Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation

September, 2010

Agenda

- Triumfant Introduction
- SCAP Implementation Basics
- Security Configuration Management
- Vulnerability Scanning
- TNC Implementation

Introduction to Triumfant

Triumfant is an endpoint security and configuration management solution that is differentiated by the ability to:

- Use change detection coupled with patented analytics to detect the malicious activity that evades other defenses
- Build a surgical and contextual remediation to address detected problems
- Continuously enforce configurations and policies
- Deliver fine-grained reporting and analytics against the endpoint population with minimal intrusion

Triumfant

Why Triumfant is Different

Differentiator	Why It Matters
Change detection triggers analysis	Eliminates need for prior knowledge, makes detection attack agnostic
Deep, continuous monitoring	Assumes nothing, monitors everything, detects all changes
Contextual Analytics	Critical intel to analyze attacks, correlate all damage, and build a remediation
Automated Remediation	Eliminates coding and re-imaging, continuous enforcement
Donor Technology	Addresses the missing/corrupted attribute problem by turning the pop. into a donor

How it Works

Continuously scans for changes

- Elemental indicator of problems or attacks
- Eliminates need for prior knowledge
- Immediately triggers analysis for suspected malicious attacks

Analyzes detected changes

- Builds and then leverages learned context of broader population
- Categorizes: benign, anomalous, malicious
- Correlates changes into broader incidents

Takes appropriate action

- Builds a remediation for each incident
- Creates alerts, powers situational awareness
- Integrates with other tools in the ecosystem

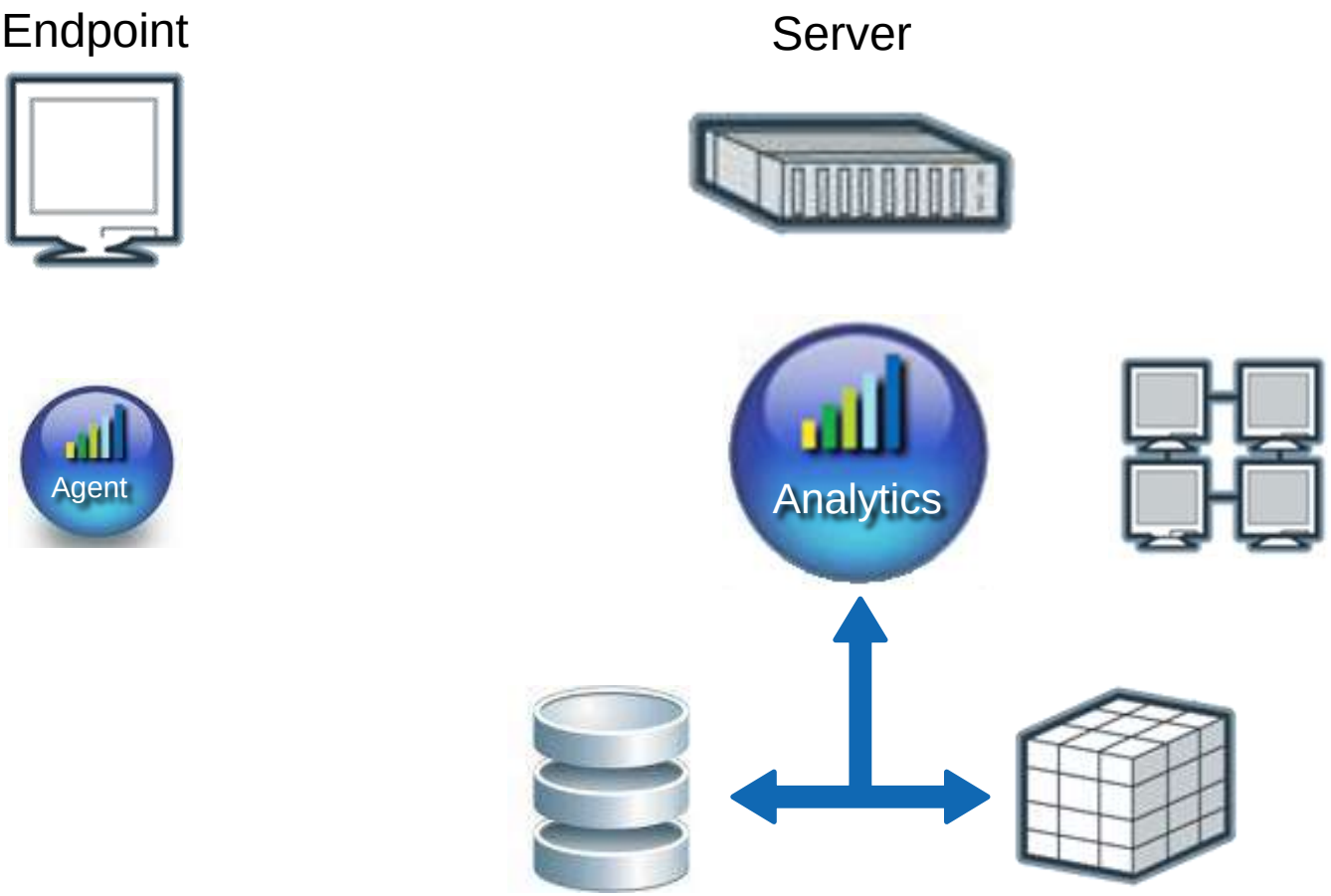
Triumfant

Triumfant and SCAP

- Early mover in SCAP integration
- Third (or so) product NIST SCAP FDCC Validated Scanning Tool
- Only tool with fully automated remediation
- Strikes balance between performance and data currency

Triumfant

Overview of the Architecture



Triumfant

Continuous Scanning to the Granular Level

Endpoint

Thin, efficient agent

- Scans, executes remediations, communicates w/server
- Small footprint: 25 Mb, < 1% of CPU, no stored information
- Minimal network traffic
- Hardened and protected
- Includes OVAL interpreter

Scans 200k+ attributes:

- Registry keys
- Files – MD5 hash
- Processes
- Services
- Event Logs
- Performance counters
- Security settings
- Hardware attributes
- Memory tables

Triumfant

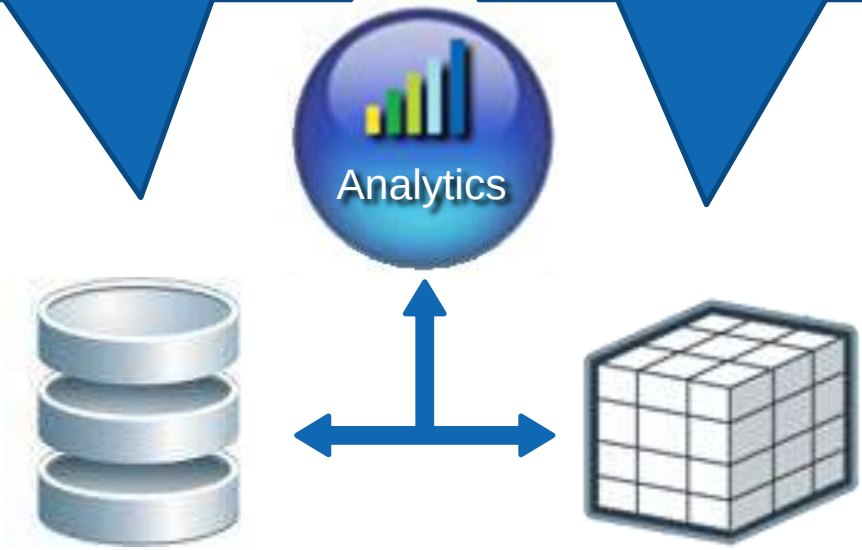
A Unique View of the Population

The data repository

- Most comprehensive endpoint attribute repository
- Maximum 24 hour latency
- Change data capture
  - Minimizes intrusion on endpoint
  - Minimizes network impact

The Adaptive Reference Model

- Multi-dimensional model of the endpoint population
- Automatically synthesized
- Continuously learns and adapts
- Normative baseline of all data



Triumfant

Configuration Management

Configuration checks are converted to Triumfant policies

- Comes out-of-the-box with policies
- Admin enables policies per population or per groups of machines
- Uses the attributes gathered in the normal scan scope

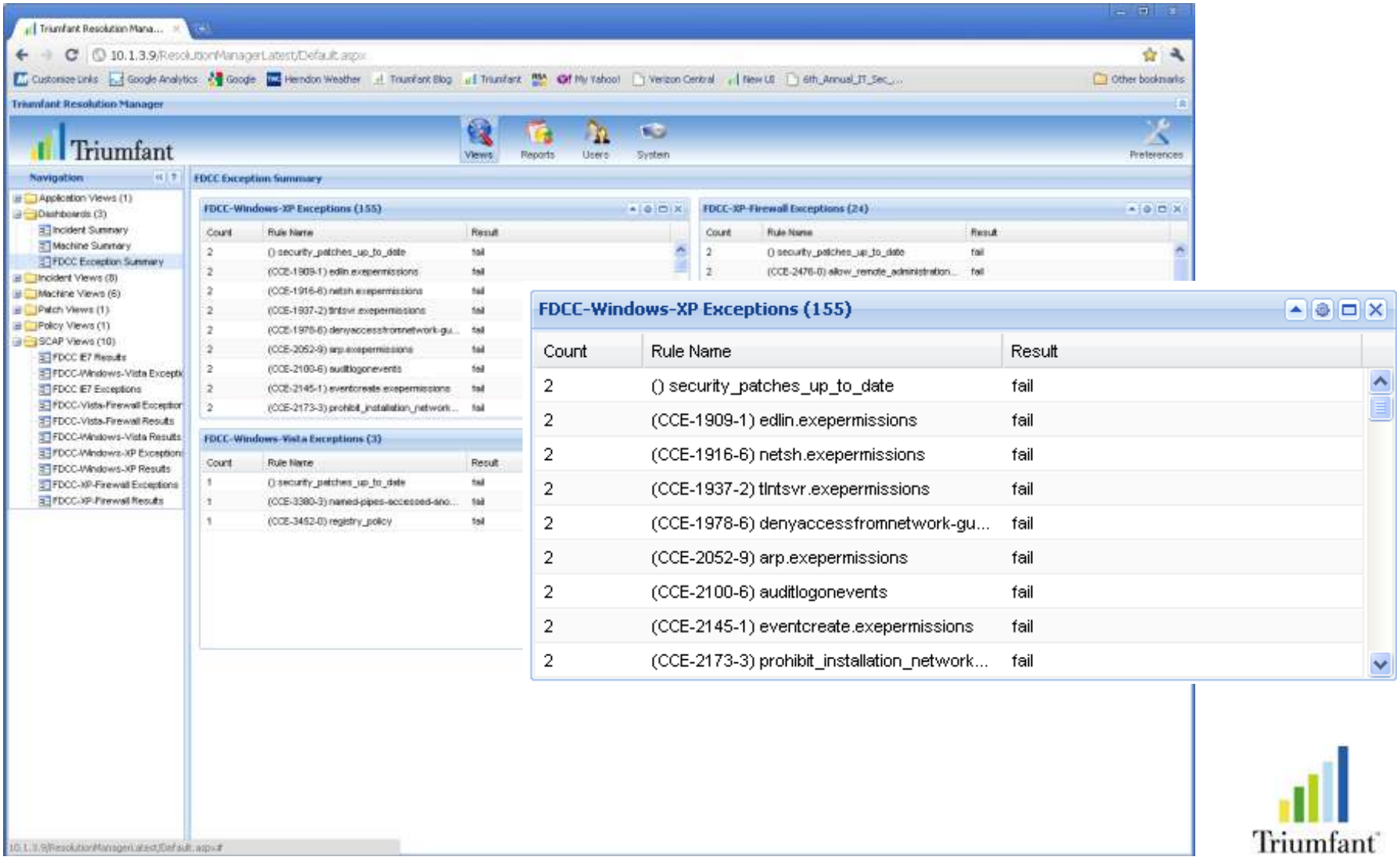
Two parts to the policy

- The actual pass/fail configuration test
- The data required to power the Triumfant remediation process
- Some specialized remediation processes – rename Admin, rename Guest

Configuration results evaluated as part of normal process

- Violations noted
- Remediation constructed using donor technology as needed

Flexible Reporting



Triumfant

Vulnerability Scanning

1. Vulnerability data extracted from MITRE database
2. OVAL content packaged with XCCDF, sent to agent
3. OVAL interpreter on agent runs scan
4. Results placed in associated registry key
5. Registry key scanned in normal processing
6. Changes noted, sent to server for analysis
7. Scan results tied back to CVEs at server level

- Fine grain control allows for specific criteria sets for specific groups
- Comes out of the box with SCAP reports
- Options to set alerts for violations

Triumfant

Vulnerability Analysis

Triumfant continuously scans for vulnerabilities

- Scans at the agent level, so it confirms the vulnerability – other tools can tell you if you ***might*** have a vulnerability
- Very efficient
  - Only returns data to the server when changes are detected
  - Minimizes impact on machine, network and server

A wealth of available data

- Vulnerability reporting without impacting the endpoints
- Vulnerability data even if the machine is offline
- Enables correlation analysis between attacks and vulnerabilities
- Significantly reduces re-imaging (6-12 month ROI)

Triumfant

Trusted Network Connect

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing

Open Standards for Network Security

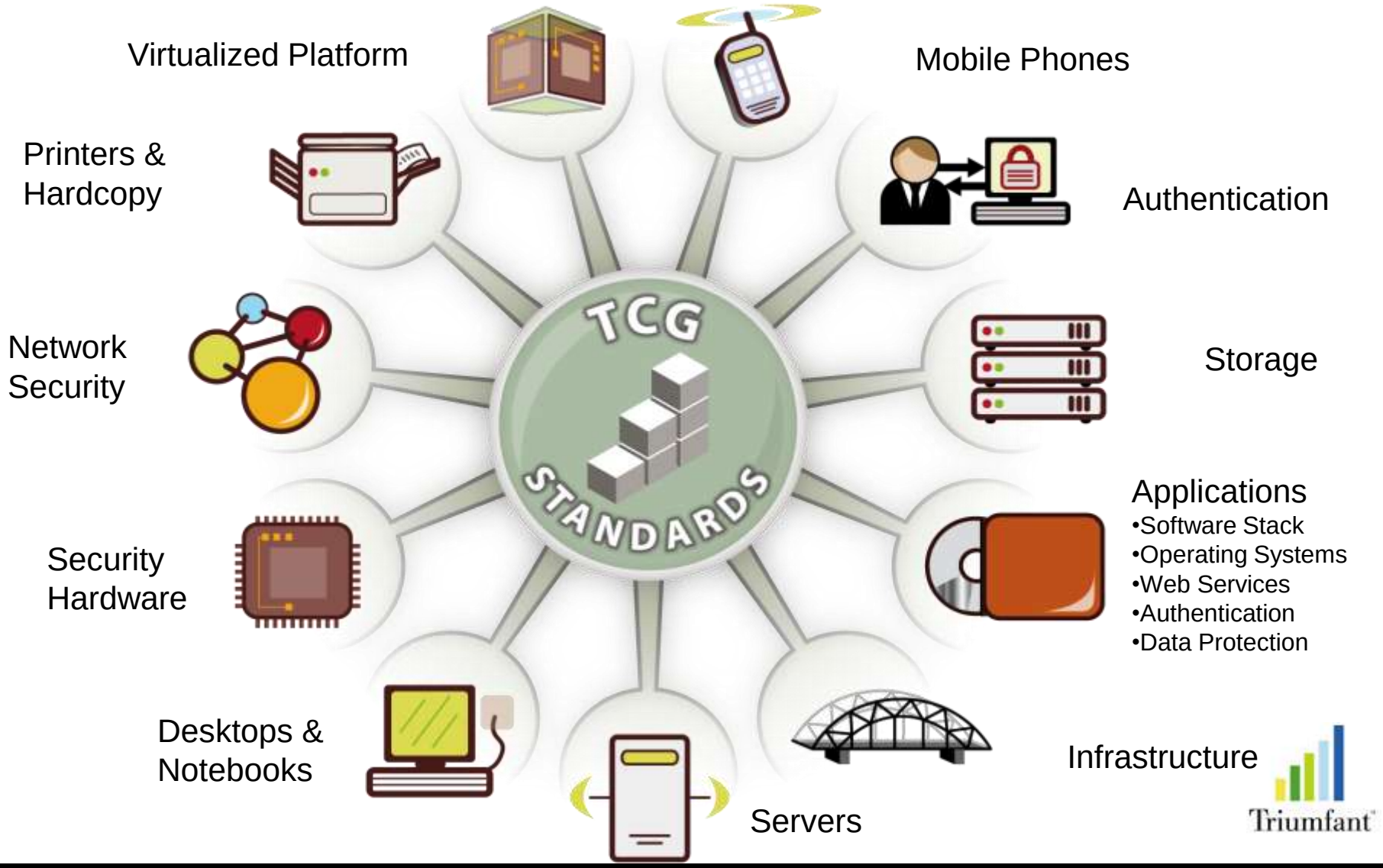
- Full set of specifications available to all
- Products shipping for more than four years

Developed by Trusted Computing Group (TCG)

- Industry standards group
- More than 100 member organizations
- Includes large vendors, small vendors, customers, etc.

Triumfant

TCG: Standards for Trusted Systems



Problems Solved by TNC

Network and Endpoint Visibility

- Who and what's on my network?
- Are devices on my network secure?
  Is user/device behavior appropriate?

Network Enforcement

- Block unauthorized users/devices
- Grant appropriate levels of access to authorized users/devices

Device Remediation

- Quarantine and repair unhealthy devices

Network Access Control (NAC)

Security System Integration

- Share real-time information about users, devices, threats, etc.

Coordinated Security

Triumfant

Sample Network Access Control Policy

To Access the Production Network...

1. User Must Be Authenticated
   - With Identity Management System

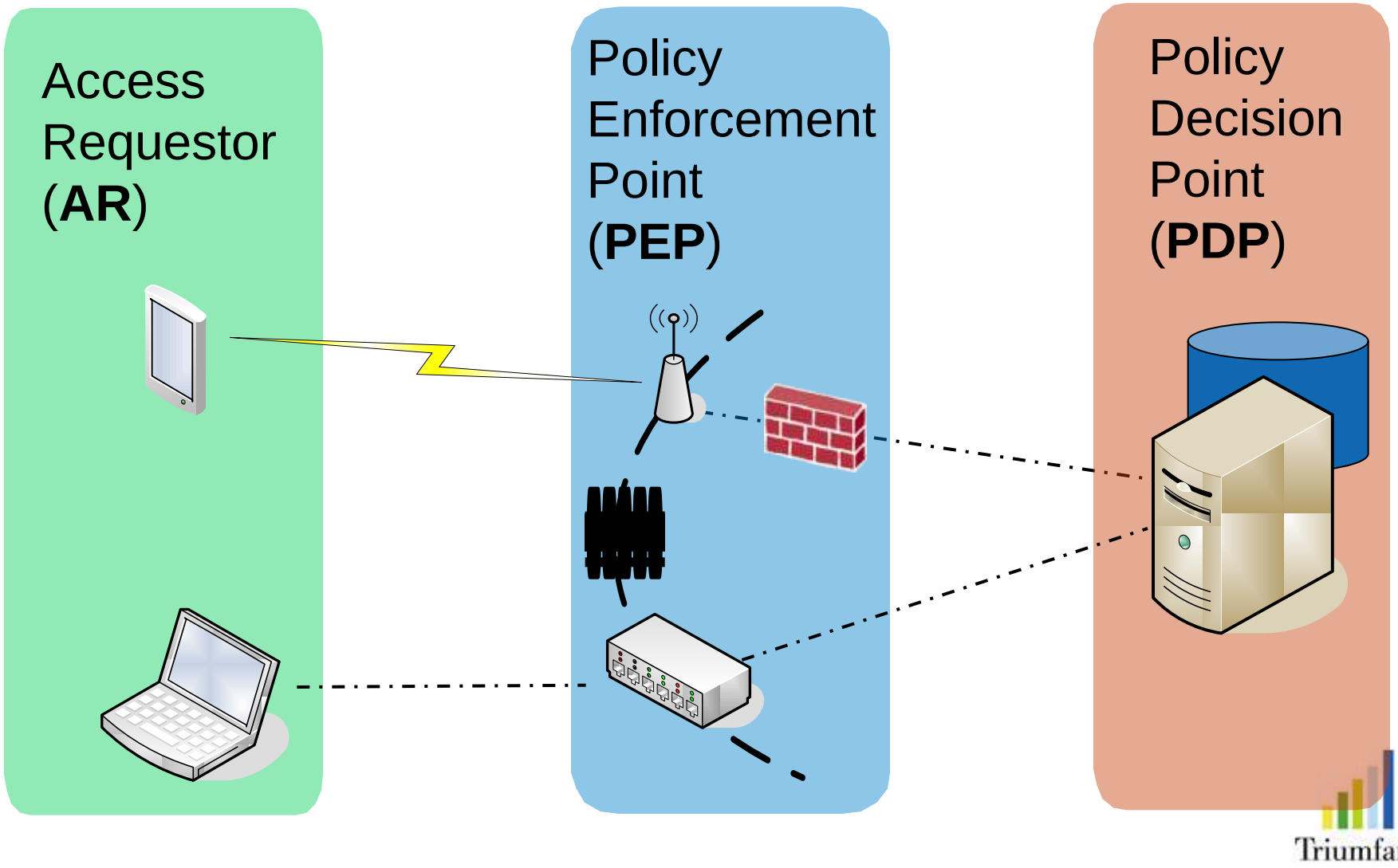
2. Endpoint Must Be Healthy
   - Anti-Virus software running and properly configured
   - Recent scan shows no malware
   - Personal Firewall running and properly configured
   - Patches up-to-date

3. Behavior Must Be Acceptable
   - No port scanning, sending spam

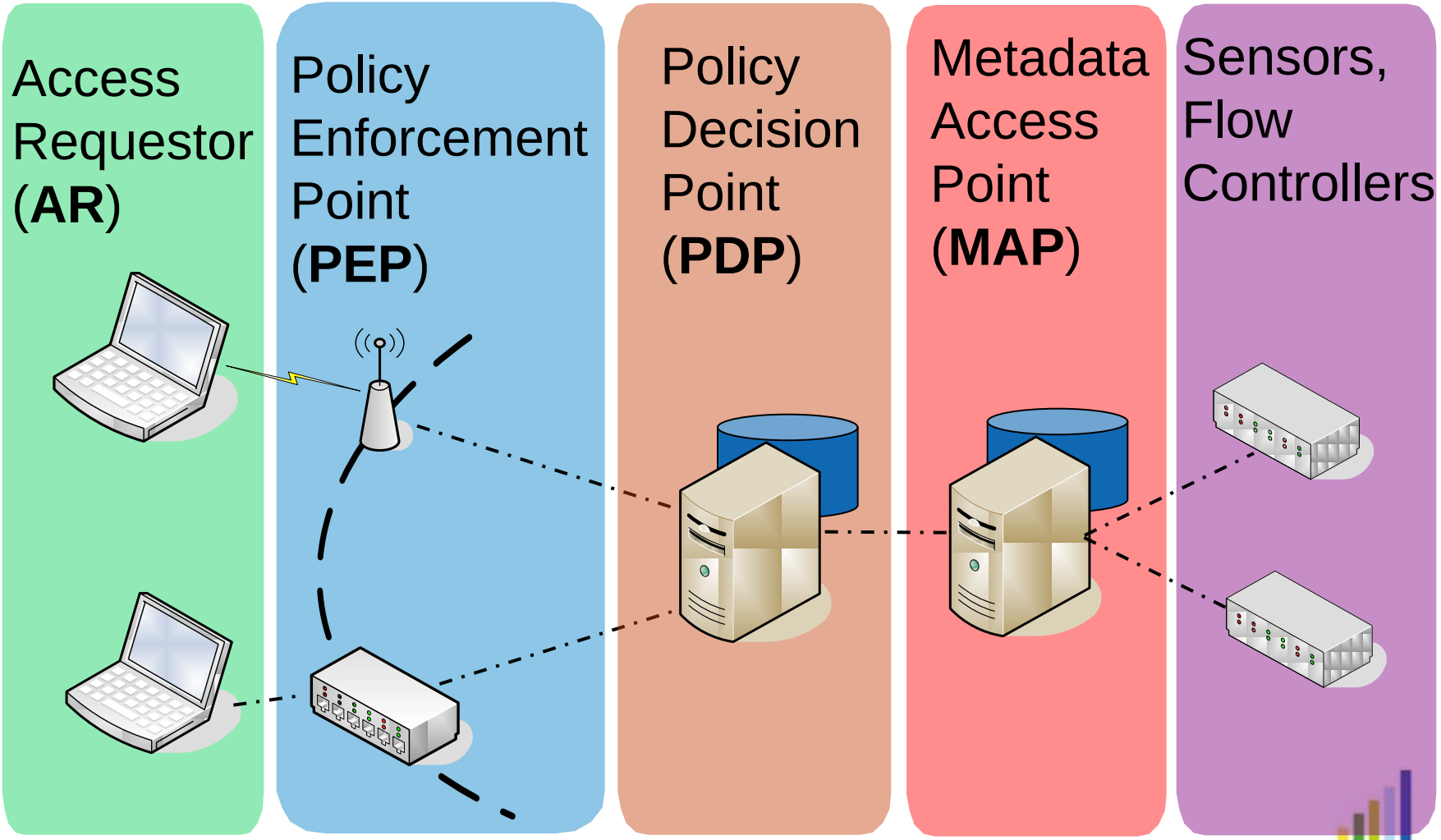
SCAP Strengths

Triumfant

Basic NAC Architecture



Coordinated Security



Triumfant

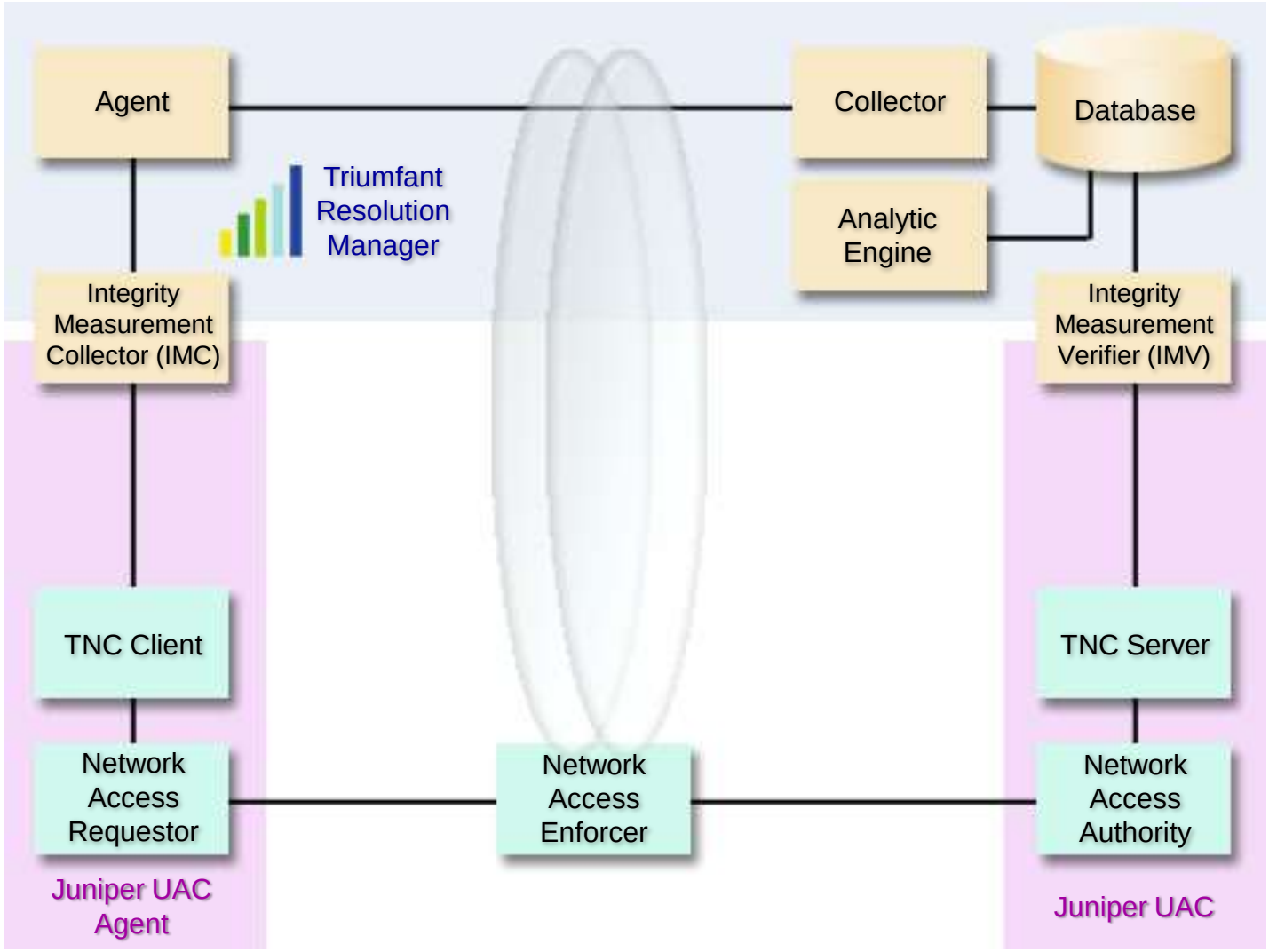
TNC and Triumfant

Triumfant's extensive data collection capabilities and its sophisticated analytic functions make it an ideal source for providing the security state information needed to make intelligent network access decisions.

- SCAP is also a logical extension, which Triumfant speaks fluently
- Triumfant keeps a current store of SCAP results, allowing for minimal intrusion to the log-in process
- Triumfant adds malware detection to the process
- Uniquely capable of automating the remediation process to restore the machine to a compliant state without human intervention

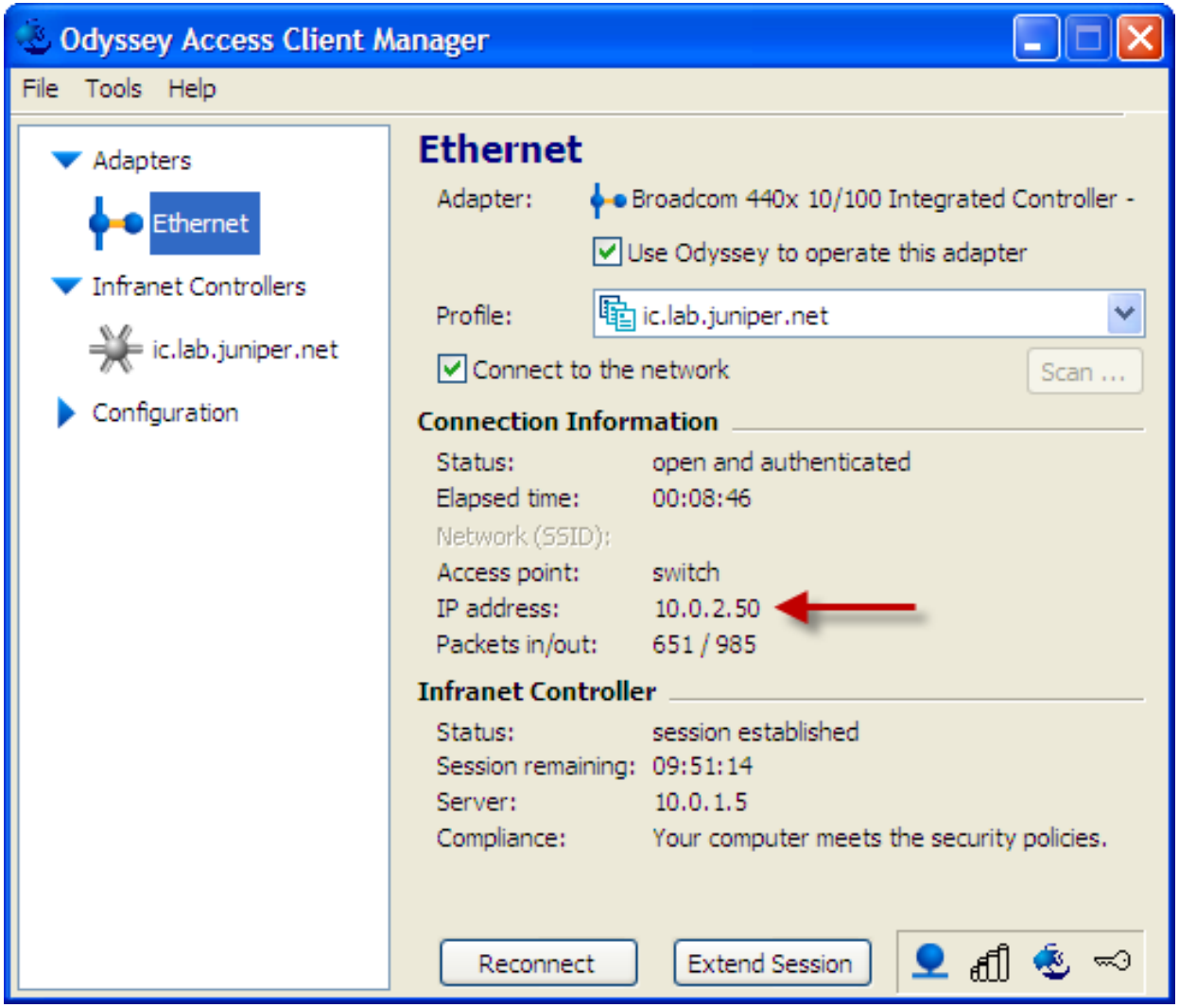
Triumfant

Triumfant TNC Implementation



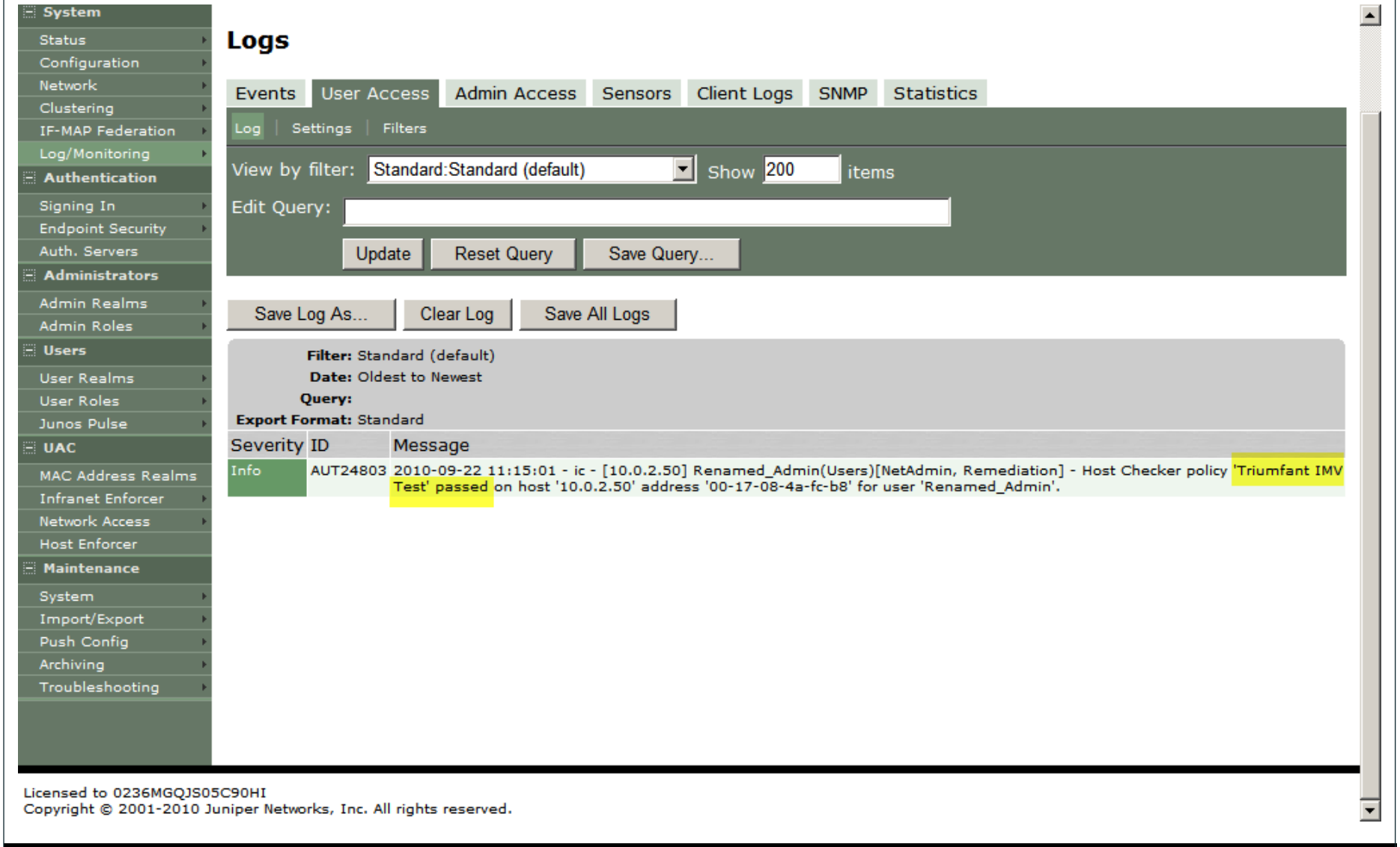
Triumfant

Starting Clean and Compliant

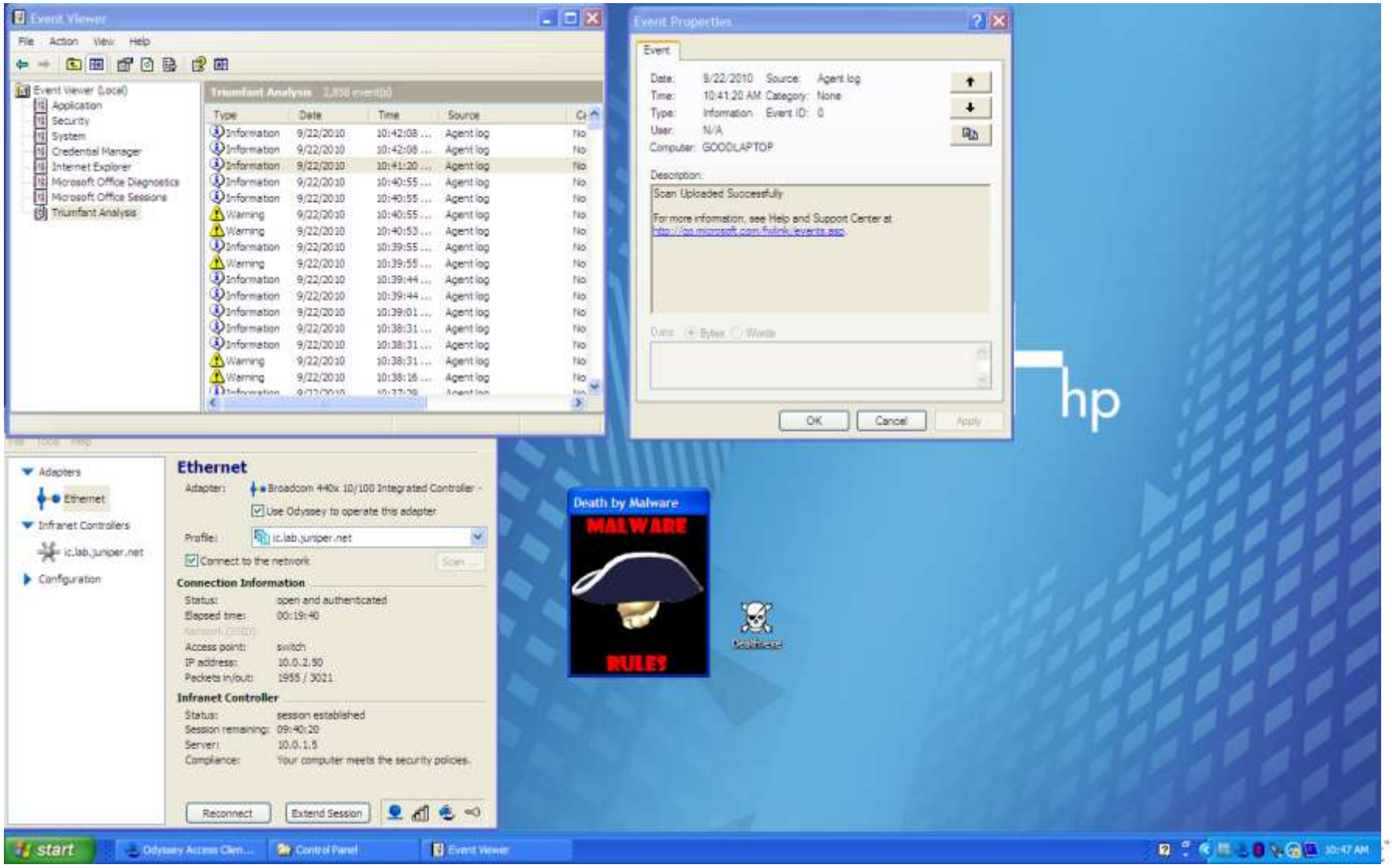


Triumfant

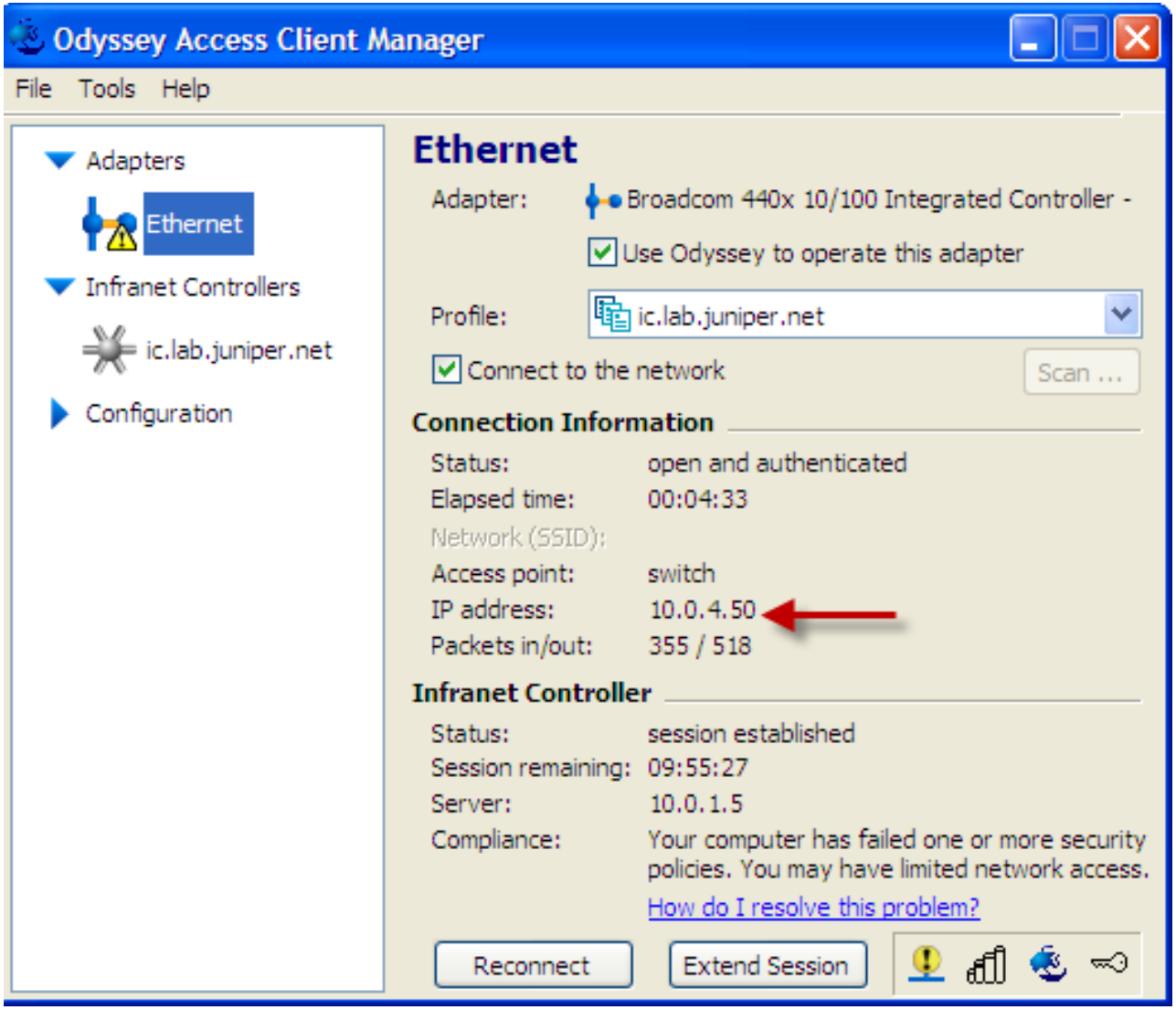
IMV Test Passed



ATTACK!

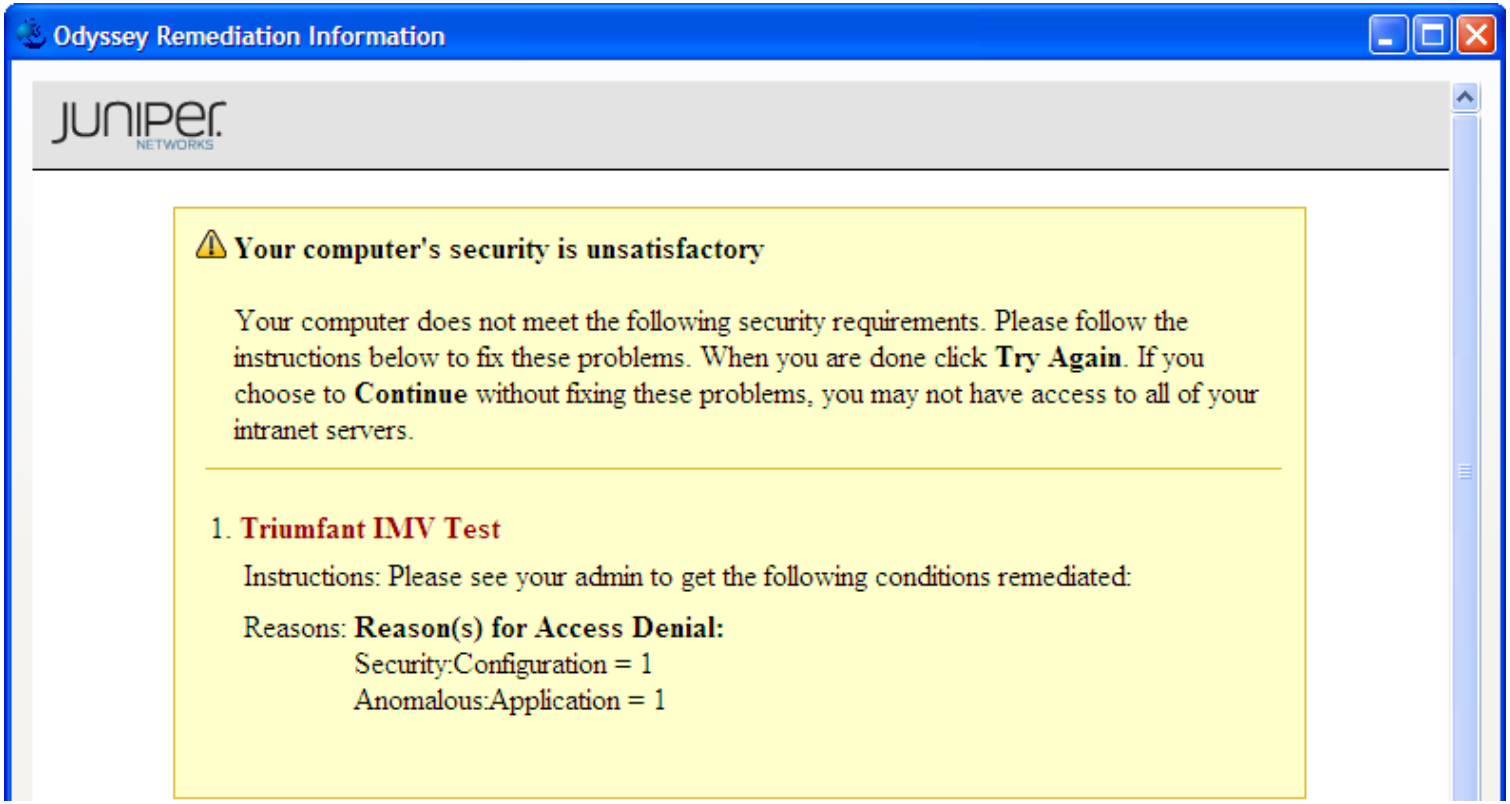


Criteria Fails, Machine Taken Off Network

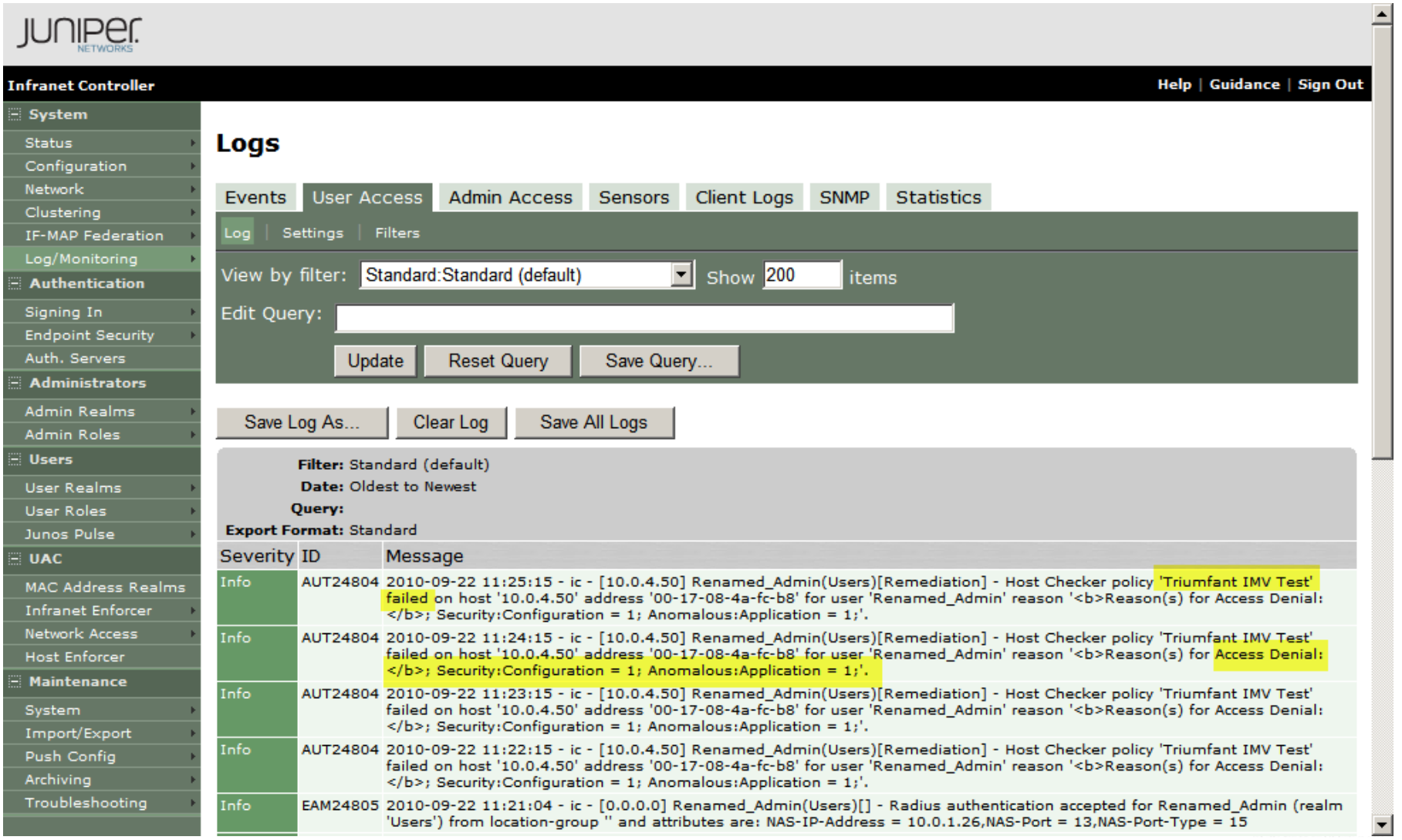


Triumfant

Messages to the User



Log Entry for Test Failure



View Diagnosis Results

Select a 'Condition Recognized' from the Diagnosis Results Summary window to view an explanation of the condition and the supporting diagnostic evidence. To export detailed filter information to a file, select a filter and press "Save to File". Select a row and click on the "Ack\Nack" button to changed the acknowledged state of a condition. Double-click on a row to see more information about the remediation status.

Parameters	Values Selected
Population Name	Demo Group
Agent Group Name	SCAP Group
Machine Name	goodlaptop
Snapshot ID	178
Snapshot Date	2010-09-22 10:47:53

Diagnosis Result Summary

Category	Sub Category	Conditions Recognized	%Matched	Priority	Ack	Workflow Position
Generic	Event	160-0 Anomalous Applicati		3	☐	Event Reported
Security	Configuration	File Permissions: regedit.e	50	3	☐	New
		Unrecognized Anomalies	0	5	☐	

Explanation

Supporting Evidence

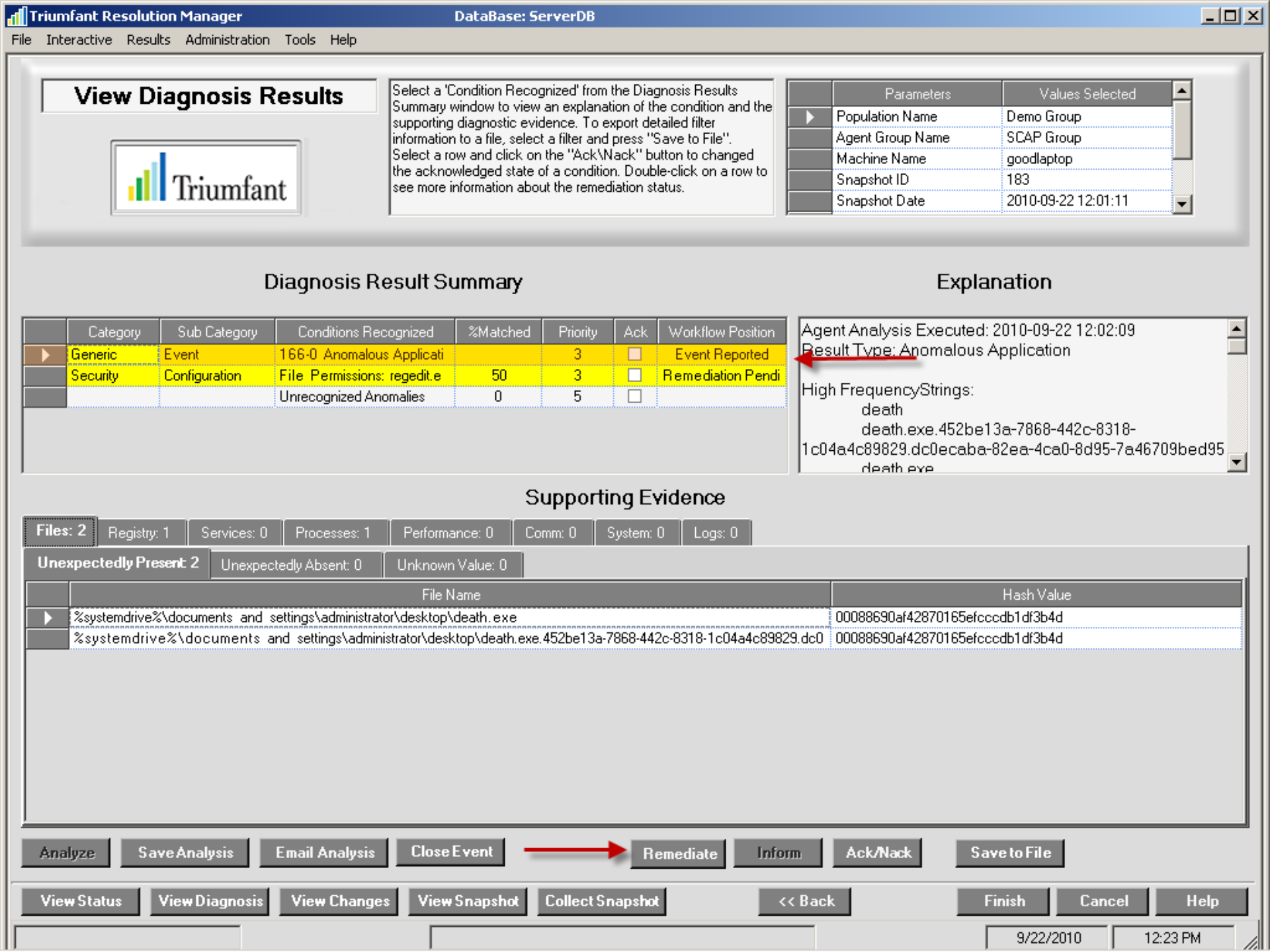
Files: 0 | Registry: 0 | Services: 0 | Processes: 0 | Performance: 0 | Comm: 0 | System: 0 | Logs: 0

Unexpectedly Present: 0 | Unexpectedly Absent: 0 | Unknown Value: 0

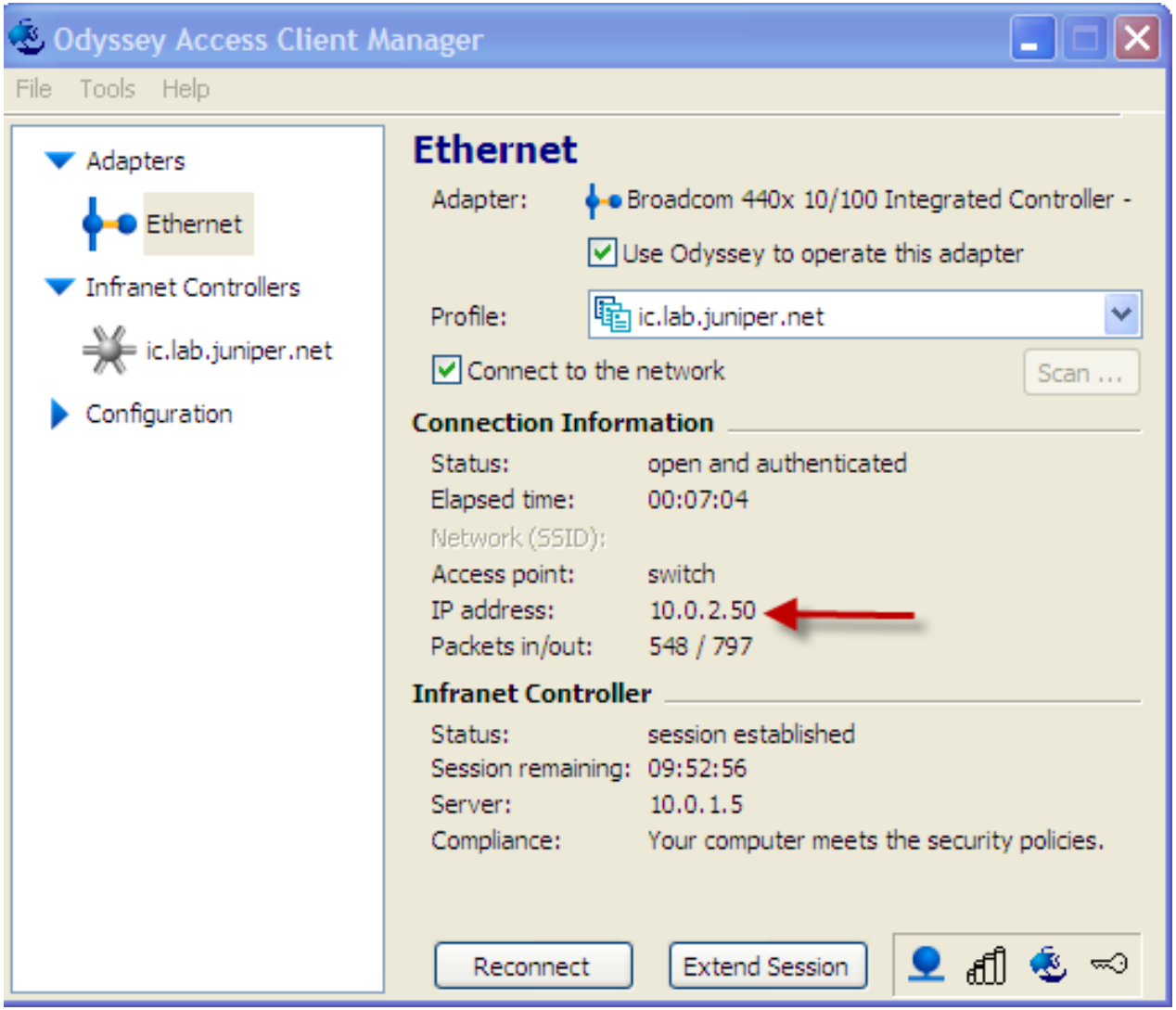
Analyze | Save Analysis | Email Analysis | Close Event | Remediate | Inform | Ack/Nack | Save to File

View Status | View Diagnosis | View Changes | View Snapshot | Collect Snapshot | << Back | Finish | Cancel | Help

9/22/2010 10:54 AM


Triumfant Resolution Manager
DataBase: ServerDB
File Interactive Results Administration Tools Help
View Diagnosis Results
Triumfant
Select a 'Condition Recognized' from the Diagnosis Results Summary window to view an explanation of the condition and the supporting diagnostic evidence. To export detailed filter information to a file, select a filter and press "Save to File". Select a row and click on the "Ack\Nack" button to changed the acknowledged state of a condition. Double-click on a row to see more information about the remediation status.
Parameters | Values Selected
Population Name | Demo Group
Agent Group Name | SCAP Group
Machine Name | goodlaptop
Snapshot ID | 183
Snapshot Date | 2010-09-22 12:01:11
Diagnosis Result Summary
Category | Sub Category | Conditions Recognized | %Matched | Priority | Ack | Workflow Position
Generic | Event | 166-0 Anomalous Applicati | | 3 | | Event Reported
Security | Configuration | File Permissions: regedit.e | 50 | 3 | | Remediation Pendi
Unrecognized Anomalies | 0 | 5
Explanation
Agent Analysis Executed: 2010-09-22 12:02:09
Result Type: Anomalous Application
High FrequencyStrings:
death
death.exe.452be13a-7868-442c-8318-1c04a4c89829.dc0ecaba-82ea-4ca0-8d95-7a46709bed95
death.exe
Supporting Evidence
Files: 2 | Registry: 1 | Services: 0 | Processes: 1 | Performance: 0 | Comm: 0 | System: 0 | Logs: 0
Unexpectedly Present: 2 | Unexpectedly Absent: 0 | Unknown Value: 0
File Name | Hash Value
%systemdrive%\documents and settings\administrator\desktop\death.exe | 00088690af42870165efcccdb1df3b4d
%systemdrive%\documents and settings\administrator\desktop\death.exe.452be13a-7868-442c-8318-1c04a4c89829.dc0 | 00088690af42870165efcccdb1df3b4d
Analyze
Save Analysis
Email Analysis
Close Event
Remediate
Inform
Ack/Nack
Save to File
View Status
View Diagnosis
View Changes
View Snapshot
Collect Snapshot
<< Back
Finish
Cancel
Help
9/22/2010
12:23 PM

Back to the Secure Network



Triumfant

Summary

- Triumfant is fully SCAP conversant
- Triumfant's unique technology creates an equally unique SCAP capability
  - Configuration management and enforcement
  - Vulnerability management
- The Triumfant repository is an extremely useful data source for analysis and reporting
- The marriage of SCAP, TNC, and Triumfant is logical and pragmatic

Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation

September 2010