Compliance

Detect Managed and Unmanaged Systems

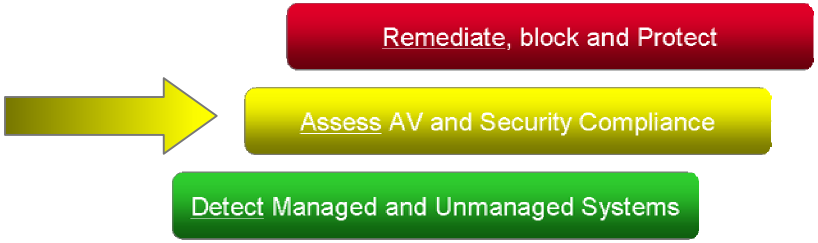
Steps to a Self-Defending Network

All the systems **connected** to the network are up-to-date with AV and OS patches

- Report systems which are not up-to-date

All the systems **connecting** to the network are up-to-date with AV and OS patches

- Report systems which are not up-to-date



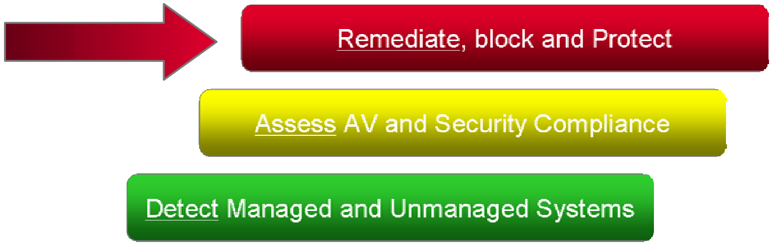
Remediate, block and Protect

Assess AV and Security Compliance

Detect Managed and Unmanaged Systems

Steps to a Self-Defending Network

Go from reporting to blocking / quarantining systems which are not compliant



Remediate, block and Protect

Assess AV and Security Compliance

Detect Managed and Unmanaged Systems

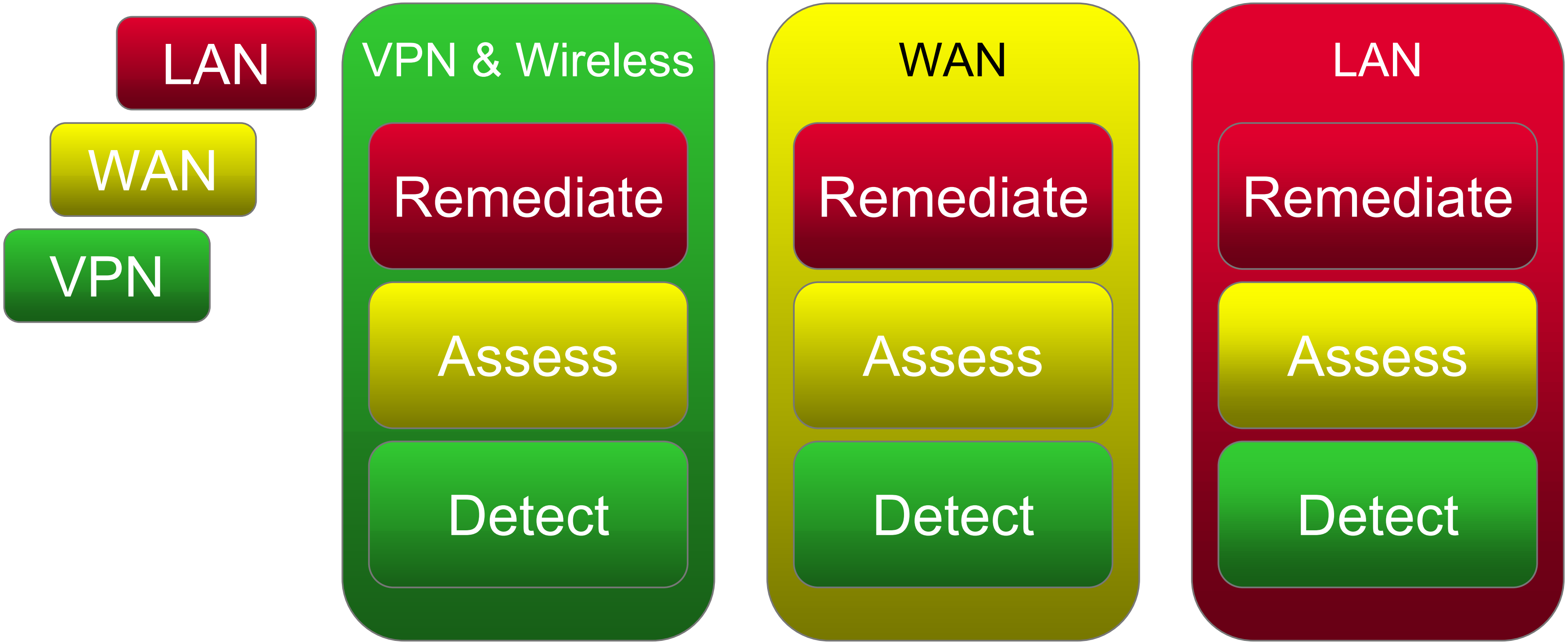
Steps to a Self-Defending Network

Implement Host Based Intrusion Detection – Intrusion Prevention System / behavior monitor running on the host. If unsafe activity is reported on the system it can be quarantined until the source or reasons have been determined

Implement Network based Intrusion Detection – Intrusion Prevention System unsafe network activity is reported and systems can be quarantined until the source or reasons have been determined

VPN, WAN and LAN

- Implement in steps: first on VPN and Wireless connections then WAN links and then systems on the internal network



The first steps

- It is not a silver bullet
- Do not rush the implementation
- Use the technology and step by step implement more and more Self-Defending functionality into the infrastructure and your network will become more resilient

Conclusion

- By building and maintaining a resilient infrastructure, security and IT operations leverage each other's expertise to prevent attacks and preserve business continuity. On a practical basis, that means an organizations is better able to *understand* its information environment, *act* to successfully address both vulnerabilities and opportunities, and *control* IT resources to proactively manage risk and keep business up and running.
- Of course, building an environment that is completely resistant to disruption is impossible, given the complexity of the IT environment and the changing threat landscape. But by building a resilient infrastructure, companies can better manage and mitigate risk and preserve their business continuity.

- Gartner Says: By 2005, enterprises that don’t enforce security policies during network logon will experience 200% more network downtime than those who do. (0.7 probability)
  - *Scan, Block and Quarantine to Survive Worm Attacks, Gartner, Jan 2004*

- By the end of 2007, 80% of enterprises will have implemented network access control policies and procedures.
  - *Protect Your Resources with a Network Access Control Process, Gartner, Dec 2004*

Thanks to

Questions ?

steen.pedersen@ementor.dk