

---

# **CSN27: Automated GRC Policy to Proactively Counter Cyberthreats**

Daniel Conroy

Managing Director, CISO and Global Head of Information Security

Bank of New York Mellon

# Technology Risk Management – Information Security

---

## **Executive Summary**

- Integration of network access control with the ArcSight SEIM platform can provide greater insight into process flaws across the network.
- Threats from insiders, Cybercrime, and sabotage represent the greatest concern to our company. Removing the burden of manually monitoring these daily issues allows our team to focus on more proactive measures.
- Our information security infrastructure has been enhanced to identify emerging threats with the implementation of new tools as part of the overall risk mitigation strategy.

# Goals & Drivers for GRC

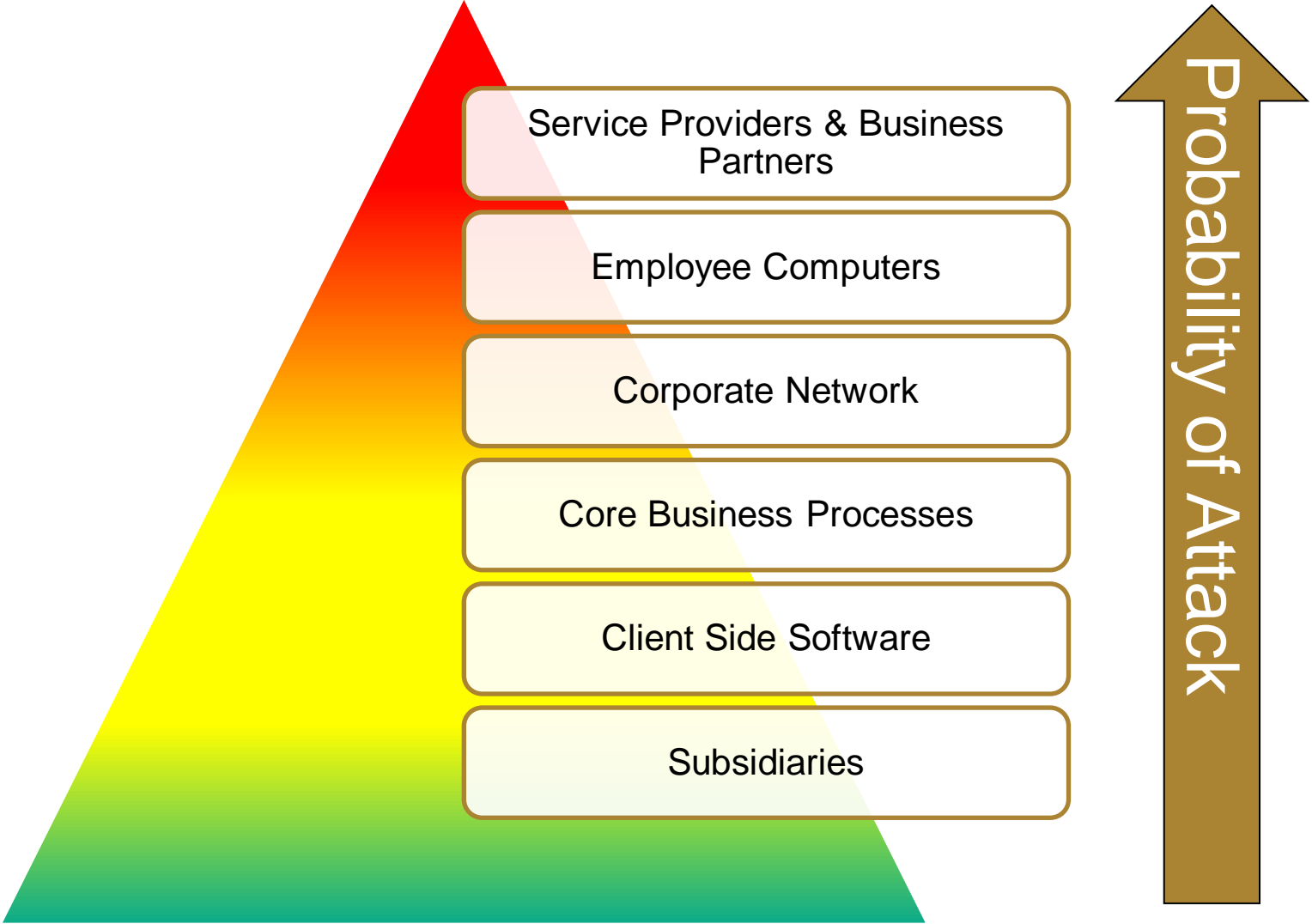
## Goals

- Implement policies and controls
- Satisfy compliance obligations
- Gather information to proactively run the business
- Create a nervous system that helps us manage our business more effectively
- Derive a competitive advantage from understanding risks

## Drivers

- Inaccurate financial reporting damages the financial system
- Failing an audit, which must be reported in public financial statements
- External and internal scrutiny
- Private companies sold to public companies
- Managing dramatic growth, costs and associated risks
- High volume of compliance

# Threat Vectors



# 2010, 2011 and Beyond

## 2010

### Detection:

- Anti-Virus installed
- Anti-Virus definition up-to-date
- Peripheral device protection installed
- Laptop encryption installed
- “Patch Now” Microsoft patches

### Automatic blocking:

- Anti-Virus not installed
- Anti-Virus not up-to-date
- SMTP mail traffic
- Skype
- Bridged networks in Chennai

## 2011 & Beyond

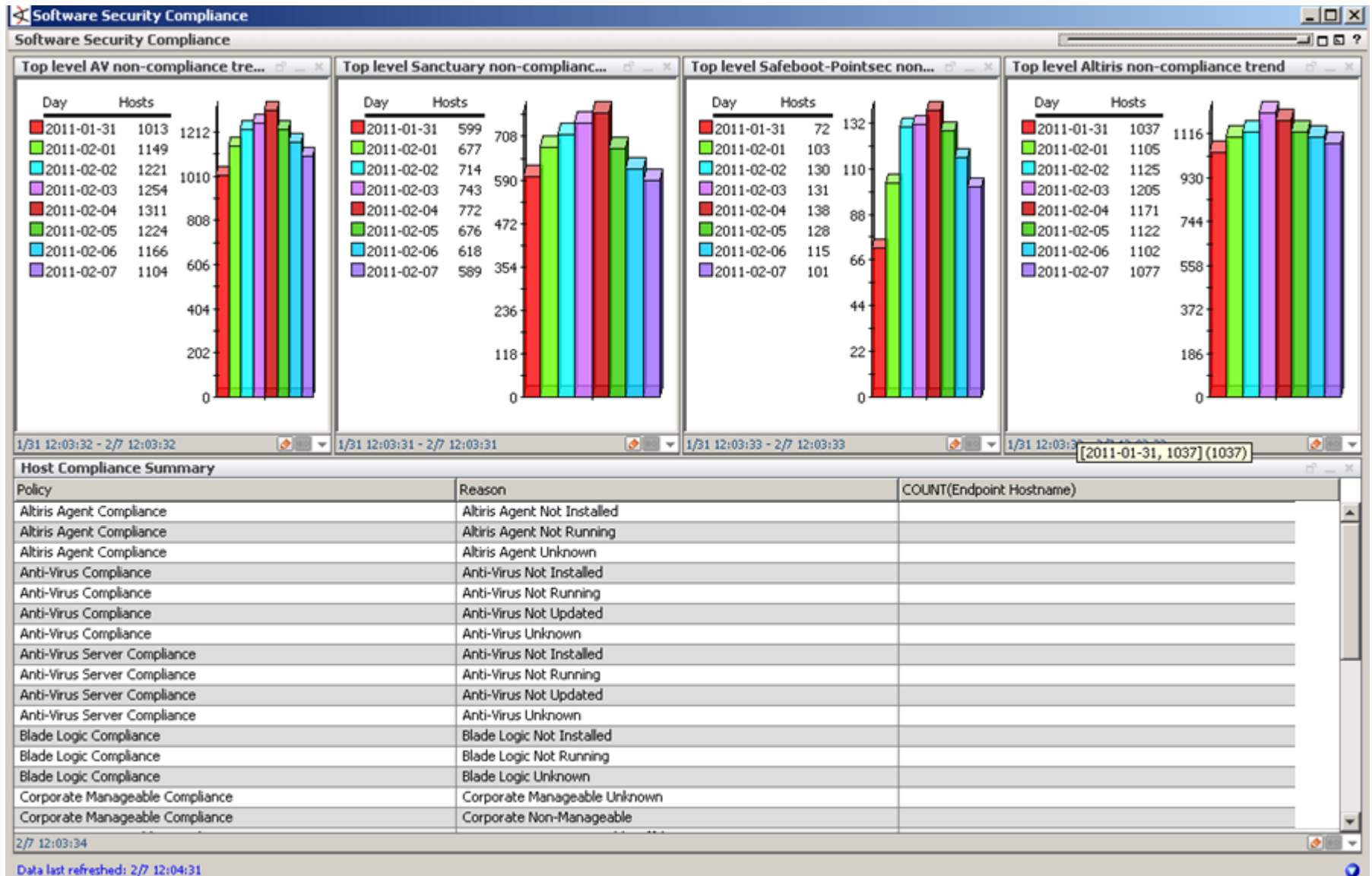
### Automatic blocking:

- Infected machine detection
- Server added to the DMZ that has not been approved
- Expanding auto-blocking of bridged networks
- Expanding to all P2P software

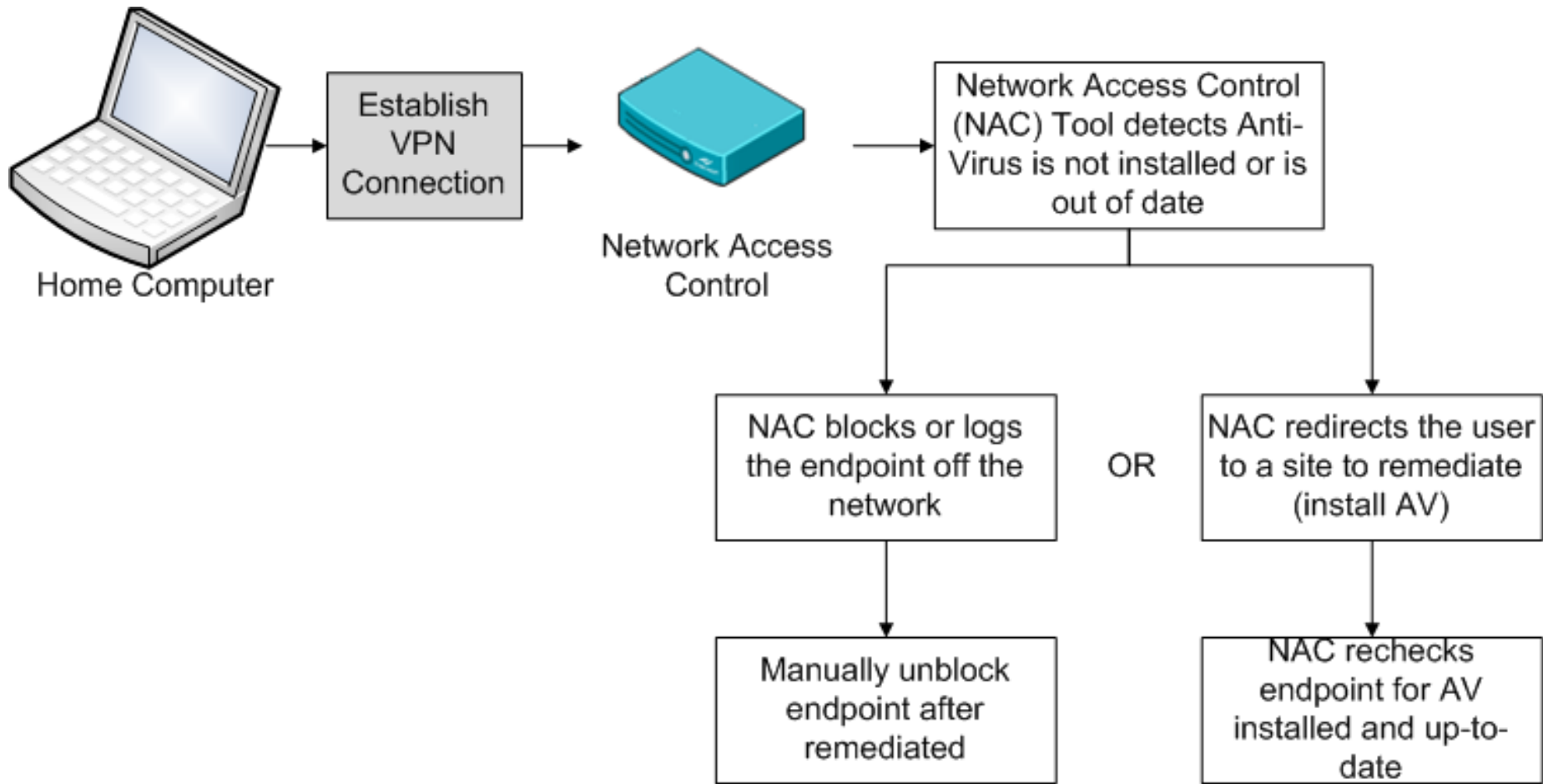
### Automatic hijacking:

- Non-BNY Mellon assets that connect to the internal network that have not yet registered
- Non-BNY Mellon assets that connect to the internal network and do not have Anti-Virus installed or up-to-date
- Segmentation of divested businesses

# Example of Risk Management Dashboard



# Automated Device Interrogation & Blocking – Infected Machine



# Automated Device Interrogation & Blocking – Infected Machine

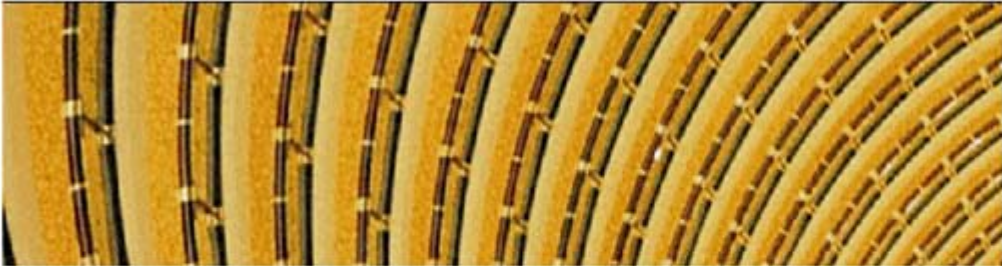
ForeScout Technologies: Assets Portal - Windows Internet Explorer

http://10.253.3.5/status?z=1671452449

SnagIt

ForeScout Technologies: Assets Portal

Information Risk Management  
Monday, July 25, 2011



IP Address: 10.1.91.122

## Message

Dear D101TEC06E5108,

The Bank of New York Mellon has been unable to detect a valid Antivirus software installed and running on your PC, as required by corporate policy.

To keep our information assets secure, all computers must have antivirus software to remain connected to the network. Please take the appropriate steps necessary to remediate this issue.

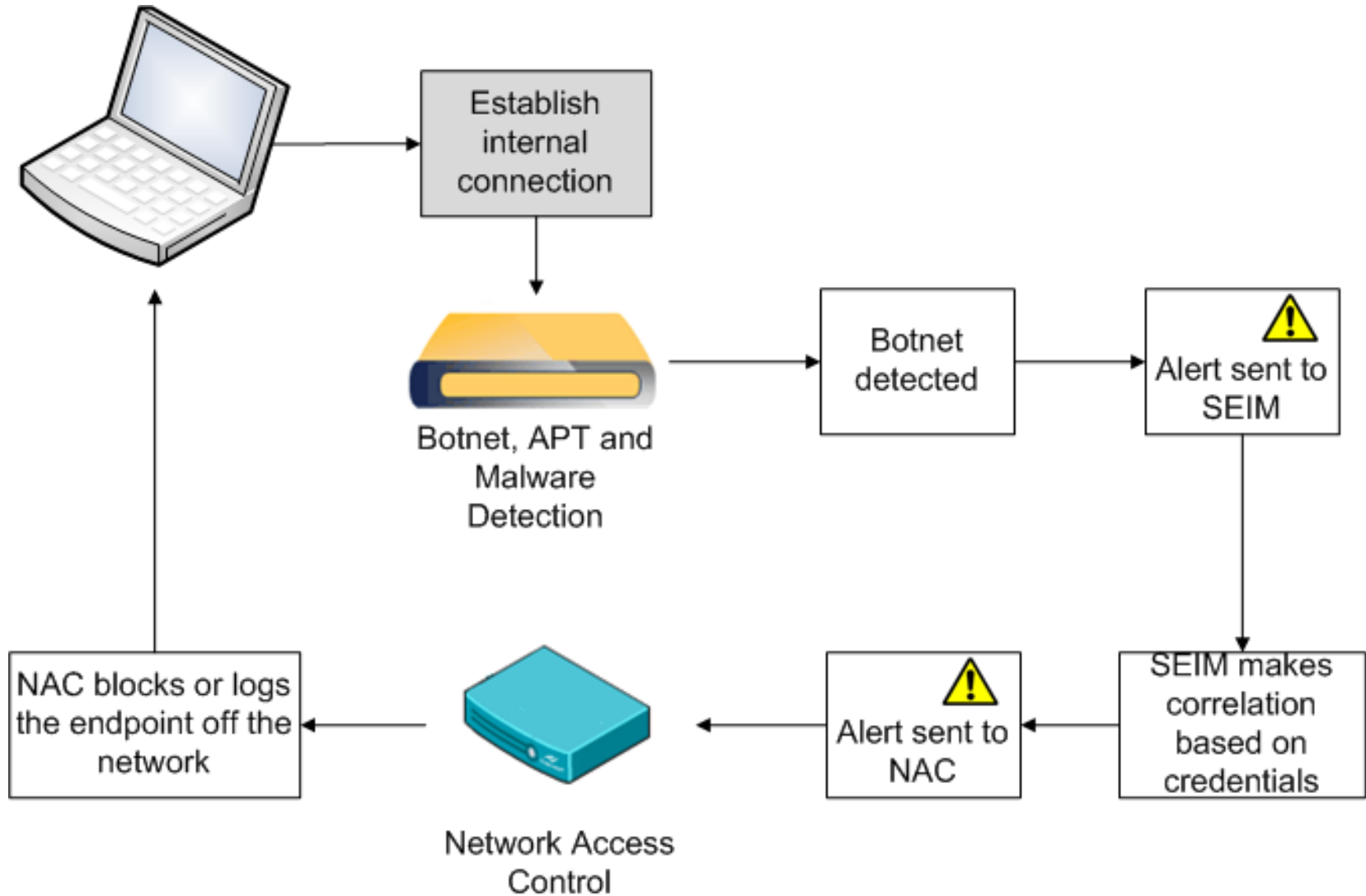
If you have any questions or concerns, or are a BNYM employee, please contact the CSD Helpdesk at 1 888 635 5666 [US] / 44 207 163 4357 [Int] and a technician will be happy to help you.

MCM users should contact MCM IT Helpdesk (415-975-2399)  
iNautix users should contact ServiceIT @ 4000/2000

Please note that your workstation has been firewalled from the network. You will not have access to network resources such as internet and email until this has been addressed.



# Automated Device Interrogation & Blocking – Botnet Detected



# Automated Device Interrogation & Blocking

## – Botnet Detected

End Time	Device Event Class ID	Device Custom String2	Source Address	Application	Destination Dns Domain	VPNUser.ExternalAd	VPNUser.UserName
25 Jul 2011 08:59:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1	DNS	ka18i7gah10.com		
25 Jul 2011 08:59:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1	DNS	ka18i7gah10.com		
25 Jul 2011 08:59:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:48:59 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:48:59 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:48:59 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:48:59 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:38:34 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:38:34 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:38:34 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:38:34 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:35 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:35 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:35 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:35 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:35 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:37:21 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:28:08 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:28:08 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:28:08 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:25:45 EDT	Compromised host	TDL/TDSS Gang	167.113.1				
25 Jul 2011 08:25:45 EDT	Compromised host	TDL/TDSS Gang	167.113.1				

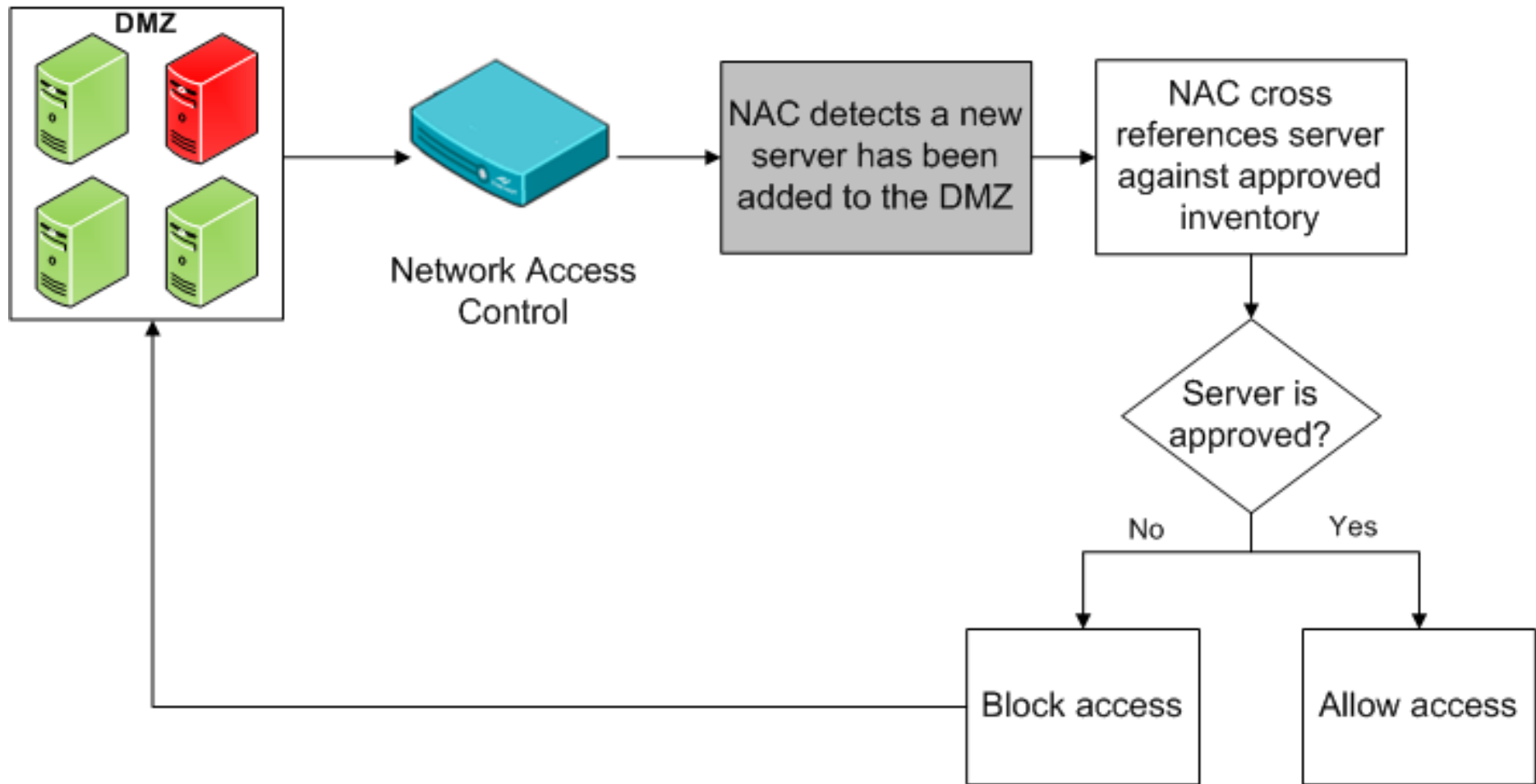
- Show Event Details
- Correlation Options
- Investigate
- Debug Filter...
- Active List
- Annotate Events... Ctrl+T
- Mark as reviewed Ctrl+R
- Select Events with Matching Cell
- Invert Selection
- Event Graph
- Rule Chain Graph
- Geographic View
- Integration Commands
- Tools
- Export
- Add to Case
- Print Selected Rows

- New Configuration ...
- Get Source User Info
- Nslookup (Linux)
- Nslookup (Windows)
- Ping (Linux)
- Ping (Windows)
- Traceroute (Linux)
- Traceroute (Windows)
- Web Search
- Whois (Linux)
- Whois (Windows)
- Block through ForeScout ...
- Logger Quick Search ...
- Logger Search ...

96.248.		x	5j
96.248.		x	5j
96.248.		x	5j
96.248.		x	5j
96.248.		x	5i

# Automated Device Interrogation & Blocking

## – New Server in DMZ

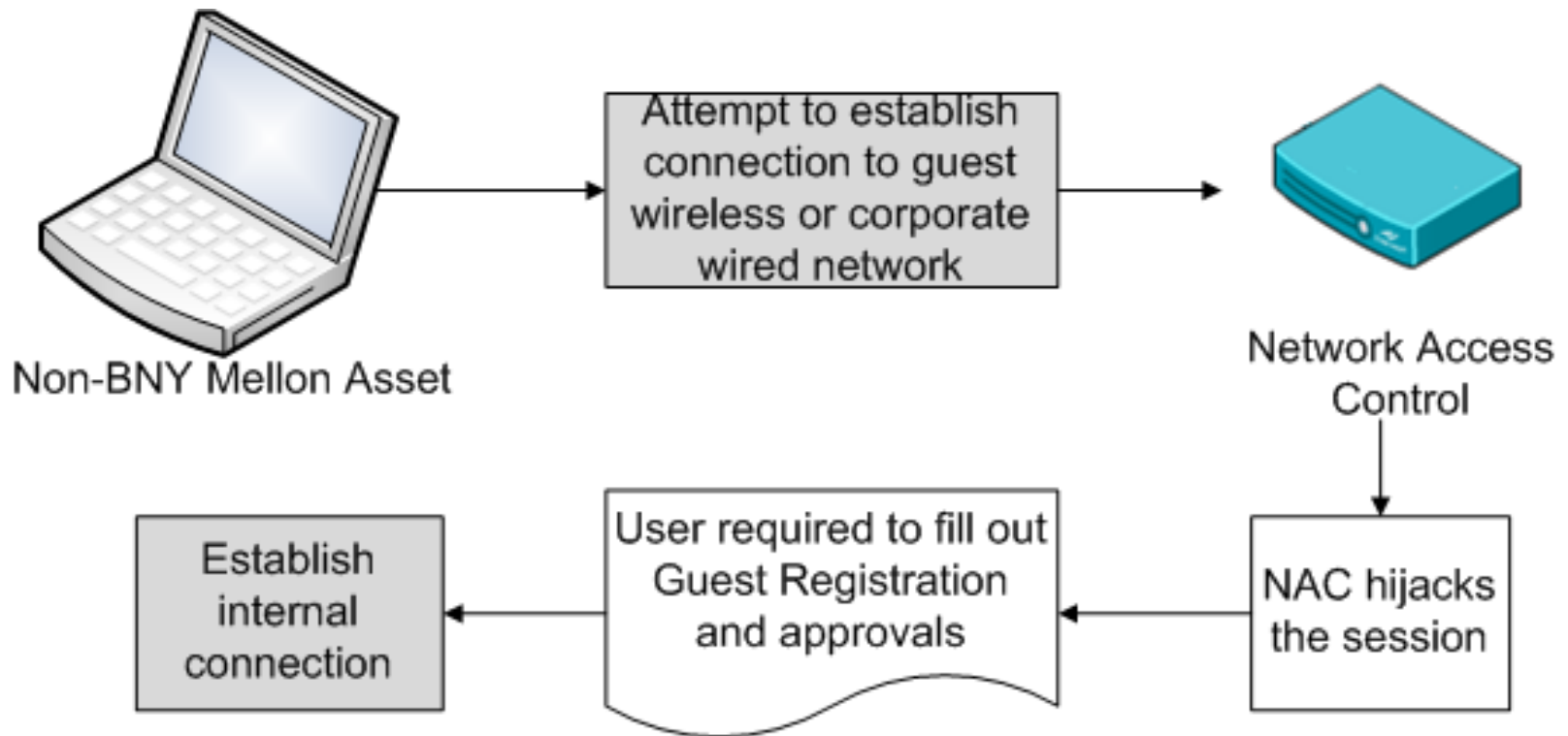


# Automated Device Interrogation & Blocking

– New Server in DMZ & Web Application Assurance Group (WAAG)

- Reviews all externally and internally accessible hosted sites
- Integrates key players from multiple functional areas, in an informative or approval method
- Ensures changes do not expose BNY Mellon to risk associated with new or modified content or code
- Approves changes as a whole end-to-end committee

# Automated Device Interrogation & Blocking – Guest Registration



# Automated Device Interrogation & Blocking

## – Guest Registration

10.15.  Hide Offline  Show only unassigned 98%

Online	Host	Host IP	Segment	Groups	MAC Address	Display Name
	WORKGROUP	10.15.		Firewalled guests, Guest Hosts - Mac, Macintosh		

---

**All policies** Host info

IP Address: **10.15.**      NetBIOS Hostname:      MAC Address:

**Policy: Asset Classification. Status: Match. Sub-Rule: Macintosh. Since: July 08 07:25:13 PM.**

**Match Main Rule**

Condition Properties: None

Actions:                  None (No actions defined for this rule)

Sub-Rules:

- Unmatch NAT devices
- Unmatch Windows Servers
- Unmatch Windows
- Unmatch Printers
- Unmatch Linux/Unix
- Match Macintosh**
  - Condition Properties: NIC Vendor:      APPLE COMPUTER  
MAC Address:  
OS Fingerprint:      *Irresolvable*  
Network Function: *Irresolvable*
  - Actions:                  Add to Group: Macintosh
- N/A*
- N/A*

The host is not inspected by the remaining sub-rules because it matches *Macintosh*

7. *N/A*      *Cisco VPN Client*

8. *N/A*      *Cisco Routers & Switches*

# Automated Device Interrogation & Blocking – Guest Registration

ForeScout Technologies: Assets Portal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ForeScout Technologies: Assets Portal

Information Risk Management  
Monday, July 22, 2011

Guest Registration

IP Address: 10.1.

Dear User,

You are attempting to connect to The Bank of New York Mellon's corporate network with a device that is not registered or not compliant with our security standards.

Before continuing, please register this device by filling out the form and clicking on register button below.

**Note: You will need to identify your Bank of New York Mellon's contact name and contact email address.** If you are a Bank of New York Mellon employee and received this message in error, please fill out the appropriate fields and list your own email address in the contact email address field.

For questions or concerns please contact IRM (Information Risk Management) at 212-815-5108 or 615-457-5137.

[BNYMellon Information Security Policy Directory](#)

\* Full Name

\* Phone

\* Email address

\* Company

Title

Location

Comment

\* Contact Email

\* Contact Name

BNY MELLON

# Benefits of Risk Management Automation

- Enablement and automation of enterprise risk management across lines of business.
- Automation of desktop remediation, cost savings realized
- Greater compliance of desktop to corporate standard
- Correlation between asset inventory and actual
- More secure guest access to the network
- Greater visibility, alerting of potential intrusions, infections
- Leverage the vast data environments in your organization including ERP, e-mail systems, spreadsheets, and documents.
- Alignment of the risk management strategy with corporate strategy.
- Real time information allows for better decision making while evaluating key risk factors.



Questions?

---

*Thank You!*