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

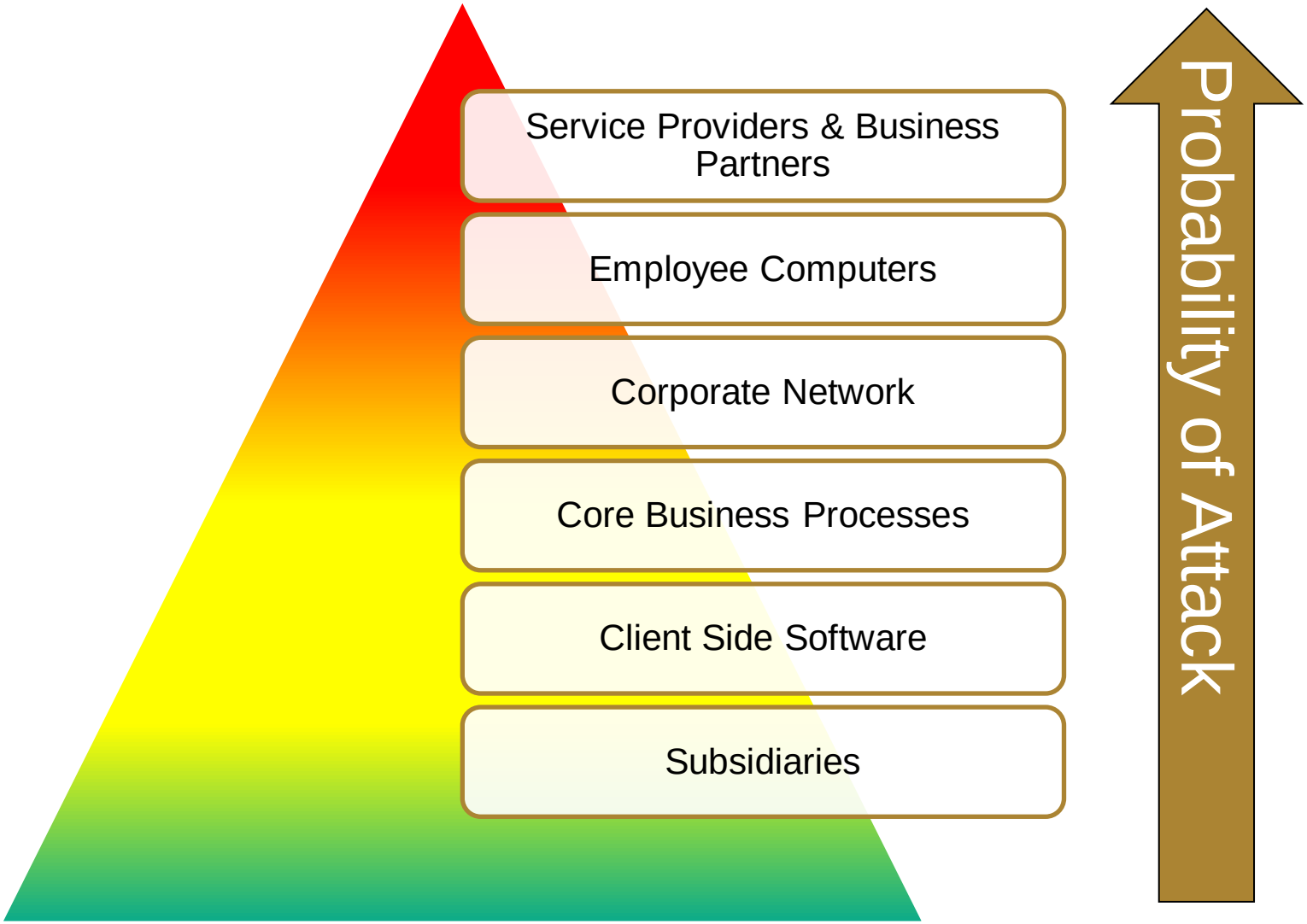
Goals

- 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

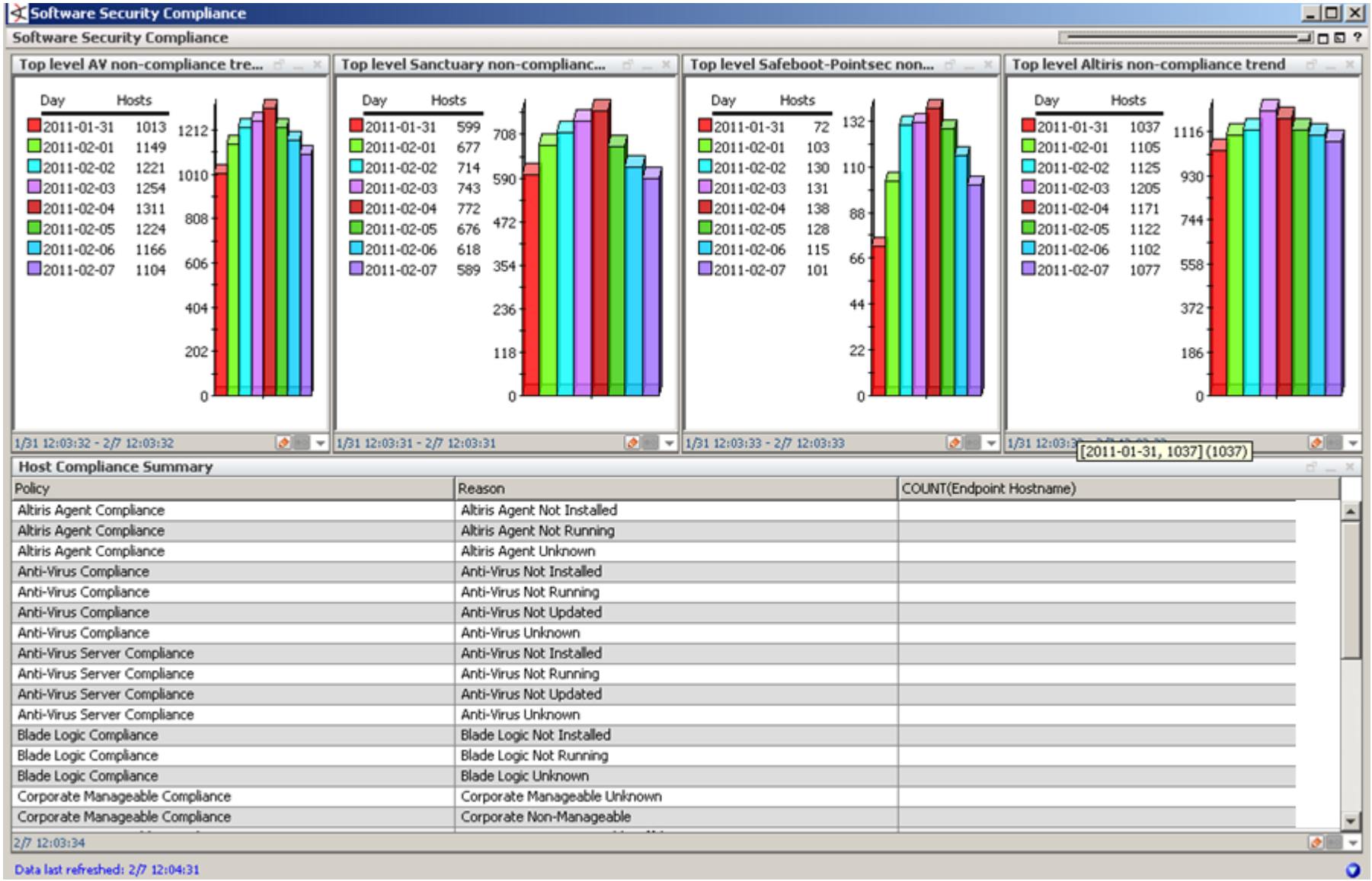
Automatic blocking:

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

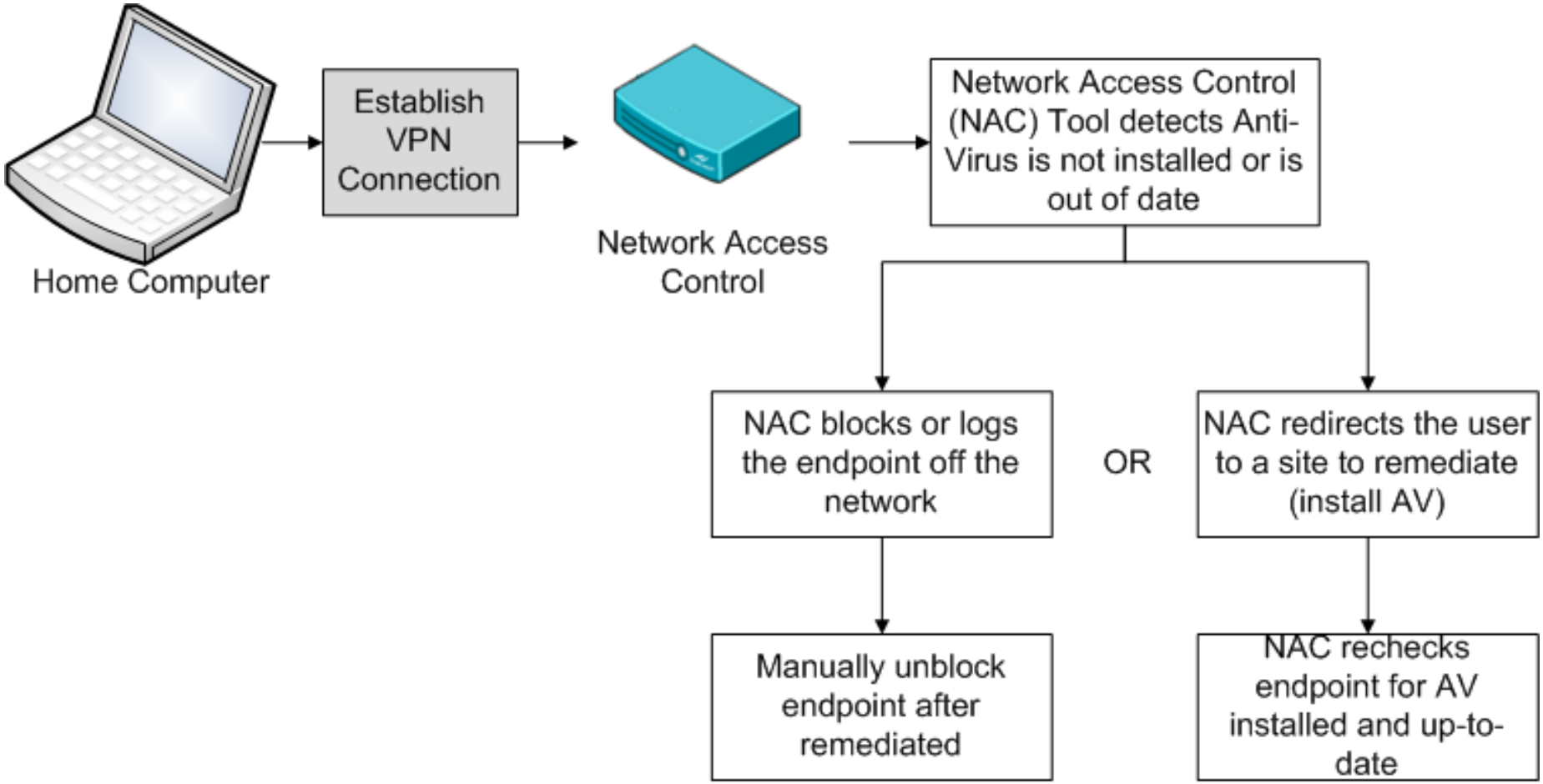
Automatic hijacking:

- 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

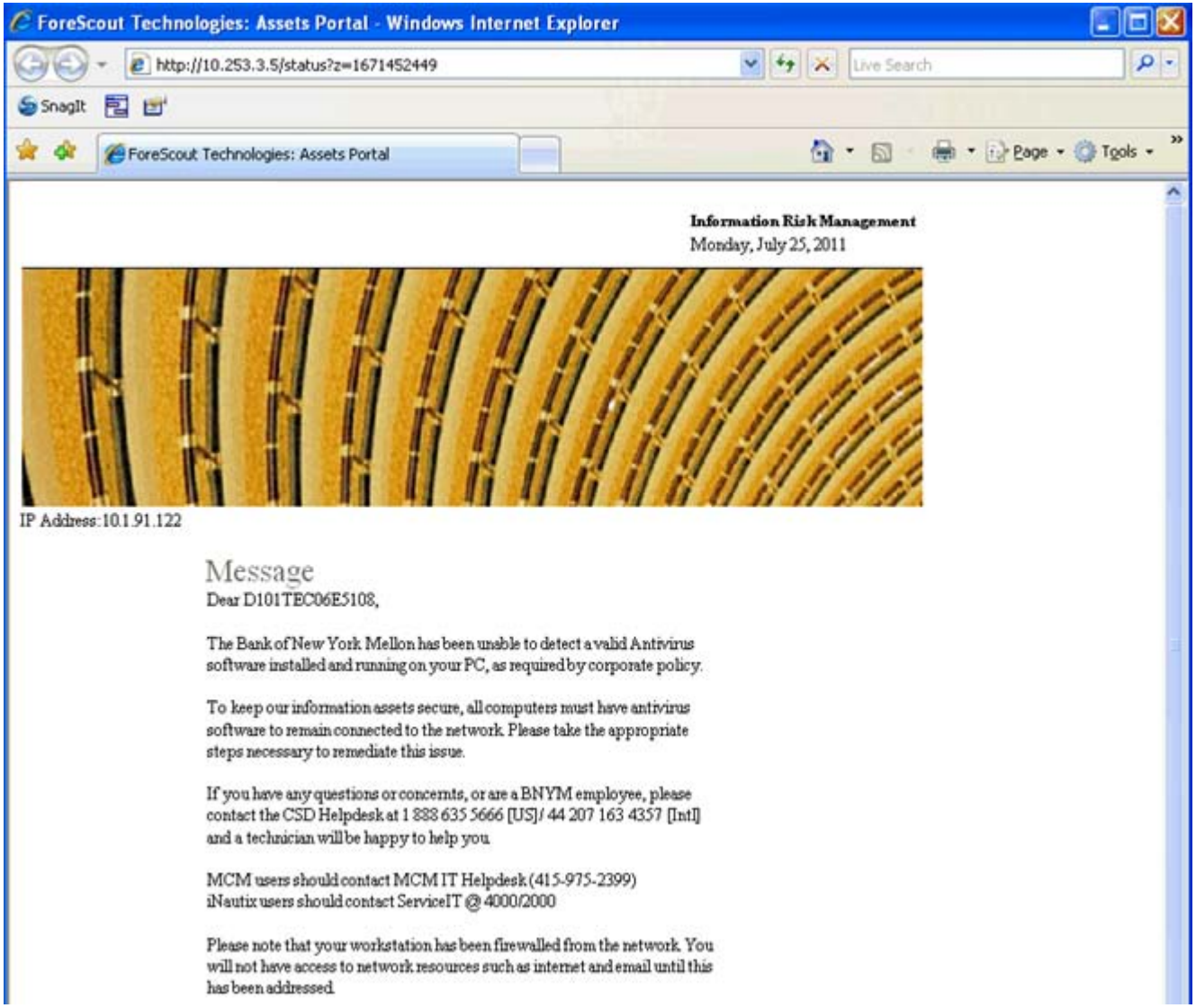
Example of Risk Management Dashboard



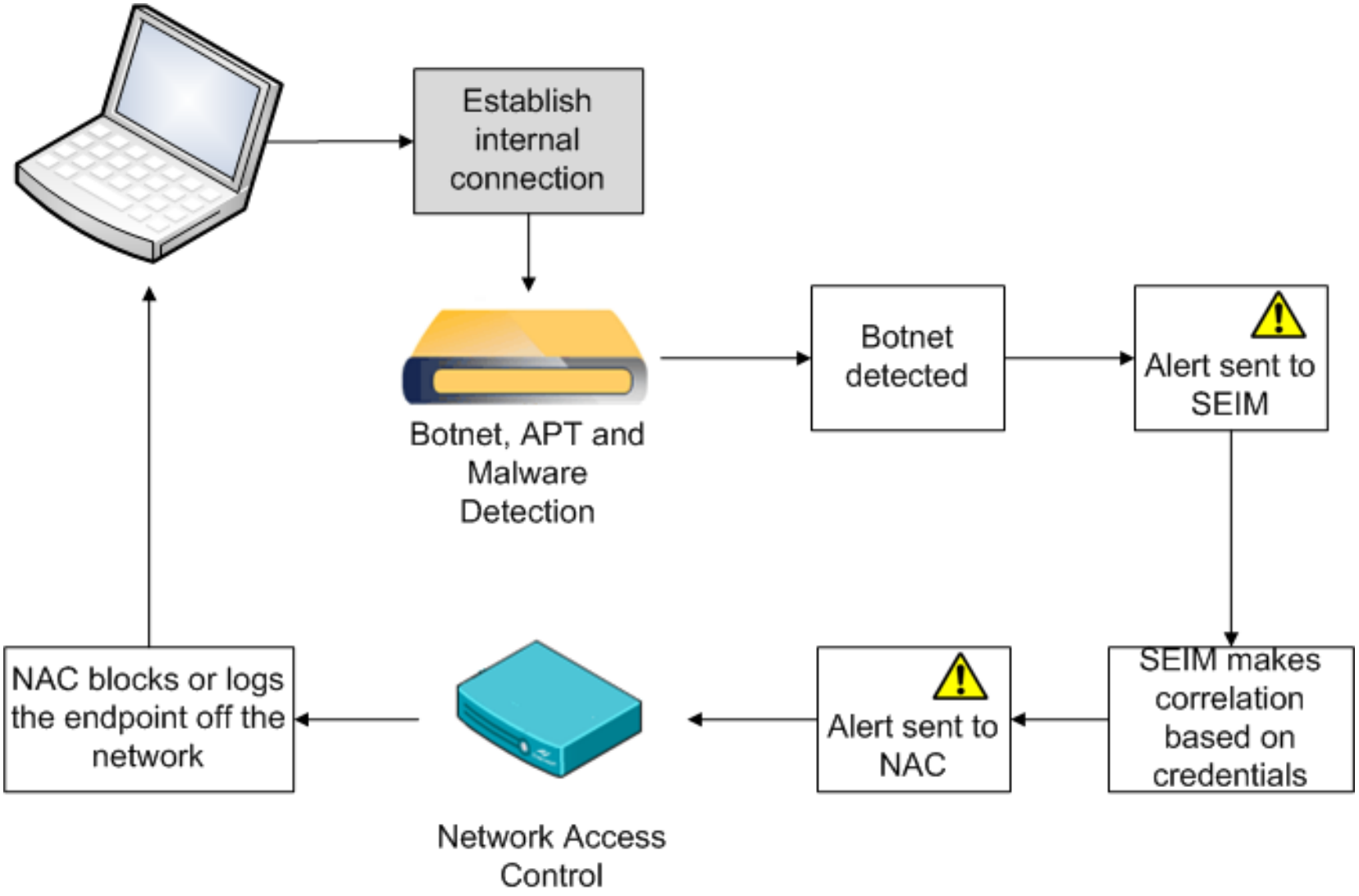
Automated Device Interrogation & Blocking – Infected Machine



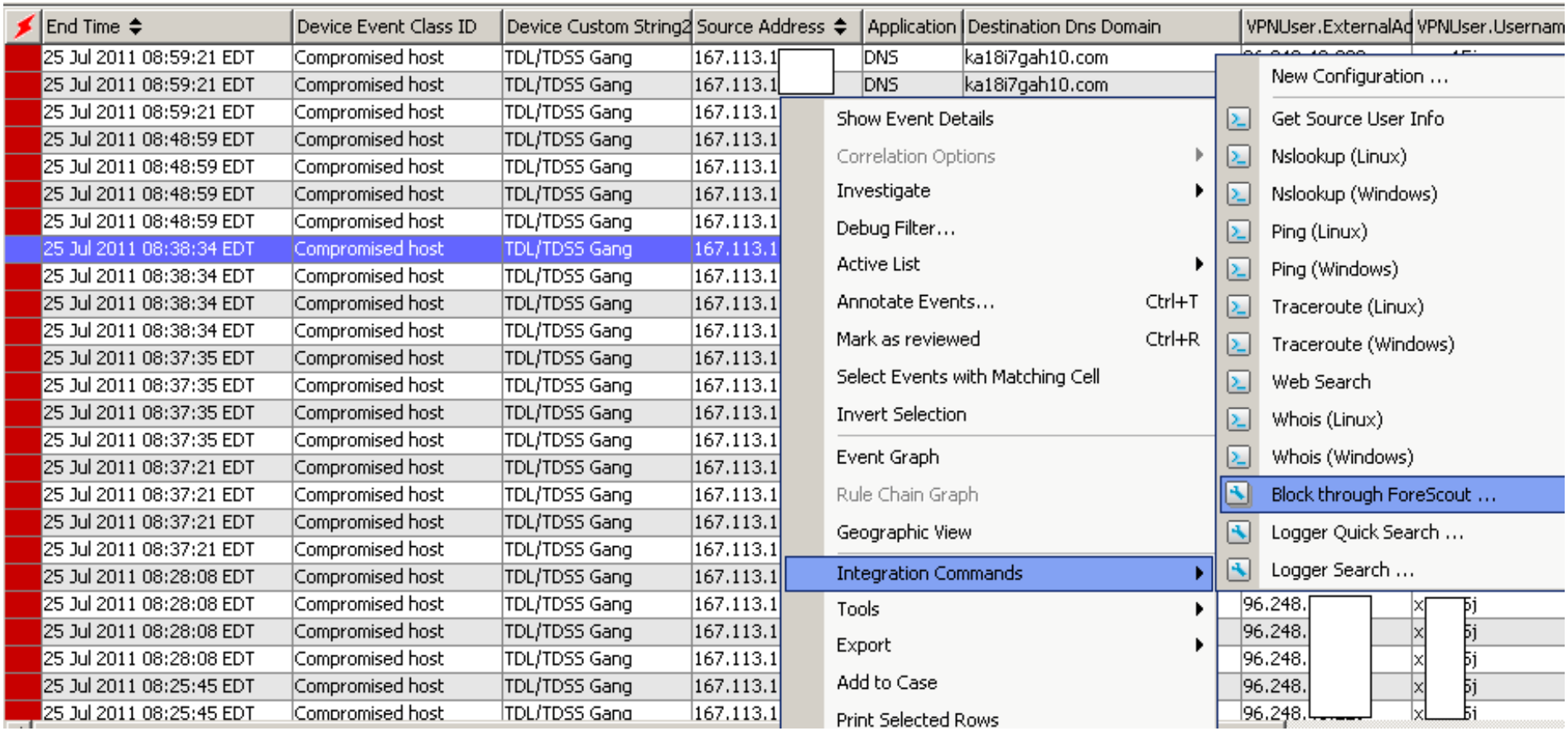
Automated Device Interrogation & Blocking – Infected Machine



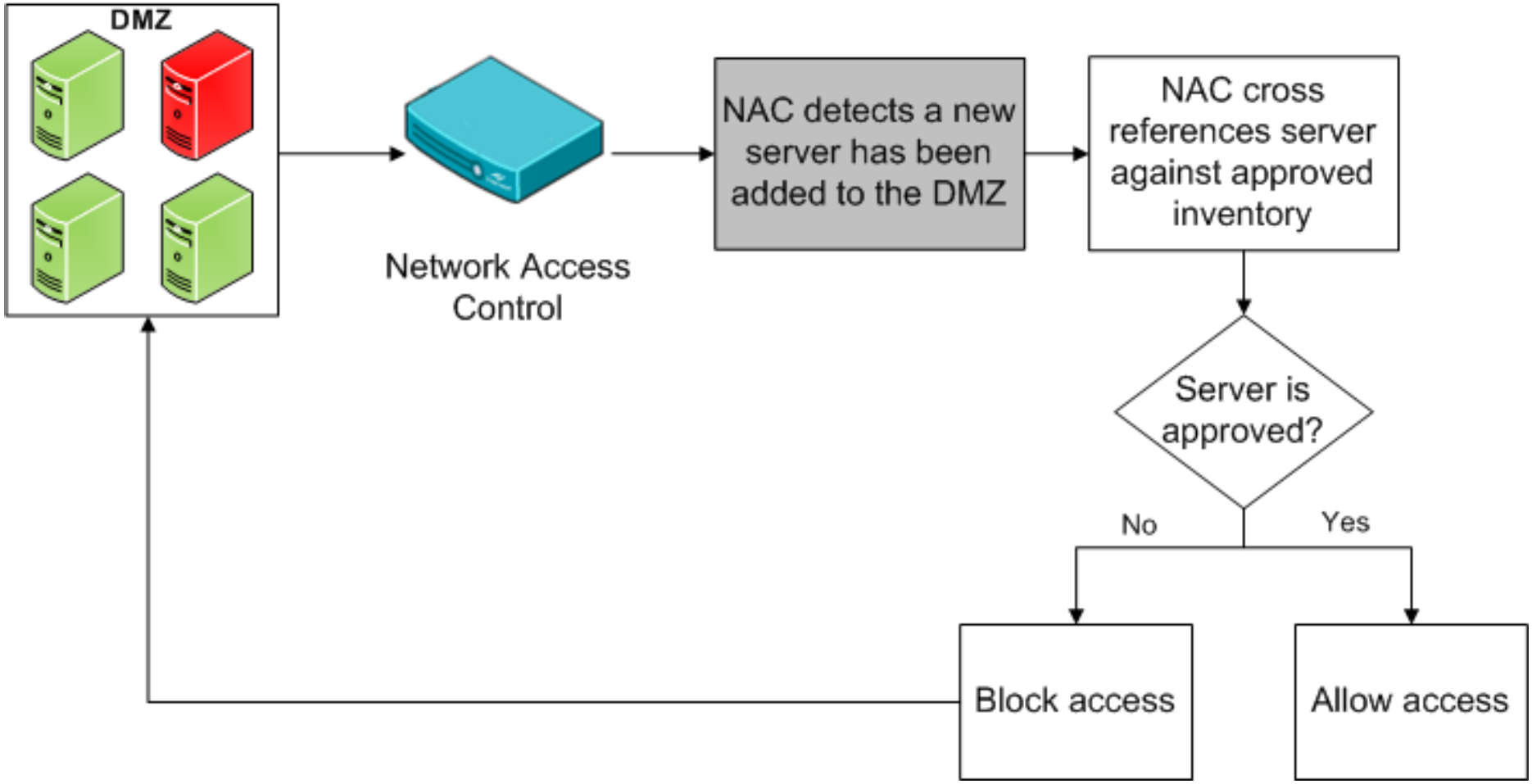
Automated Device Interrogation & Blocking – Botnet Detected



Automated Device Interrogation & Blocking – Botnet Detected



Automated Device Interrogation & Blocking – New Server in DMZ

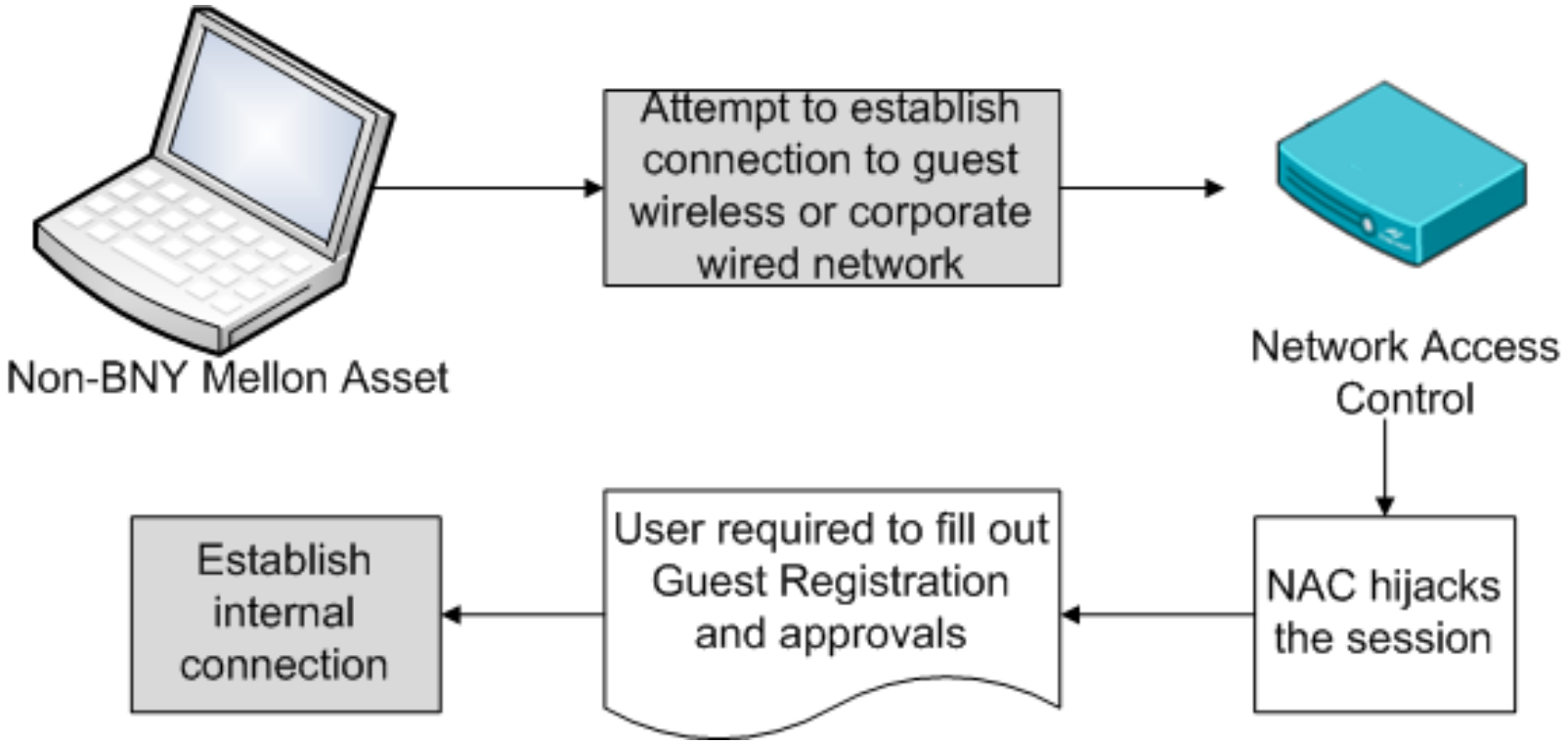


Automated Device Interrogation & Blocking

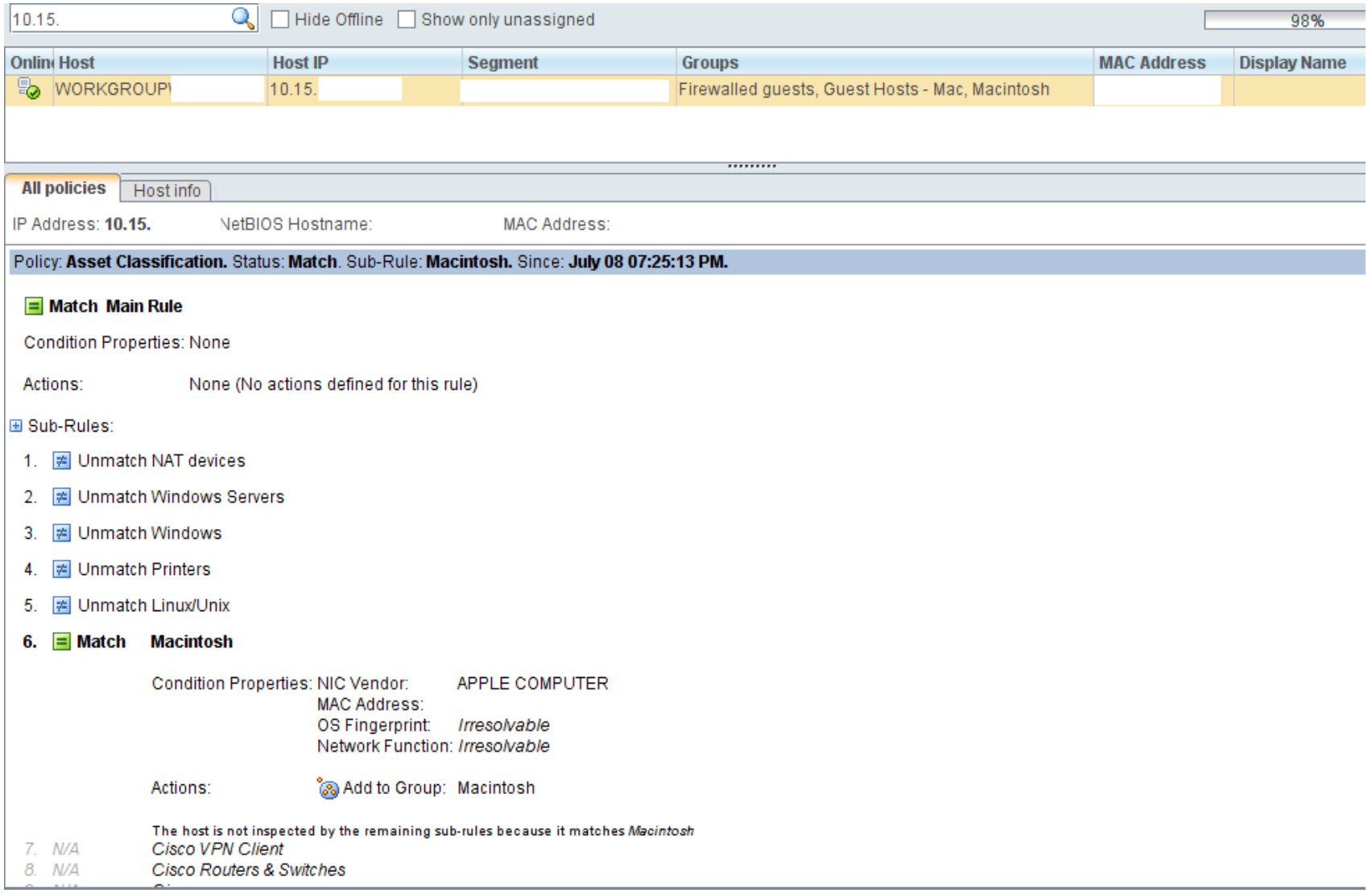
– New Server in DMZ & Web Application Assurance Group (WAAG)

- 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

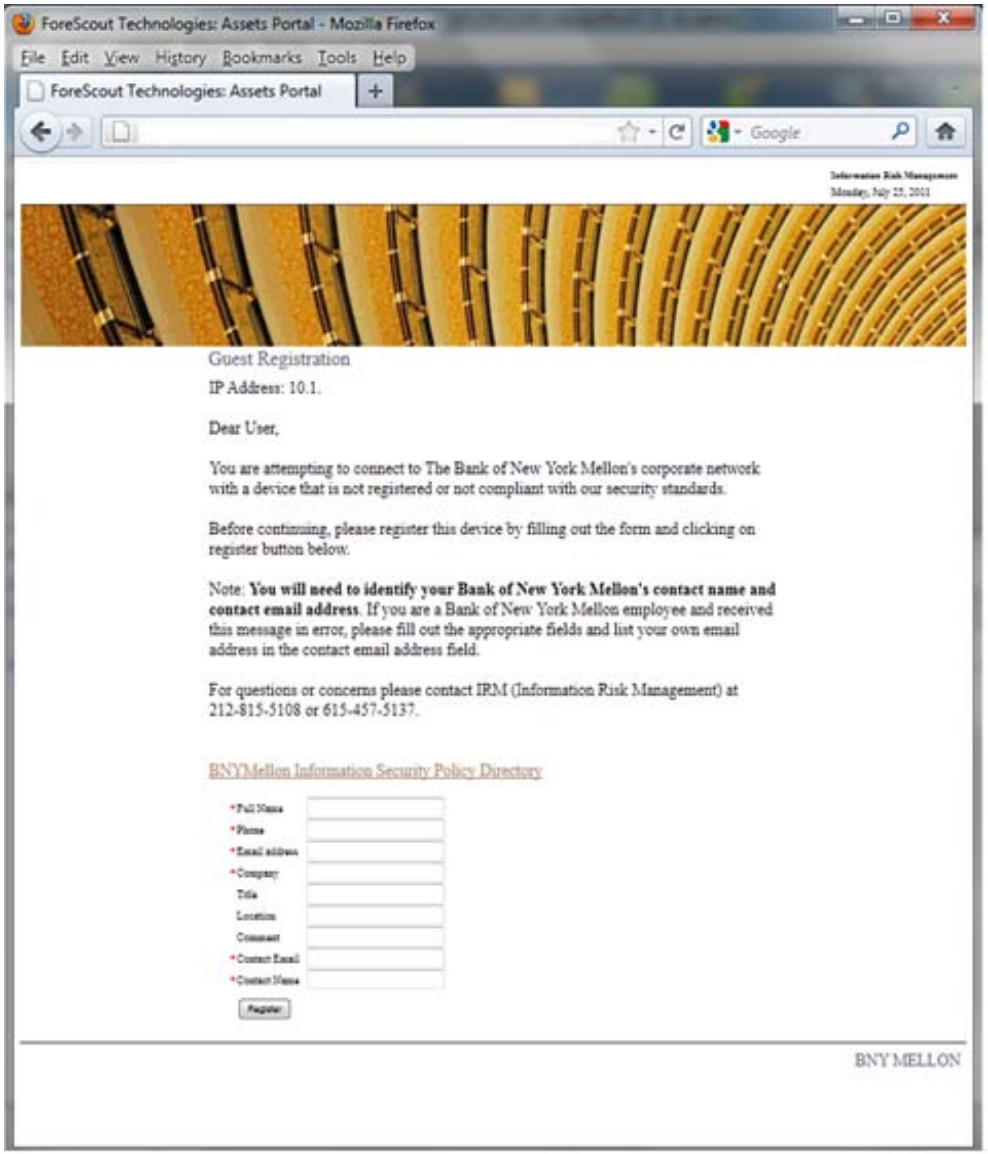
Automated Device Interrogation & Blocking – Guest Registration



Automated Device Interrogation & Blocking – Guest Registration



Automated Device Interrogation & Blocking – Guest Registration



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!