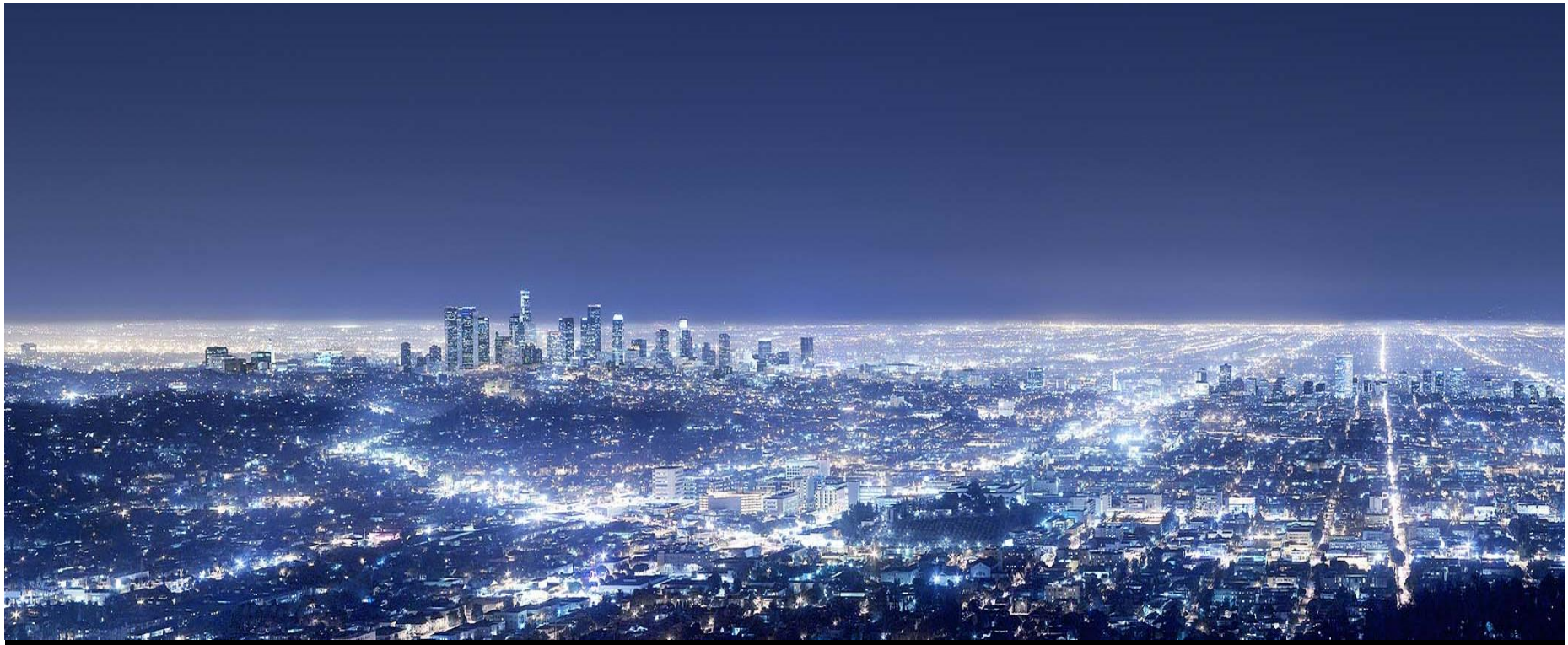
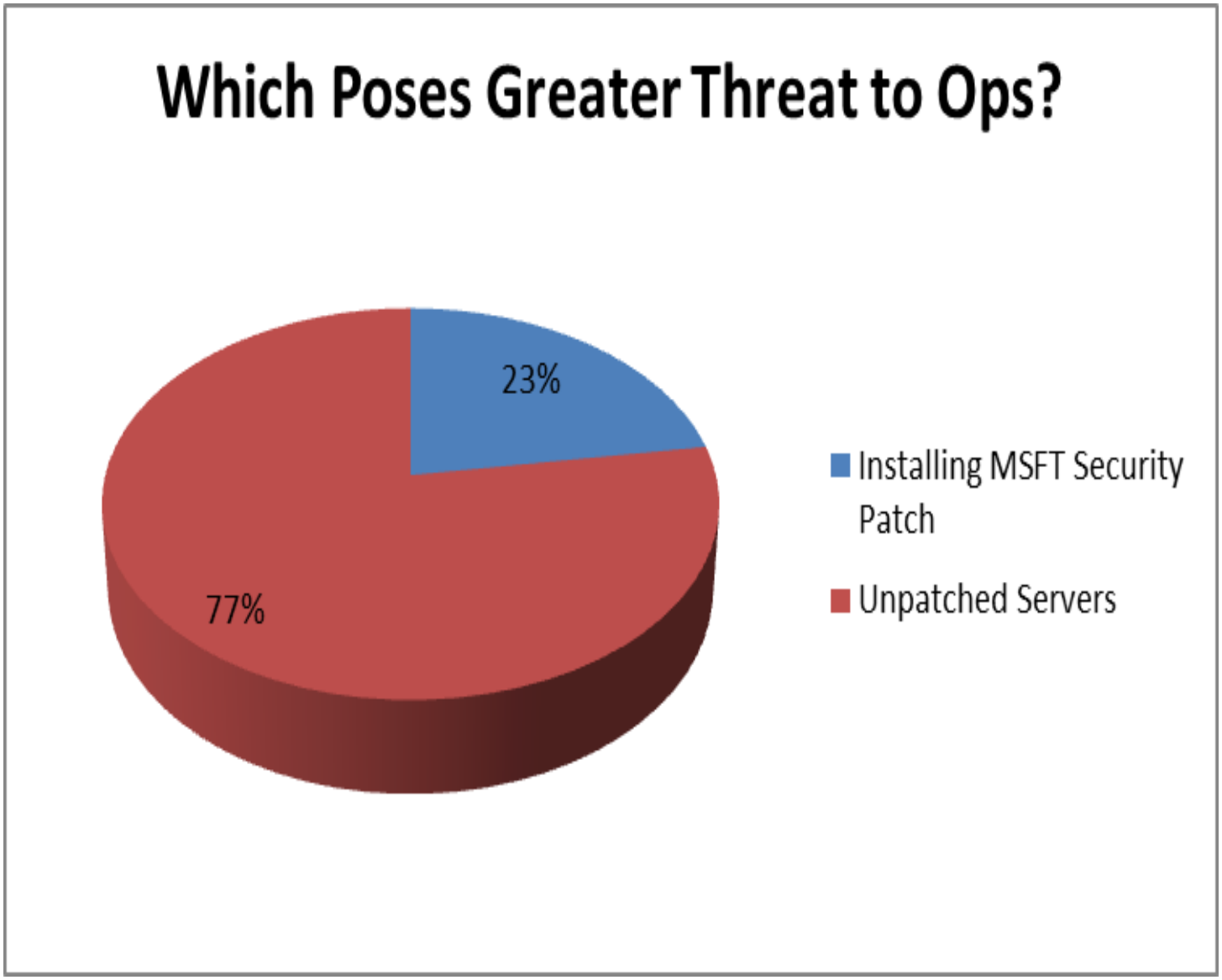


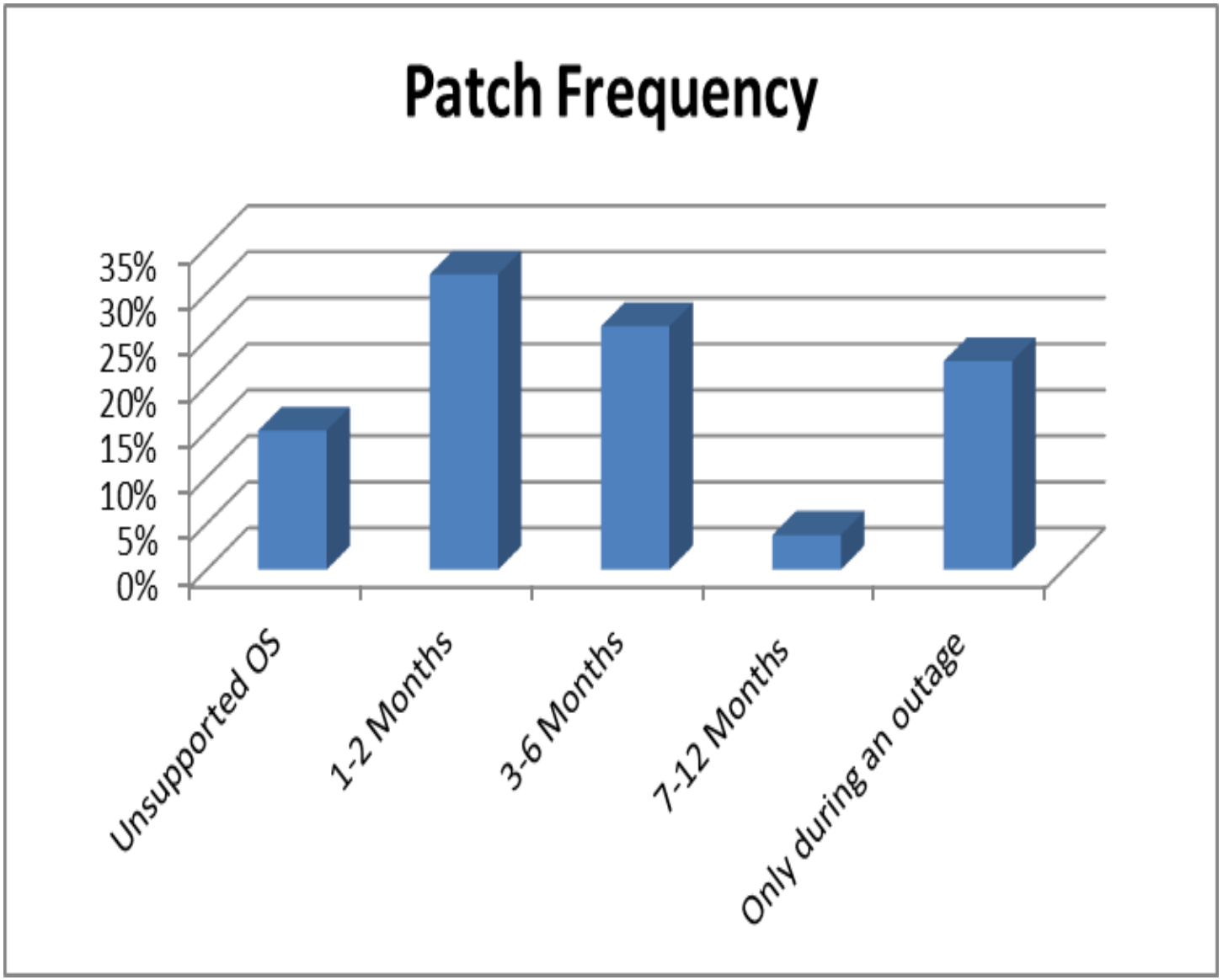
April 23, 2015

ABB Power Generation DCS Users Group
Cyber Security Special Interest Group

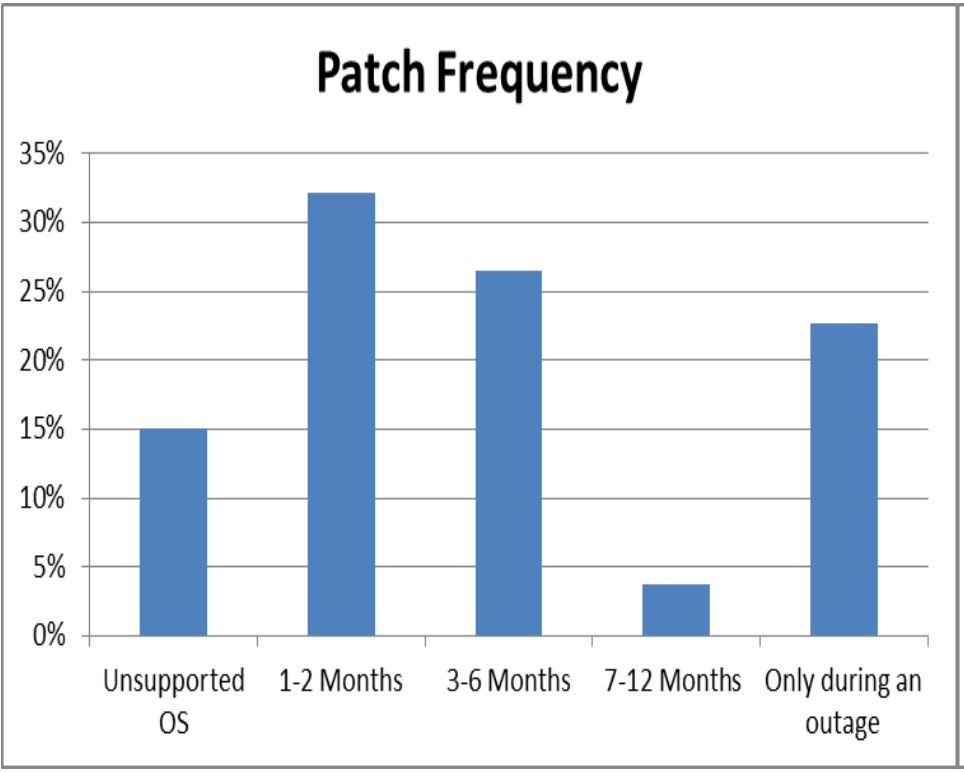
Registration Peer Group Survey

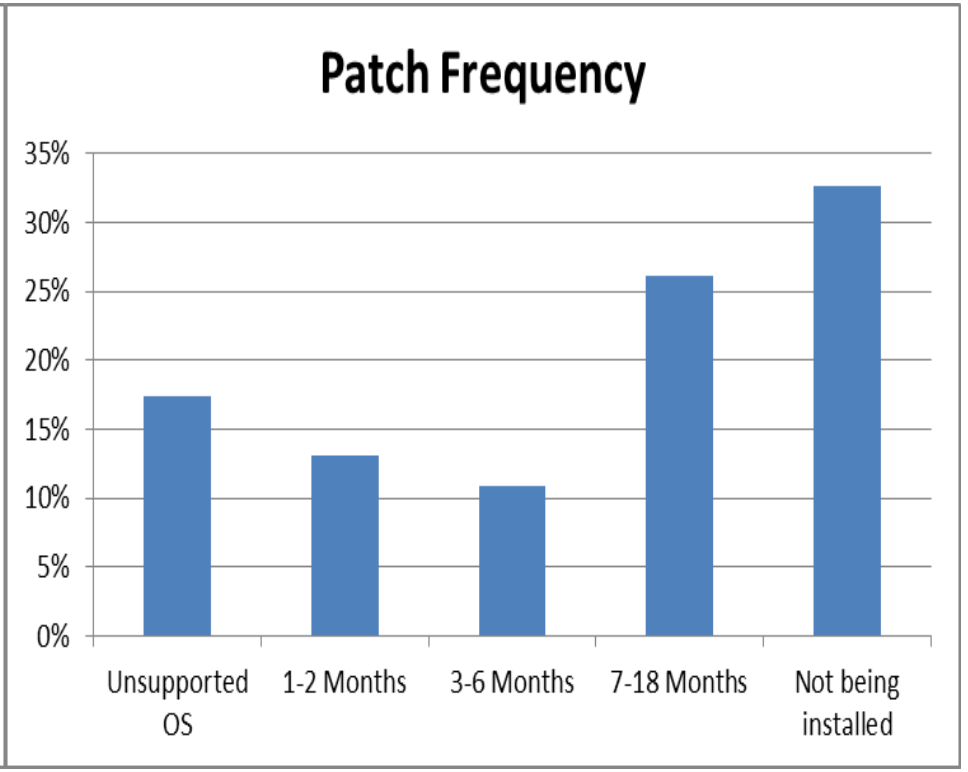


Registration Peer Group Survey

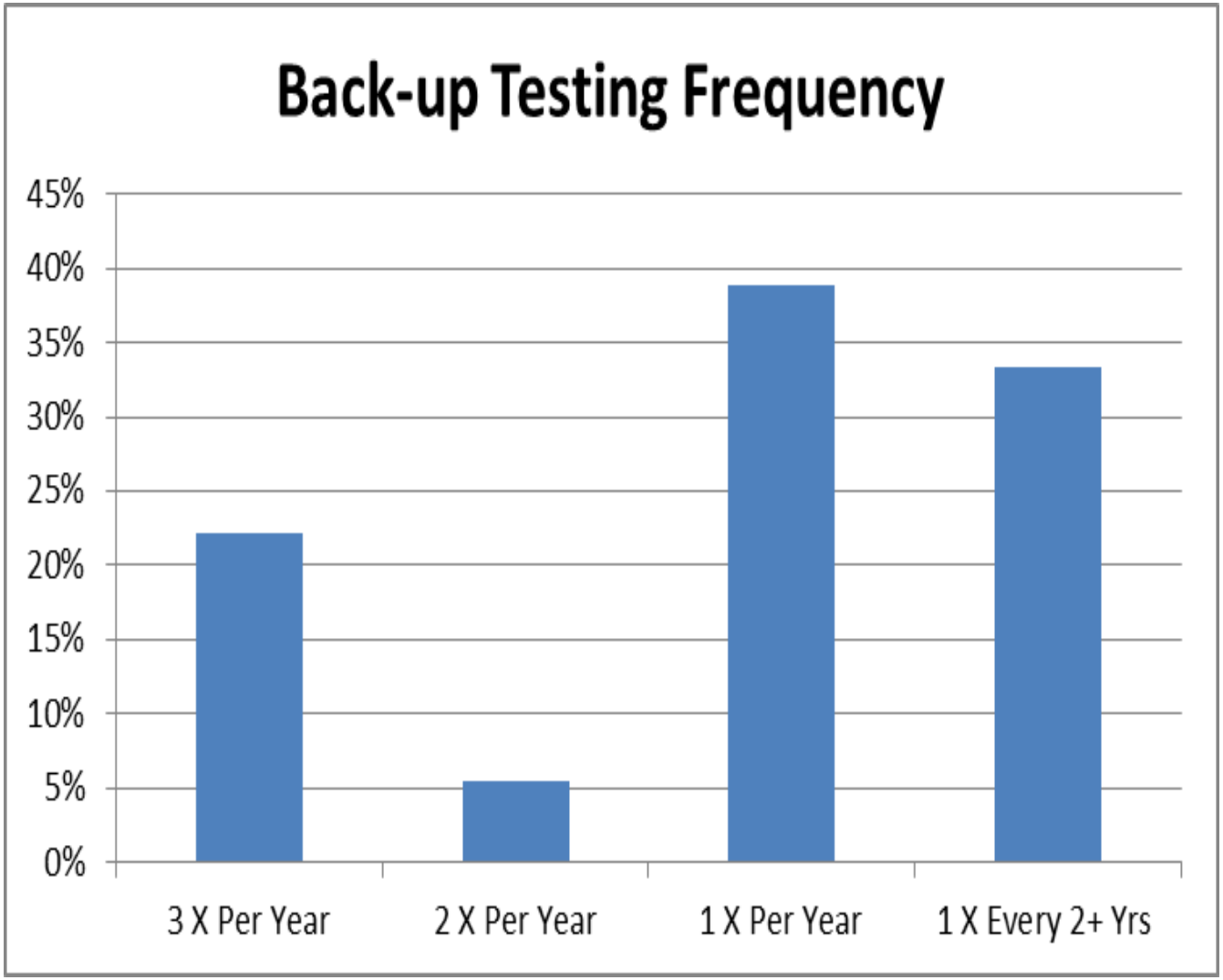


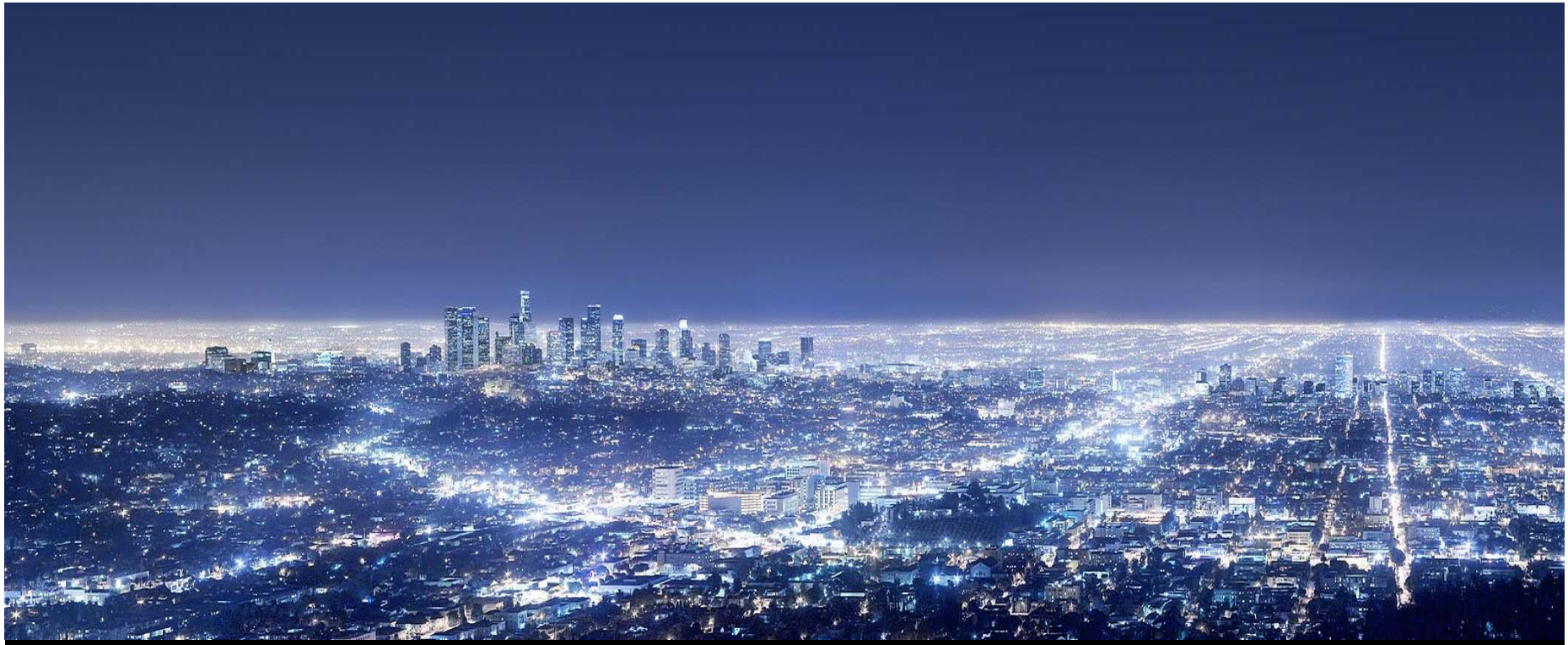
Registration Peer Group Survey





Registration Peer Group Survey – Future Topic





April 23, 2015

ABB Power Generation DCS Users Group
Cyber Security Special Interest Group
ABB Cyber Security Solutions

Join the ABB DCS Users Group
Share, exchange, and connect with your peers!

- **Website:** www.adcsug.com
- Users of ABB control system products and services in the power and water industries.
  - Forum to: share experiences, learn and collaborate with industry peers, measurably influence and improve AB

- Top 5 reasons to join the group:
  - Networking: true peer-to-peer forums
  - Improvement suggestions: day-to-day challenges discussed and ideas exchanged
  - News: related articles and information from the industry
  - Events calendar: stay connected with users and ABB Power Generation
  - Polls / surveys: express your opinion and make your voice heard

- "The value of a users group, and that in particular of ABB DCS Users Group, is that as a group we have more access and leverage to change and improve the product than as individuals acting alone. It also allows us to participate in discussions that bring the best ideas forward and facilitates sharing information that helps everyone." - Bill Ossman, ABB DCS Users Group STECO member

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- ABB Security Solutions Overview
- MAINTAIN Demonstrations
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Today's Panel

- Mike Radigan, Senior Advisor, Cyber Risk Management, ABB PSPG
  - Mike.Radigan@us.abb.com (614) 398-6241
- Joe Catanese, Application Engineer, ABB Power Generation
  - joseph.p.catanese@us.abb.com (440) 585-2789
- Matt Virostek, Application Engineer, ABB Power Generation
  - matthew.virostek@us.abb.com (440) 585-2789

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- **ABB Security Solutions Overview**
- MAINTAIN Demonstrations
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Security Workplace
Package Overview and Maintain Demonstration

- Speaker name: Joe Catanese
- Speaker title: Sr. Application Engineer – Cyber Security
- Company name: ABB Inc.
- Location: Wickliffe, Ohio
- Phone: 440-585-2789
- E-Mail: joseph.p.Catanese@us.abb.com

Presentation Outline
Overview

- Package Overview
- Maintain Package
- Defend Package
- Comply Package
- Continuing Development
- Maintain Demonstration

Security Workplace

Package Overview

Security Workplace
Package overview

Security Workplace

MAINTAIN
- System Hardening
- User Access Control
- MS Patches, Anti Virus, Patch Disk
- **Centralized Microsoft Patching***
- Centralized Anti-Virus Management
- Automated Backup and Recovery
- **Secure File Transfer (ODI-X)***

DEFEND
- **Detect-in-Depth (Sophia)***
- NIDS (Network Intrusion Detection)
- Security Event Monitoring
- **Application Whitelisting ***
- Configuration Change Management
- IT Asset Management

COMPLY
- Automated Data Collection
- Automated Compliance Reporting
- Workflow Automation Suite

* Indicates product is in managed release

Security Workplace
Package overview

Security Baseline Requirements**	MAINTAIN	DEFEND	COMPLY
Automated back-up & recovery	✓	✓	✓
System and network hardening	✓	✓	✓
Centralized anti-virus management	✓	✓	✓
Centralized Microsoft patch management	✓	✓	✓
Proactive Security Measures			
Electronic perimeter protection*		✓	✓
Security event management*		✓	✓
ICS asset management*		✓	✓
Configuration change management*		✓	✓
Automated data collection*		✓	✓
NERC CIP Compliance			
Automated compliance reporting*			✓
Policy management*			✓
Workflow Automation Suite			✓

*Available for Fleet-Wide and Multi-Vendor Control Systems

**Active ServiceGrid contract required

✓= Included

ABB Security Workplace
NERC-CIP version 5 Requirements

002 BES Cyber System Categorization	003 Security Management Controls	004 Personnel and Training	005 Electronic Security Perimeter	006 Physical Security of CCAs	007 System Security Management	008 Incident Reporting and Response Planning	009 Recovery Plans for CCAs	010 Change Management and Vulnerability Assessments	011 Information Protection
Impact Rating	Cyber Security Policy	Awareness	Electronic Security Perimeter	Physical Security Plan	Test Procedures	Incident Response Plan	Recovery Plan	Configuration Change Management	Information Protection
15 Month Review	Management Approval	Cyber Security Training	Remote Access Management	Visitor Control Program	Ports and Services	Implementation and Testing	Exercises	Configuration Monitoring	Media Reuse and Disposal
	Leadership	Personnel Risk Assessment		PACS Maintenance and Testing	Security Patch Management	Review, Update and Communicate	Change Control	Vulnerability Assessment	
	Delegation	Access Management Plan		Physical Access Controls	Malicious Software Prevention				
		Access Revocation			Security Event Monitoring				
					System Access Controls				

- Security Workplace assists in compliance of requirements marked by

Security Workplace

Maintain Package

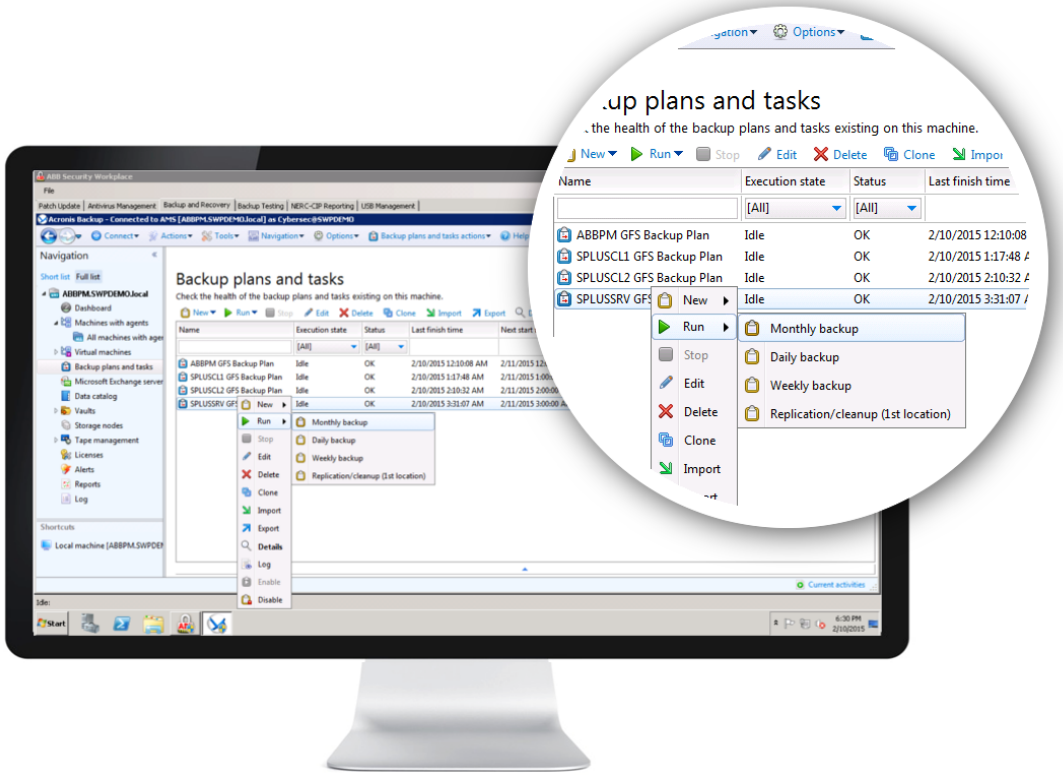
ABB Security Workplace
Maintain

Automated Backup & Recovery

System & Network Hardening

Centralized Anti-Virus Management

Centralized Microsoft Patch Management



- Grandfather – Father – Son
- Centrally manages backup plans
- Recovery plans
- Conversion to VM

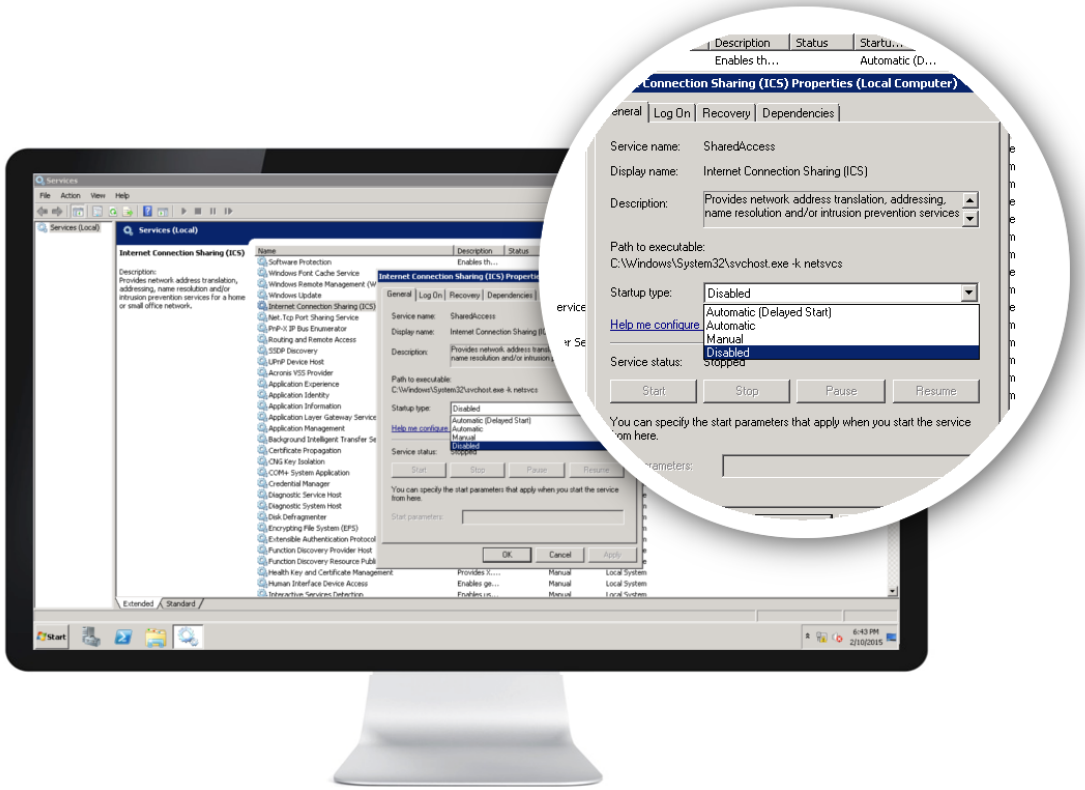
ABB Security Workplace
Maintain

Automated Backup & Recovery

System & Network Hardening

Centralized Anti-Virus Management

Centralized Microsoft Patch Management



- Reduce surface area of vulnerability
  - Services
  - Firewall
  - Applications
- Close unused networking ports
- System state documentation

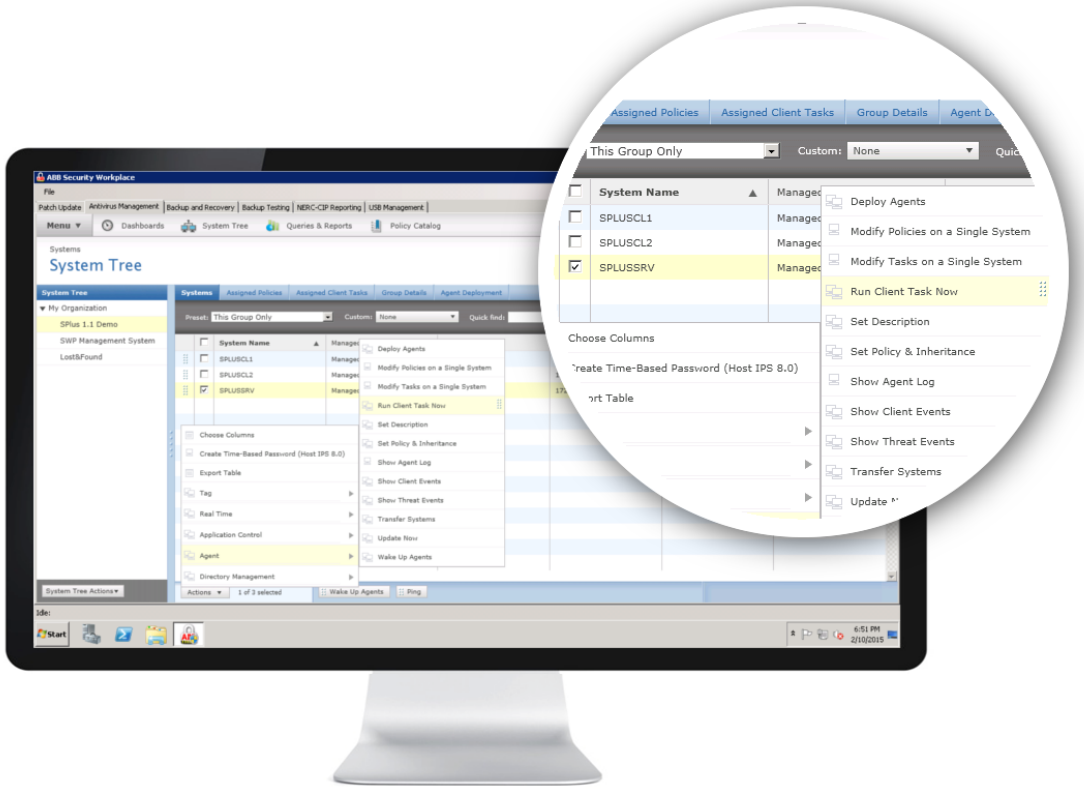
ABB Security Workplace
Maintain

Automated Backup & Recovery

System & Network Hardening

Centralized Anti-Virus Management

Centralized Microsoft Patch Management



- Manage AV Policies
- Manage DAT file deployments

ABB Security Workplace
Maintain

Automated Backup & Recovery

System & Network Hardening

Centralized Anti-Virus Management

Centralized Microsoft Patch Management

- PSPG developed and maintained
- Reduces effort in deploying Microsoft patching
- Aligned with ABB Validation Documents

Security Workplace

Defend Package

ABB Security Workplace
Defend

Electronic Perimeter Protection

Security Event Management

ICS Asset Management

Configuration Change Management

- Edge Routing/Firewall
- Intrusion Protection
- Unified Threat Manager
- IPSec / SSL VPN

ABB Security Workplace
Defend

Electronic Perimeter Protection

Security Event Management

ICS Asset Management

Configuration Change Management

- Improve situational awareness
- Monitor system performance
- Consolidate event logs
- Detect anomalies
- Triage alerts
- Generate reports

ABB Security Workplace
Defend

Electronic Perimeter Protection

Security Event Management

ICS Asset Management

Configuration Change Management

- Reduce cyber security risks
- Meet compliance requirements
- Unified, single view of asset base

ABB Security Workplace
Defend

Electronic Perimeter Protection

Security Event Management

ICS Asset Management

Configuration Change Management

- Reduce manual activities by 80%
- Improve change management
- Eliminate configuration drift
- Report compliance effortlessly
- Improve control system cyber security

Security Workplace

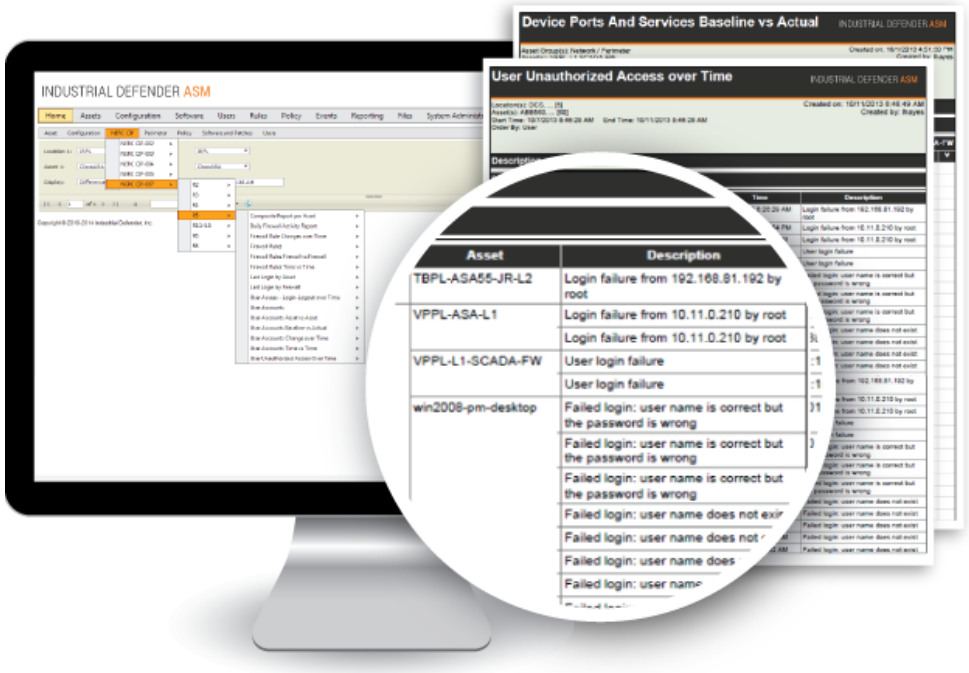
Comply Package

ABB Security Workplace
Comply

Automated Compliance Reporting

Policy Management

Workflow Automation Suite



- NERC-CIP compliance
- Ports and services
- Software inventory
- Password policy
- User accounts

ABB Security Workplace
Comply

Automated Compliance Reporting

Policy Management

Workflow Automation Suite

- Communicate new policies
- Track acceptance
- Manage conformance
- Always be audit-ready

ABB Security Workplace
Comply

Automated Compliance Reporting

Policy Management

Workflow Automation Suite

- Initiate, track, approve, document and report on workflows
- Document management
- Automated reporting

Security Workplace

Continuing Development

ABB Security Workplace
Continuing development

Application Control

USB/Media Control

Disaster Recovery

- Application whitelisting
- At-a-glance dashboard
- Easy policy creation
- Fully integrated into AV management console
- Pilots shipped and running

ABB Security Workplace
Continuing development

Application Control

USB/Media Control

Disaster Recovery

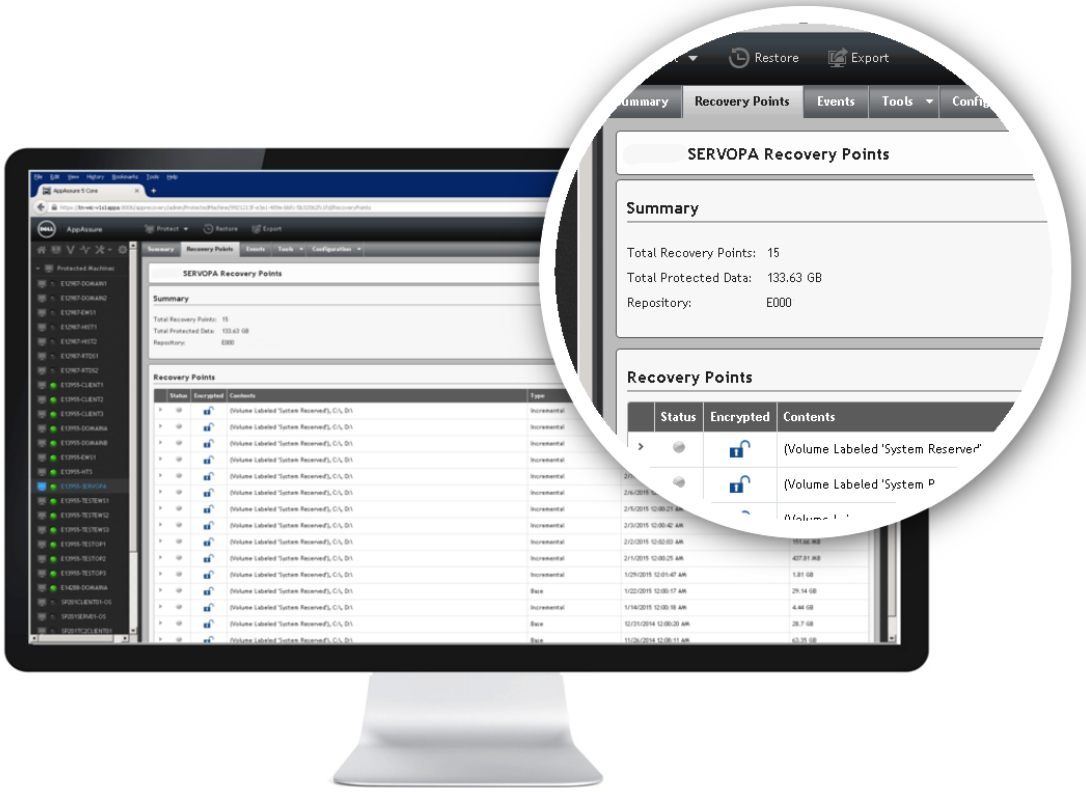
- Control files entering your system
- Scan for viruses
- Prevents distributed attacks
- Easy and fast to use
- Files upload directly to share

ABB Security Workplace
Continuing development

Application Control

USB/Media Control

Disaster Recovery



- Alternative to Acronis
- Dell OEM driver support
- Tighter integration with SWP
- Easier to manage

Security Workplace

Maintain Package Walkthrough

ABB Security Workplace
Maintain - Demonstration

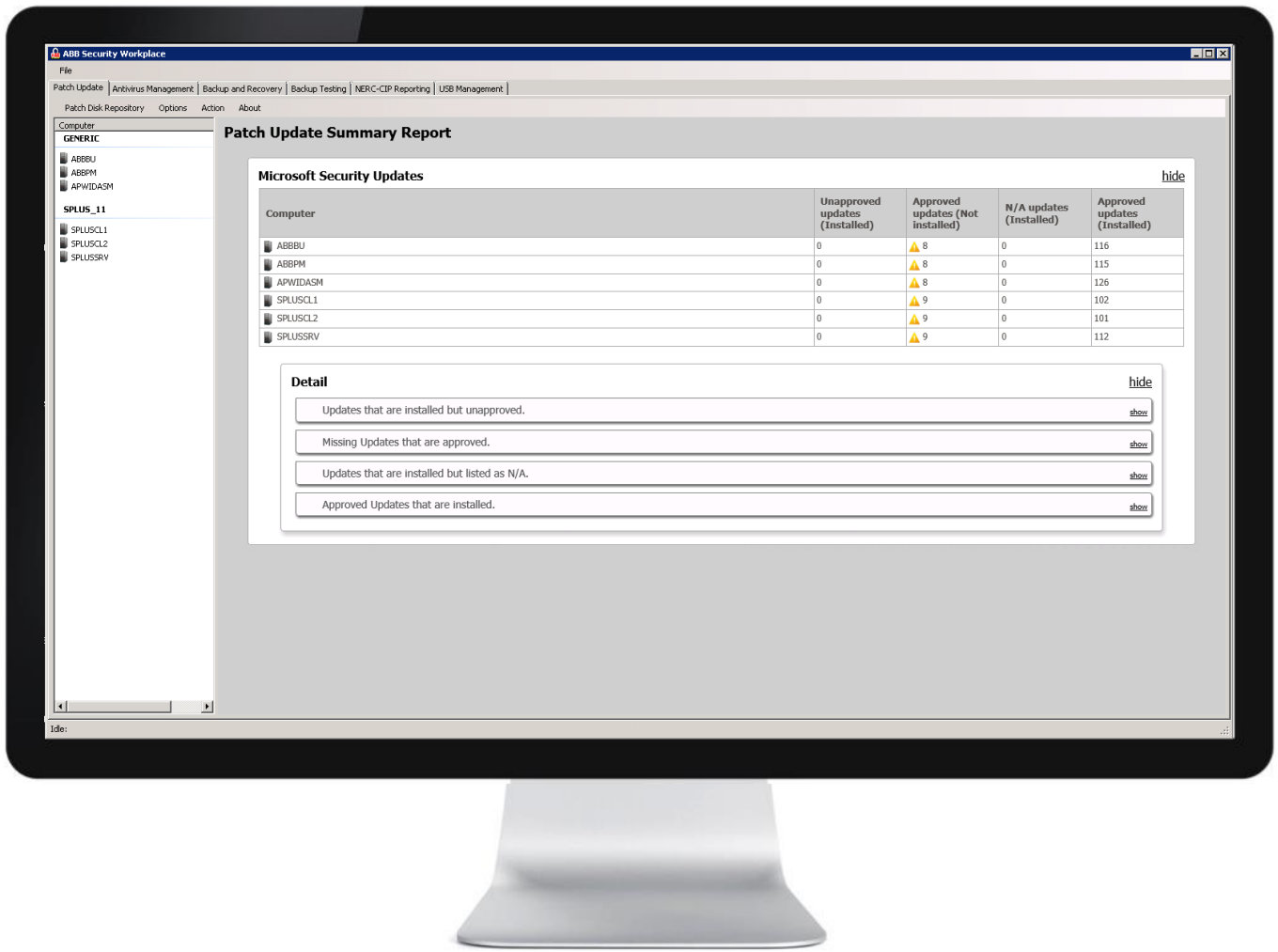


ABB Security Workplace
Maintain - Demonstration

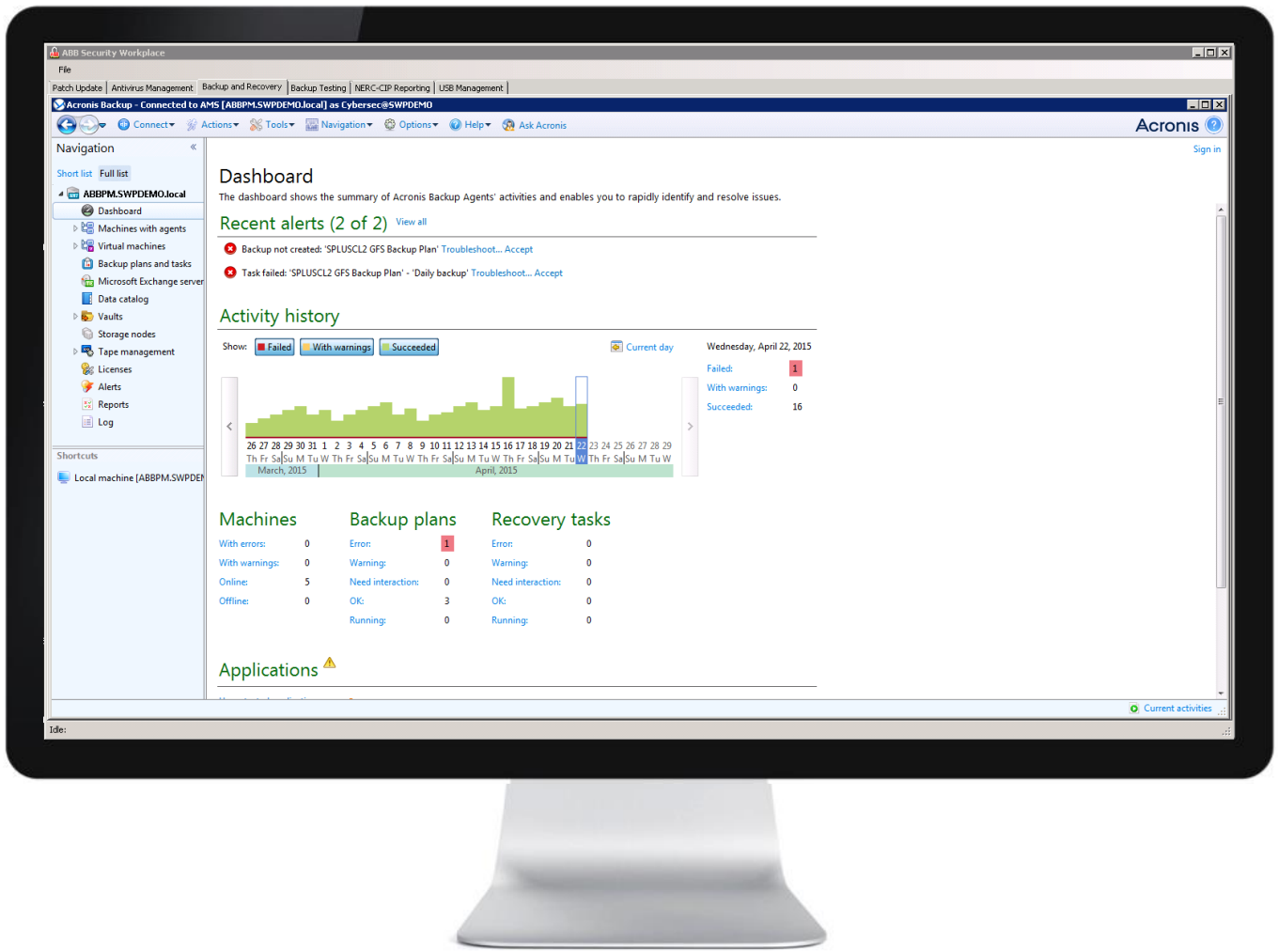


ABB Security Workplace
Maintain - Demonstration

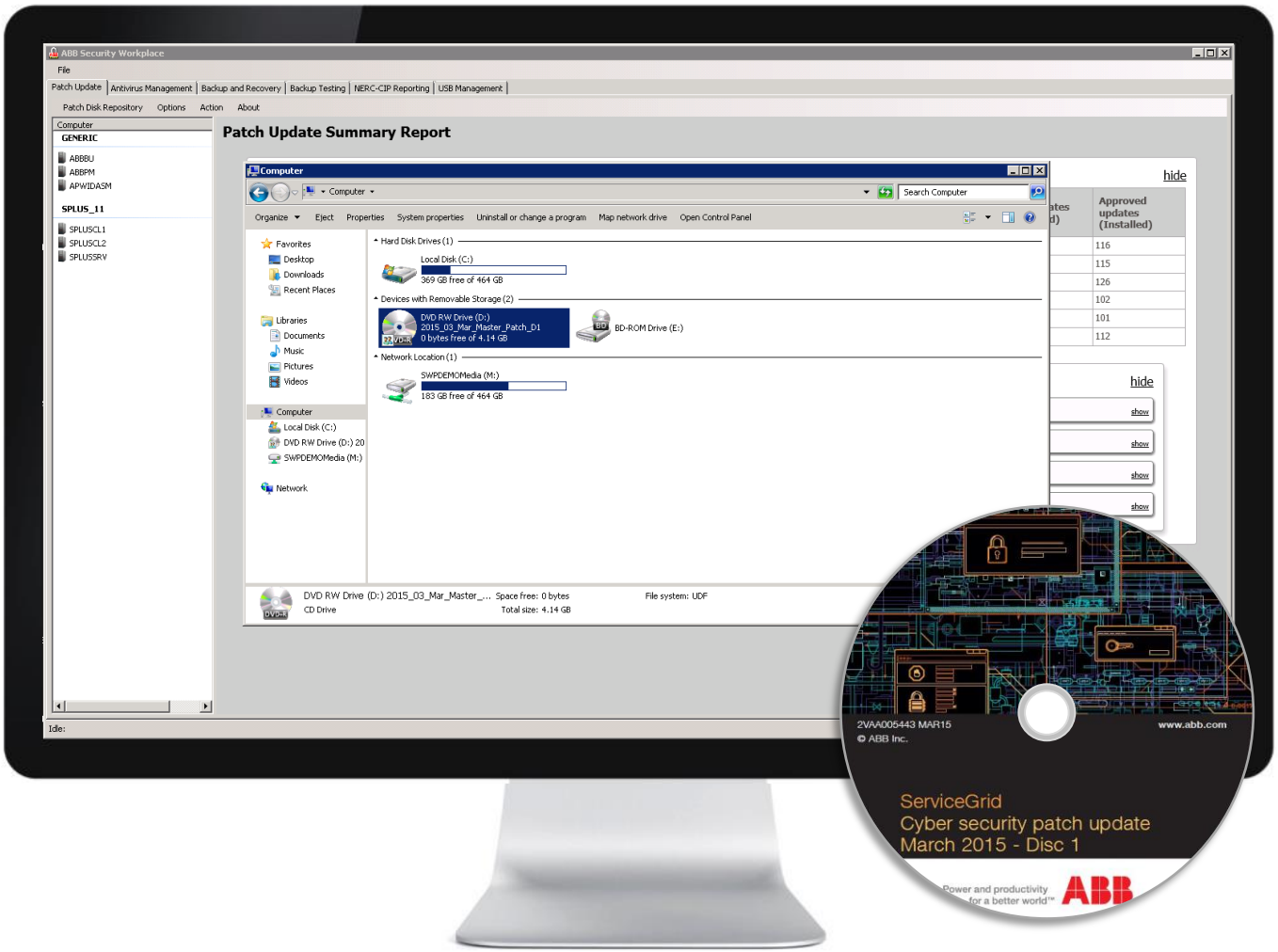


ABB Security Workplace
Maintain - Demonstration

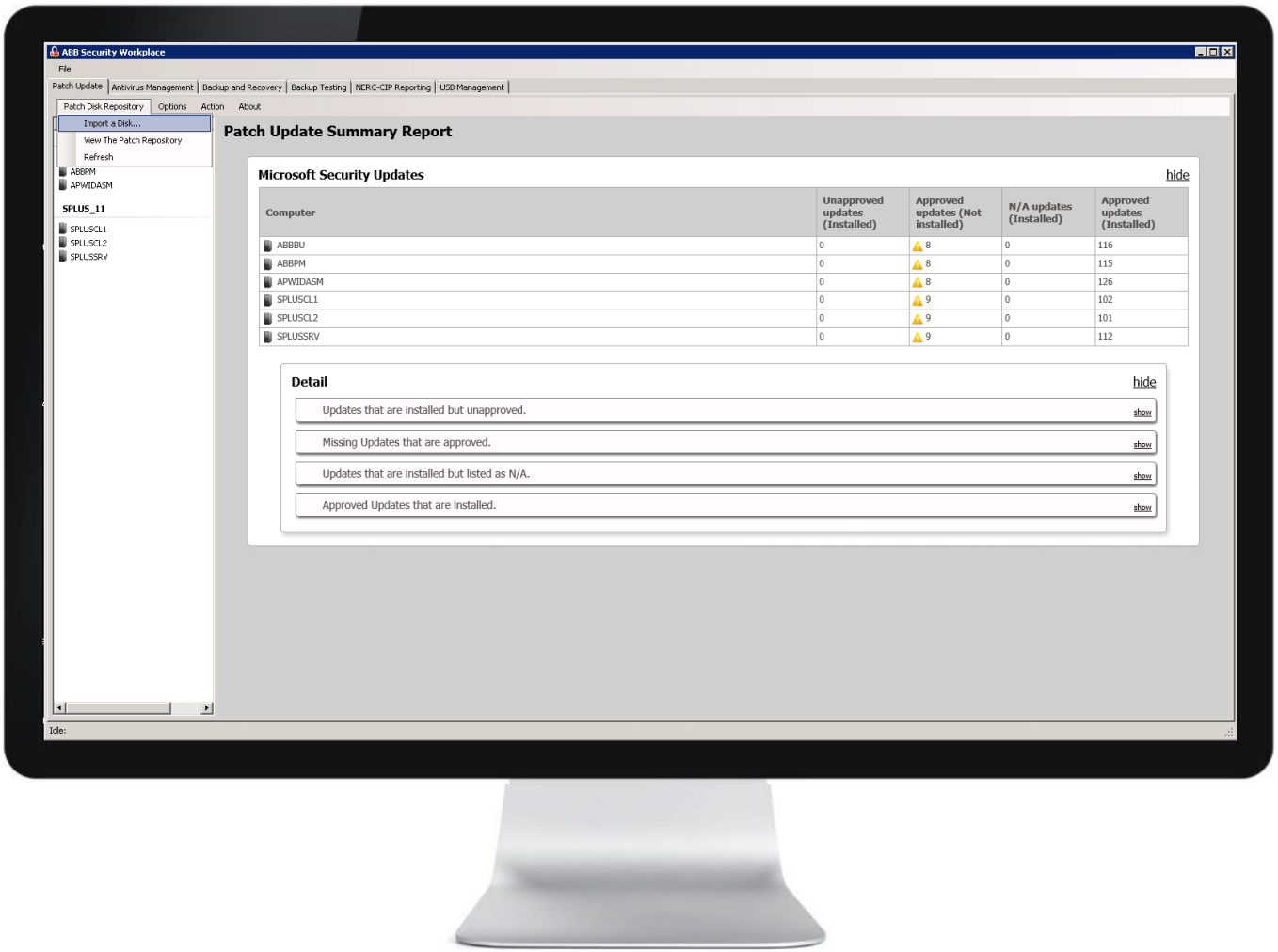


ABB Security Workplace
Maintain - Demonstration

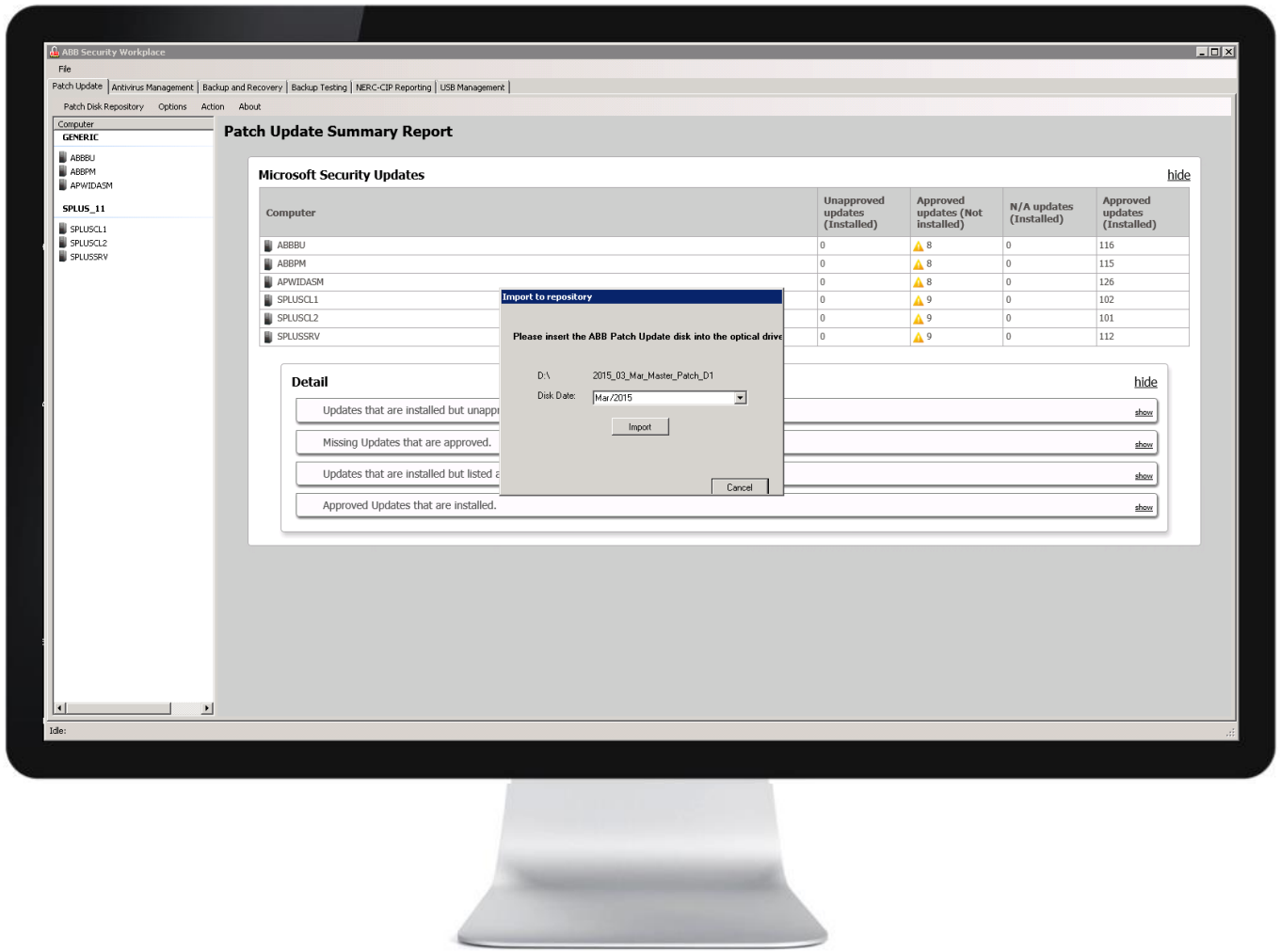


ABB Security Workplace
Maintain - Demonstration

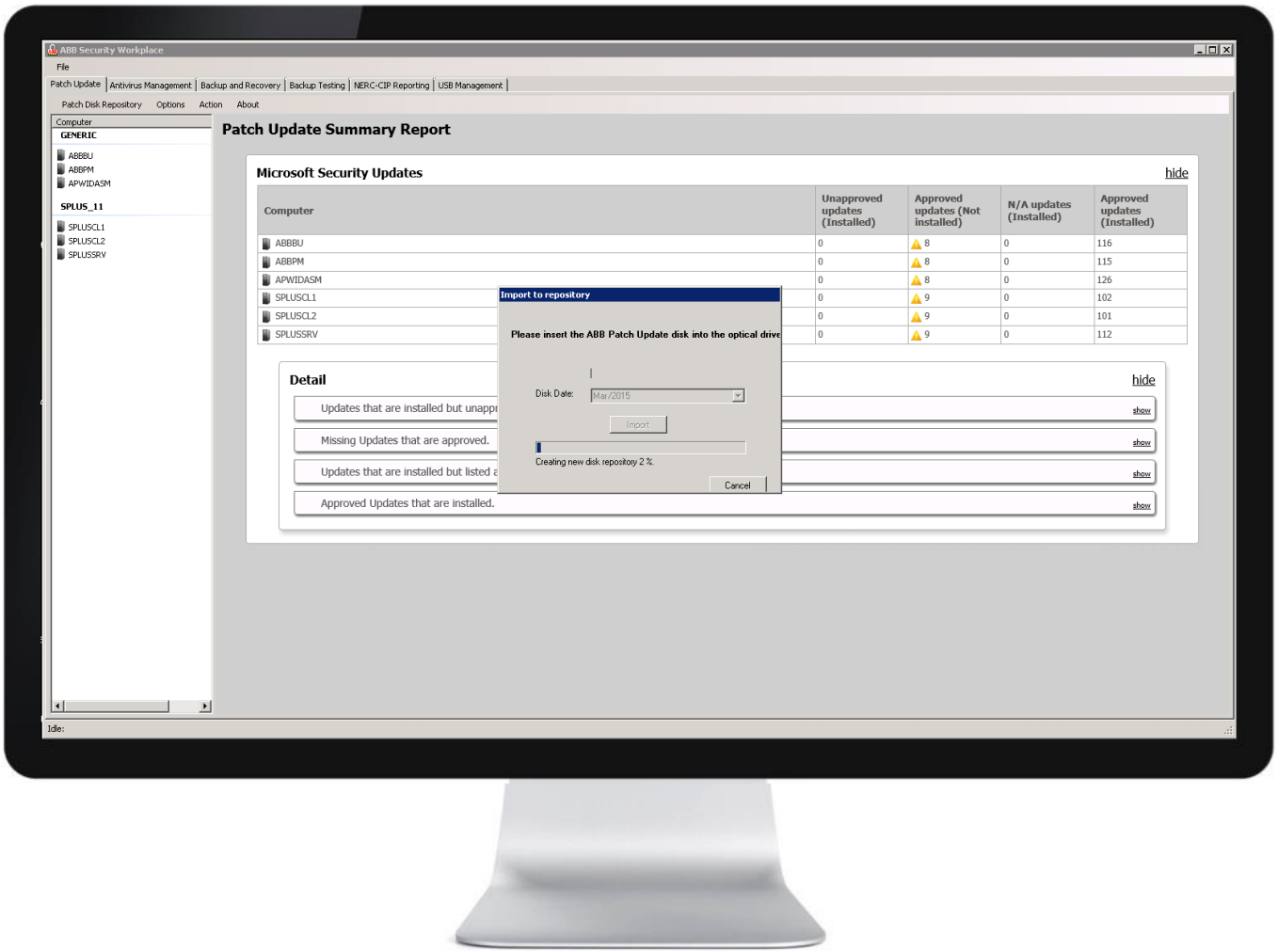


ABB Security Workplace
Maintain - Demonstration

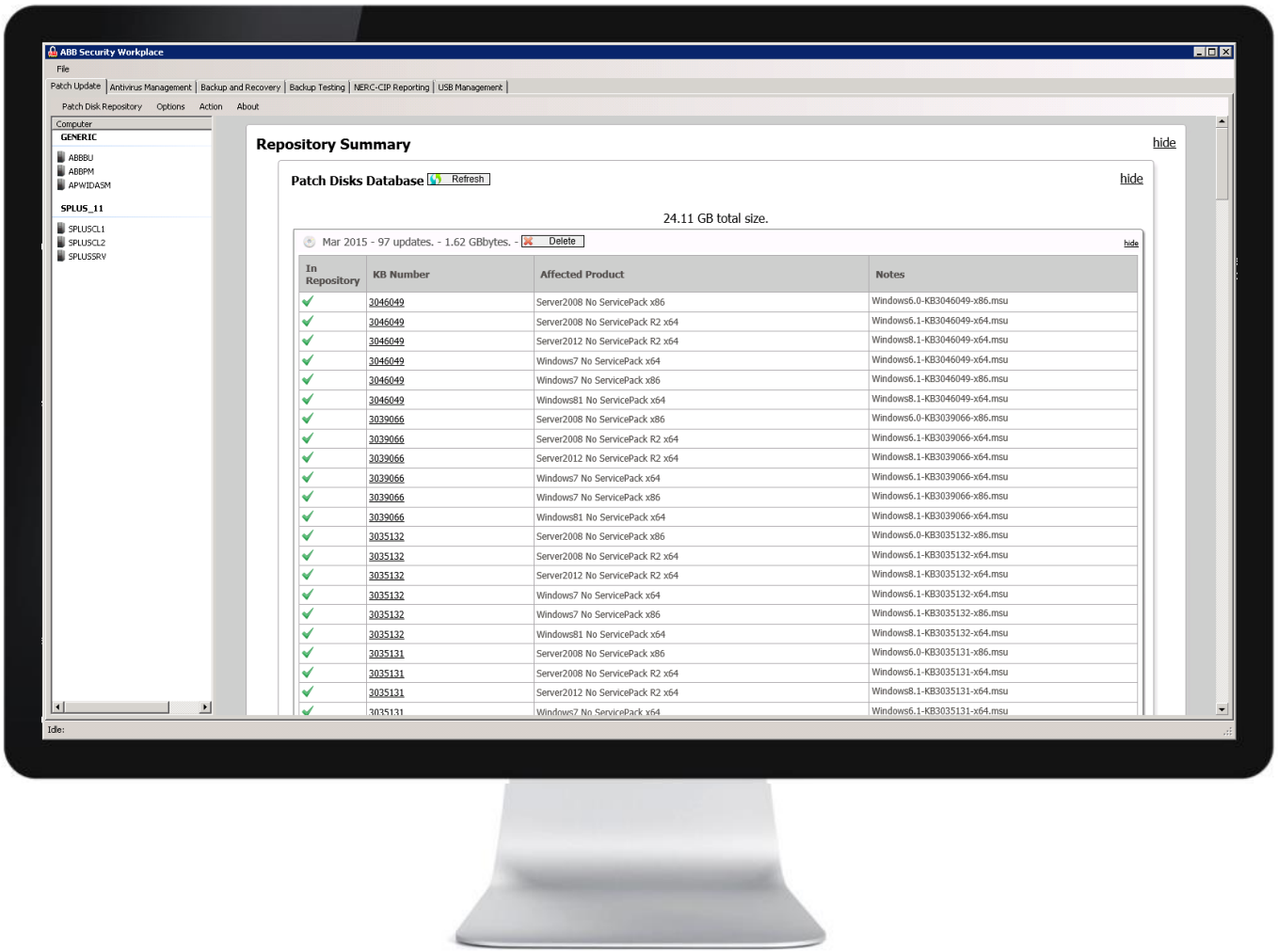


ABB Security Workplace
Maintain - Demonstration

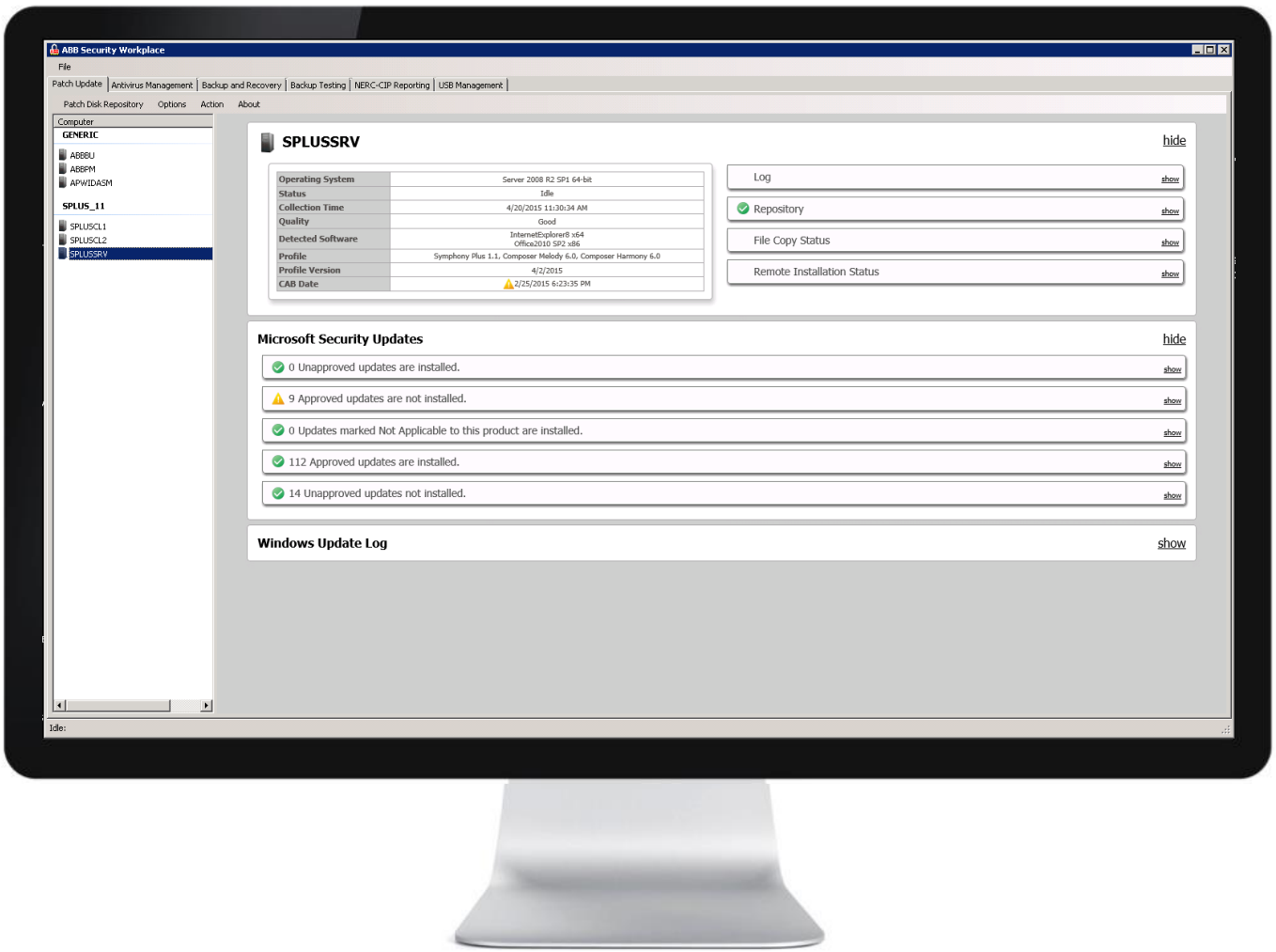


ABB Security Workplace
Maintain - Demonstration

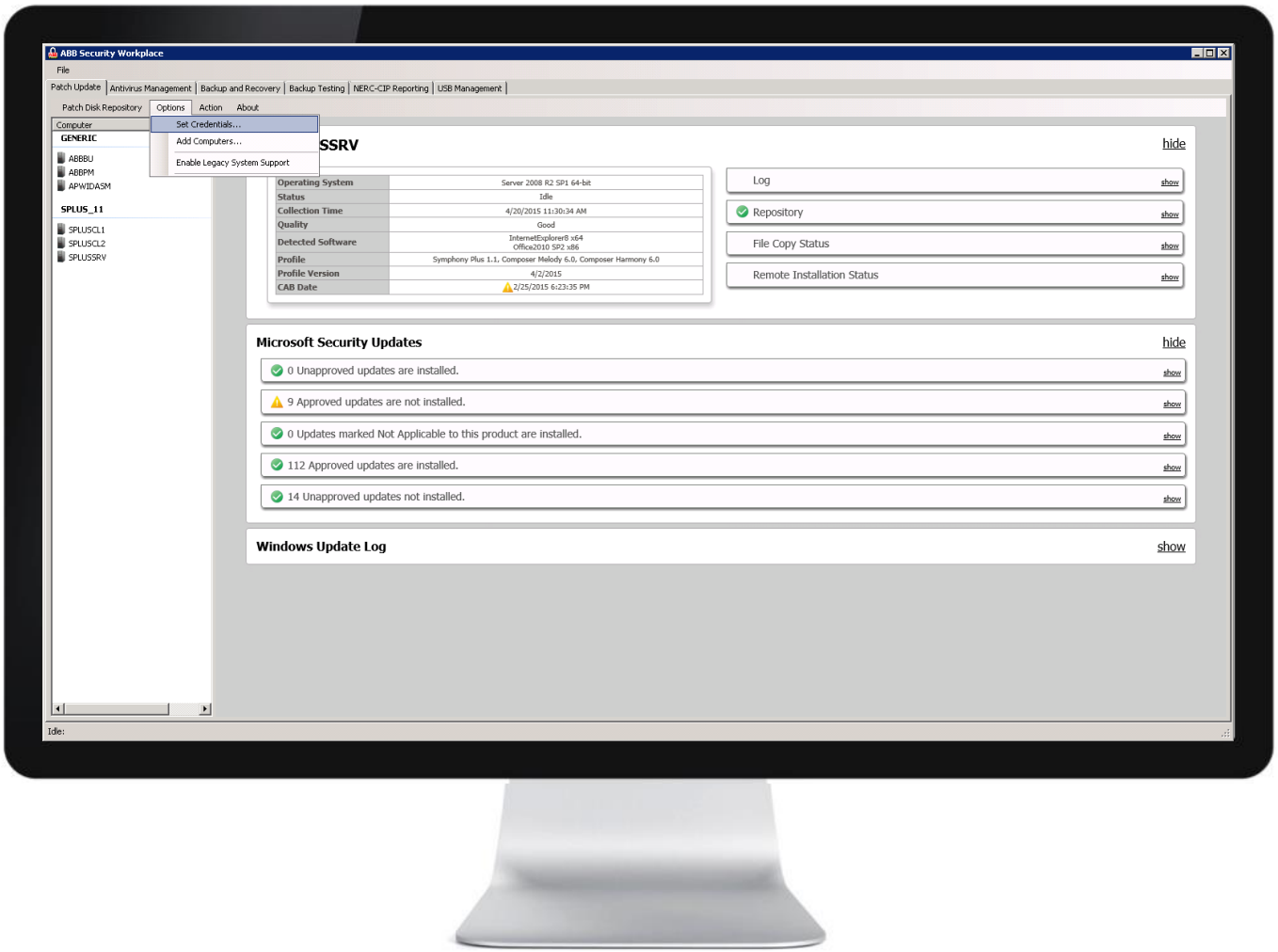


ABB Security Workplace
Maintain - Demonstration

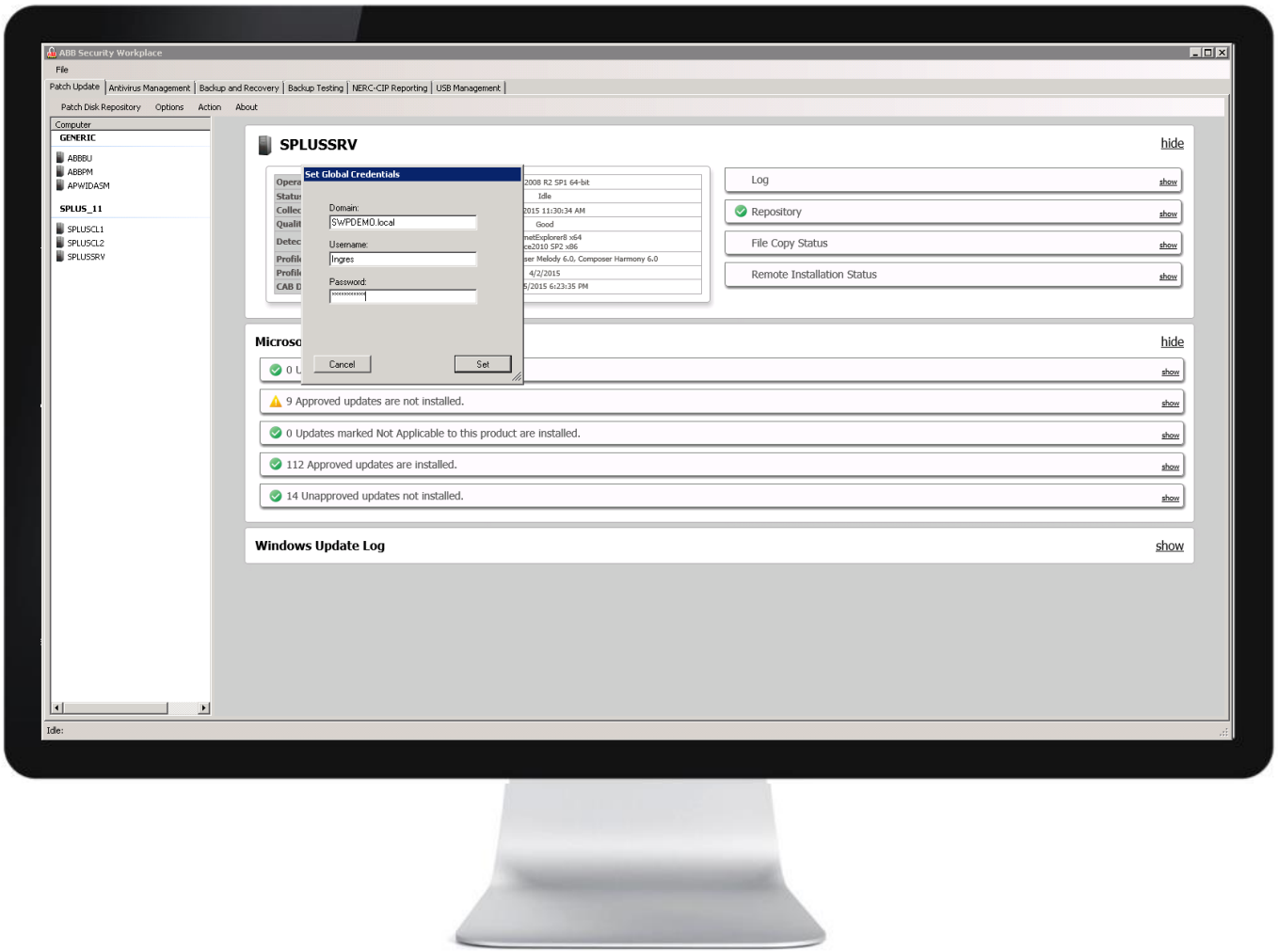


ABB Security Workplace
Maintain - Demonstration

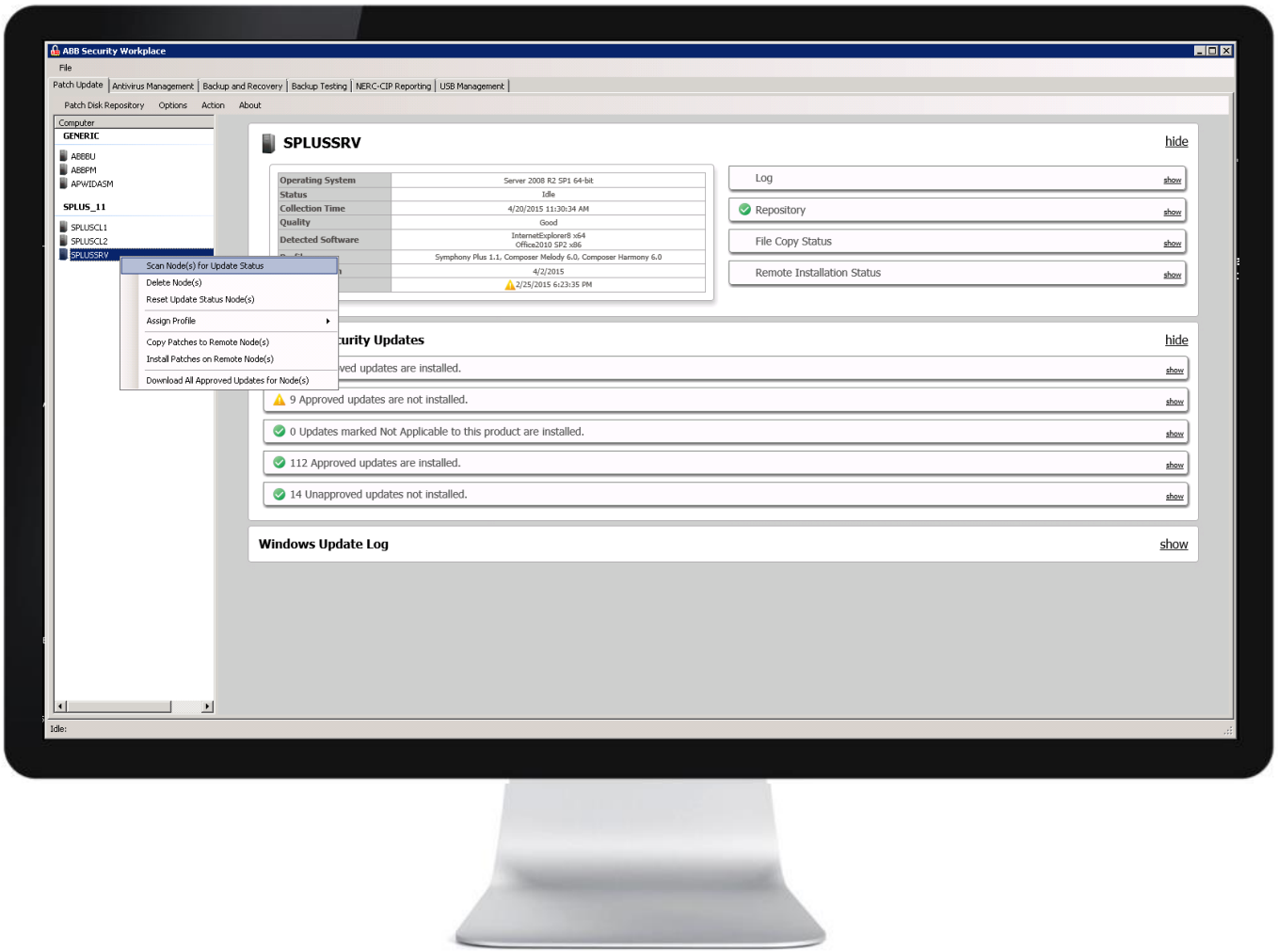


ABB Security Workplace
Maintain - Demonstration

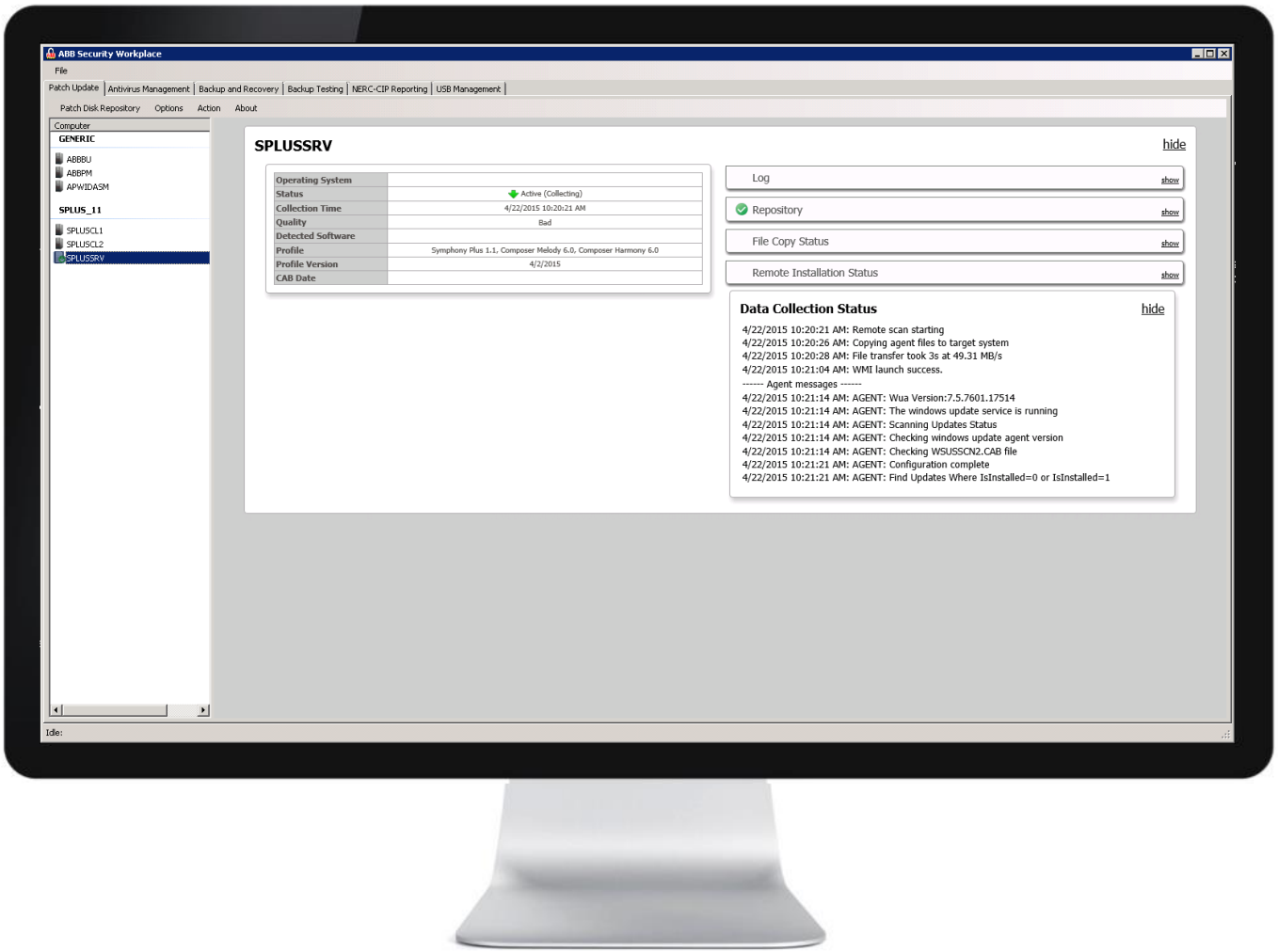


ABB Security Workplace
Maintain - Demonstration

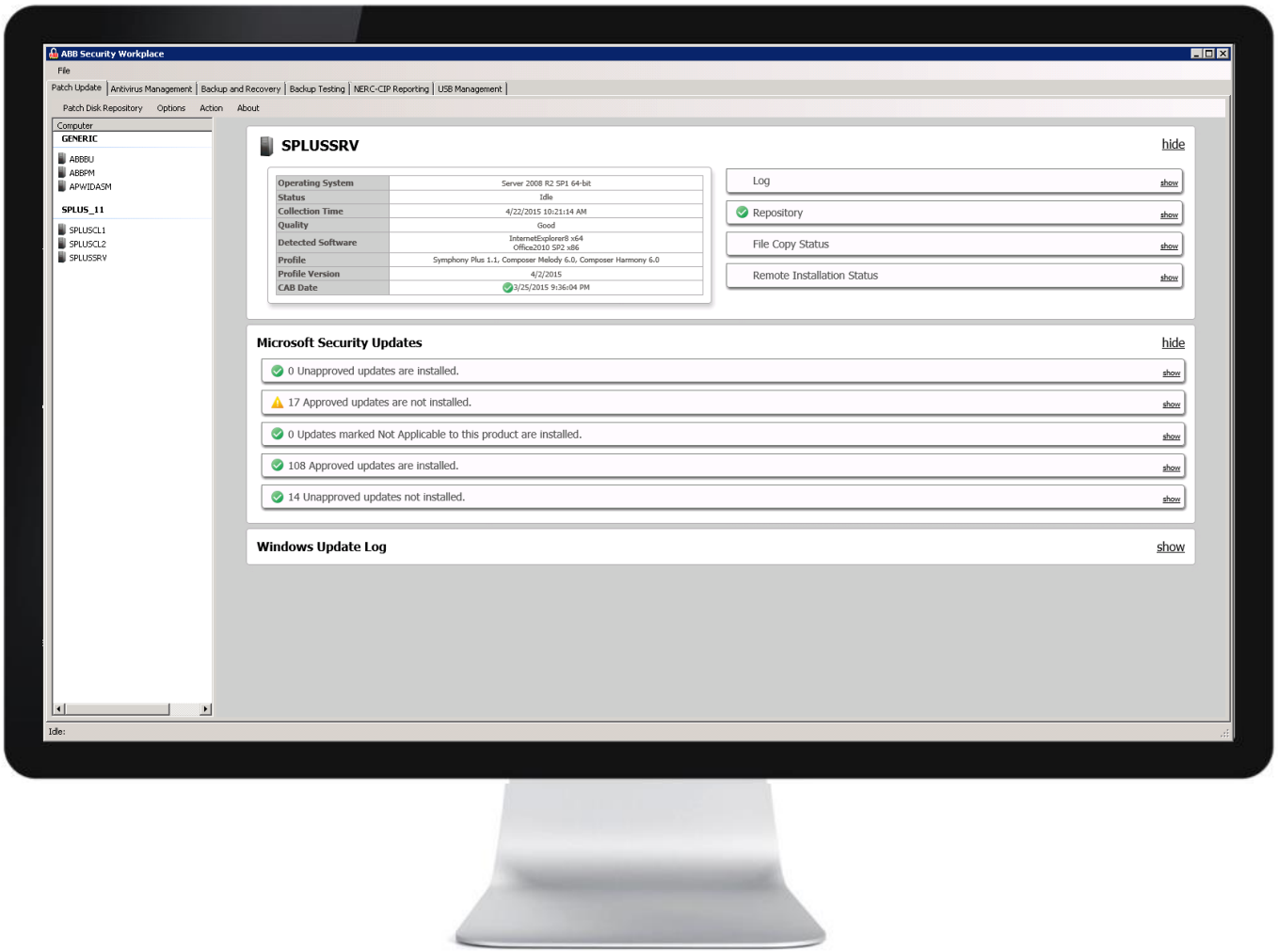


ABB Security Workplace
Maintain - Demonstration

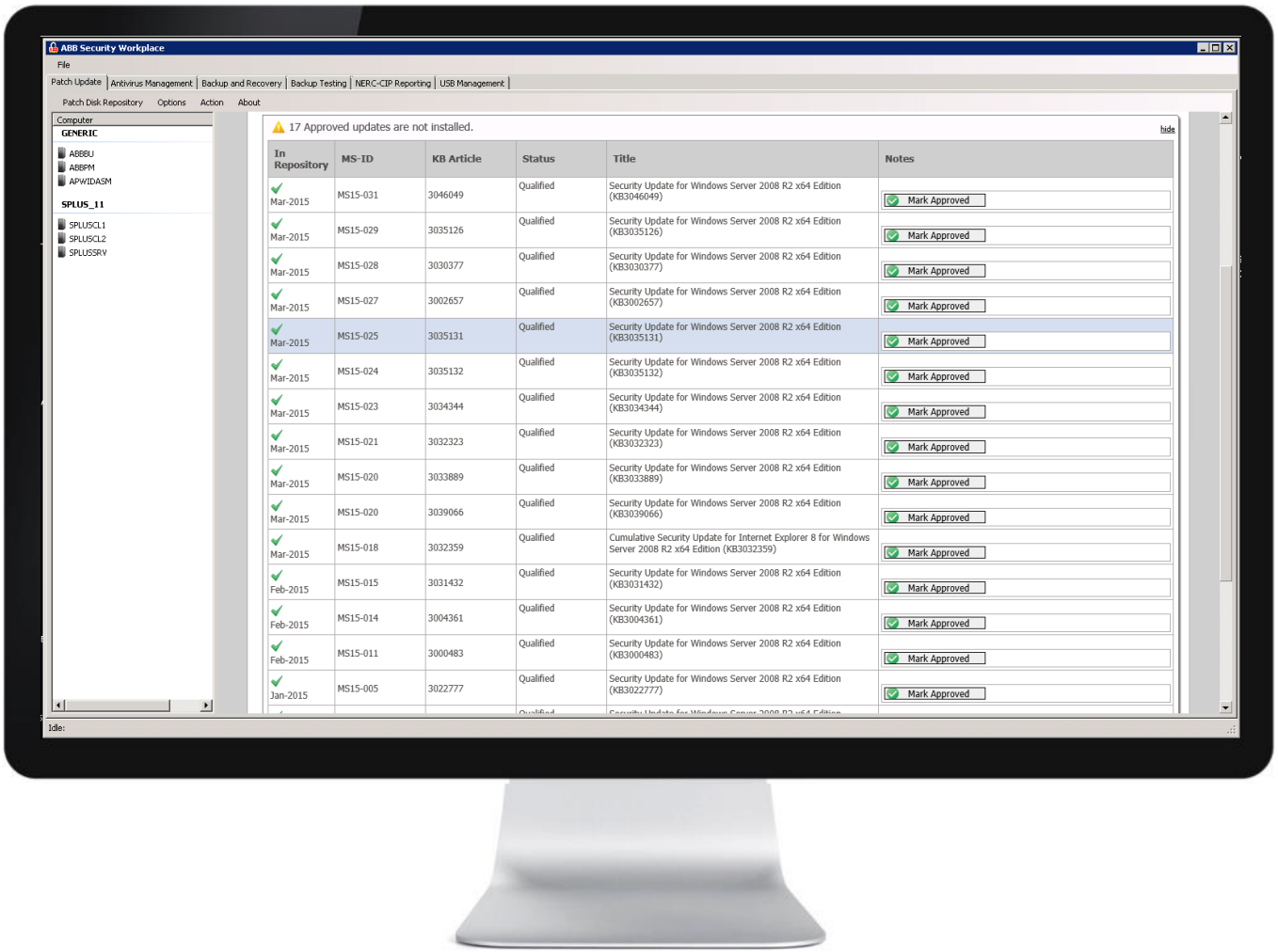


ABB Security Workplace
Maintain - Demonstration

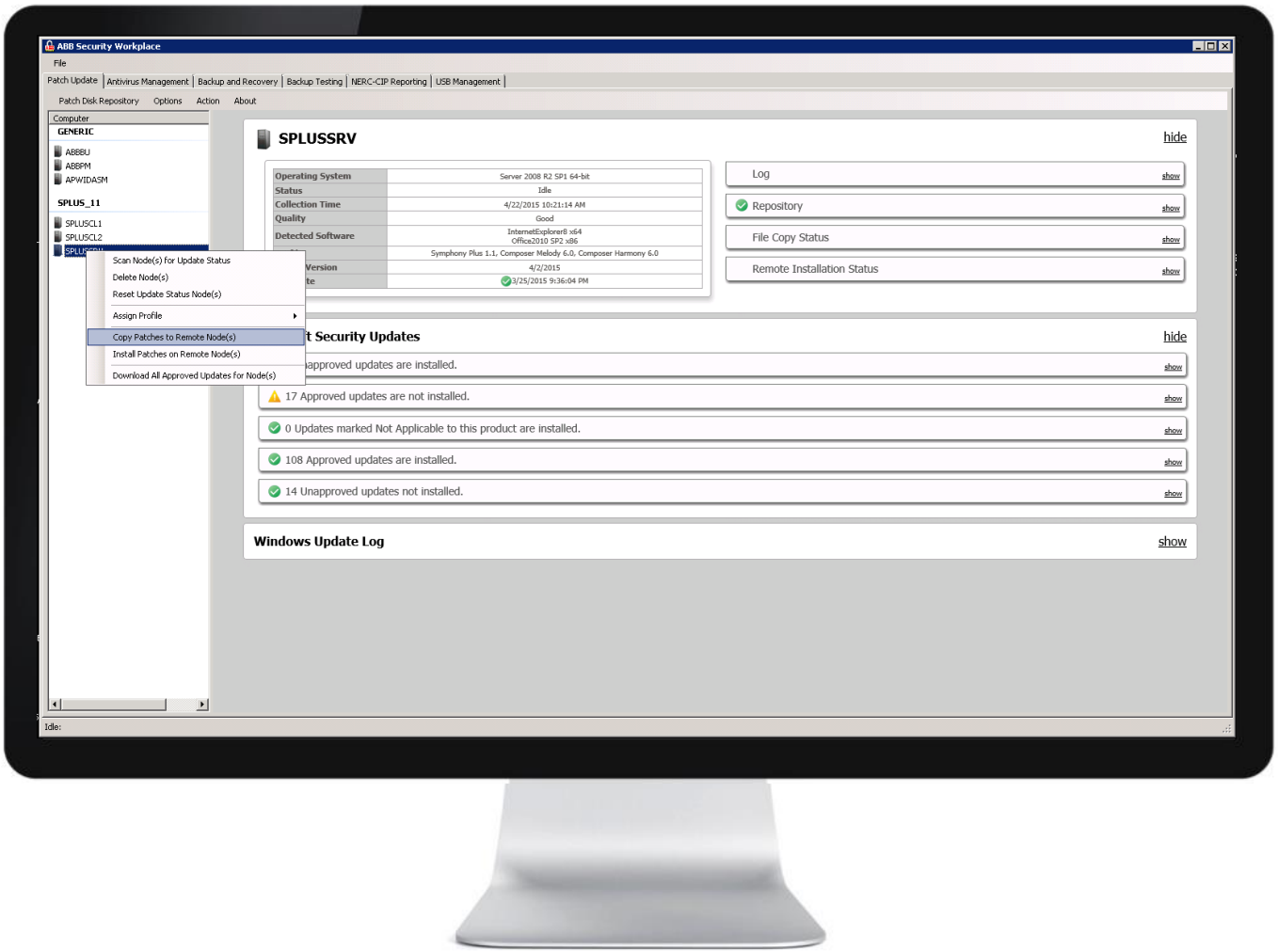


ABB Security Workplace
Maintain - Demonstration

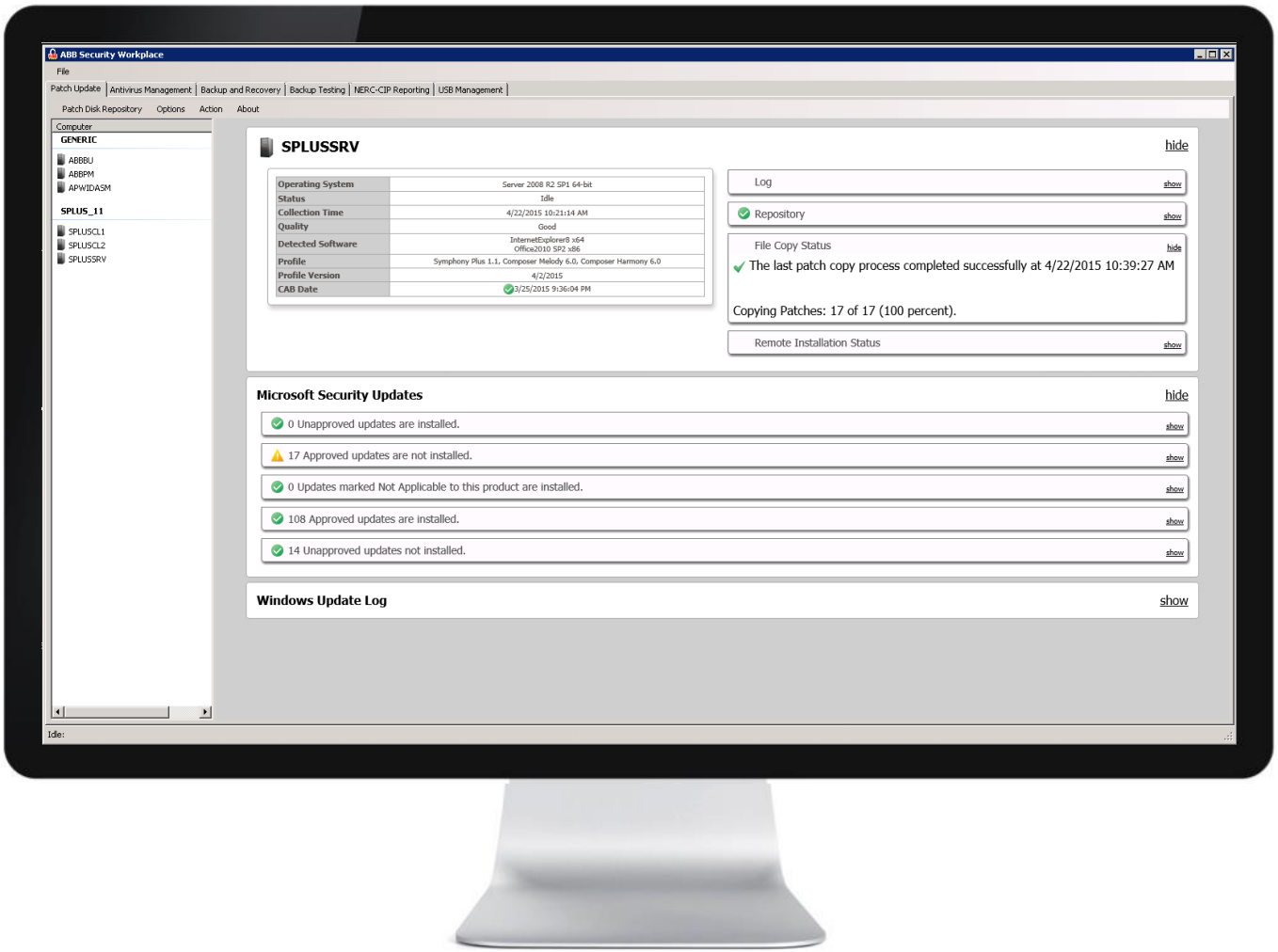


ABB Security Workplace
Maintain - Demonstration

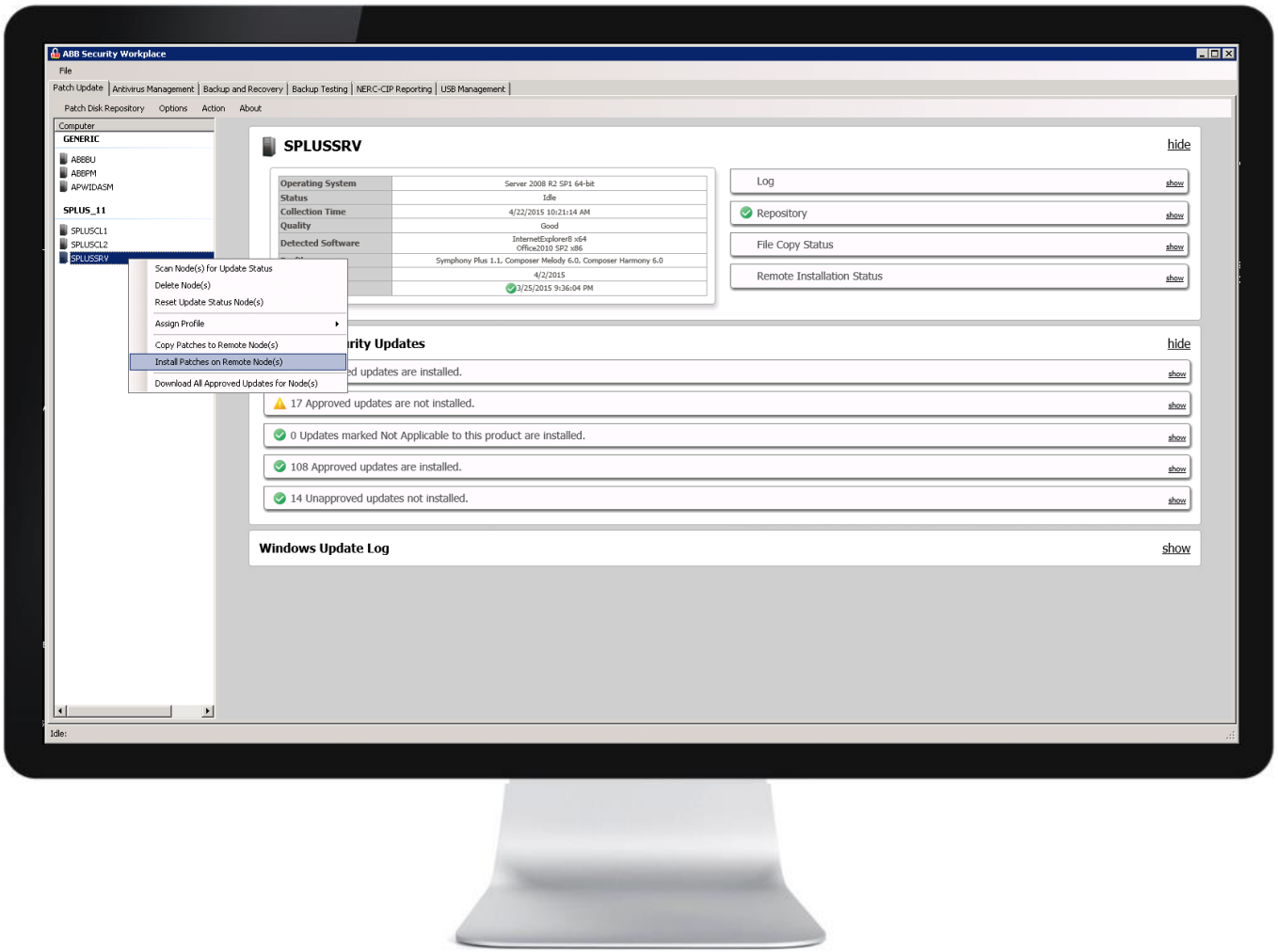


ABB Security Workplace
Maintain - Demonstration

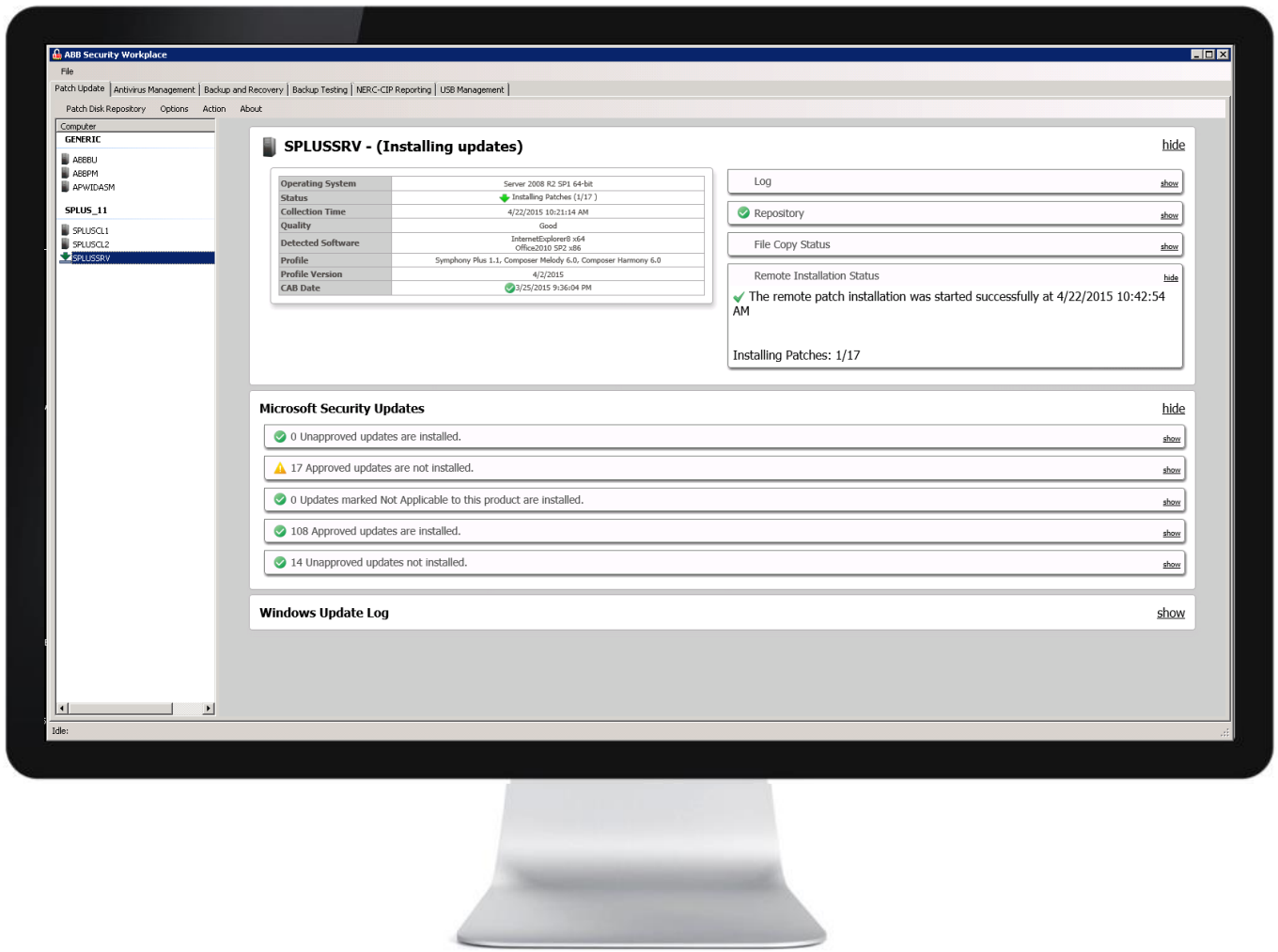


ABB Security Workplace
Maintain - Demonstration

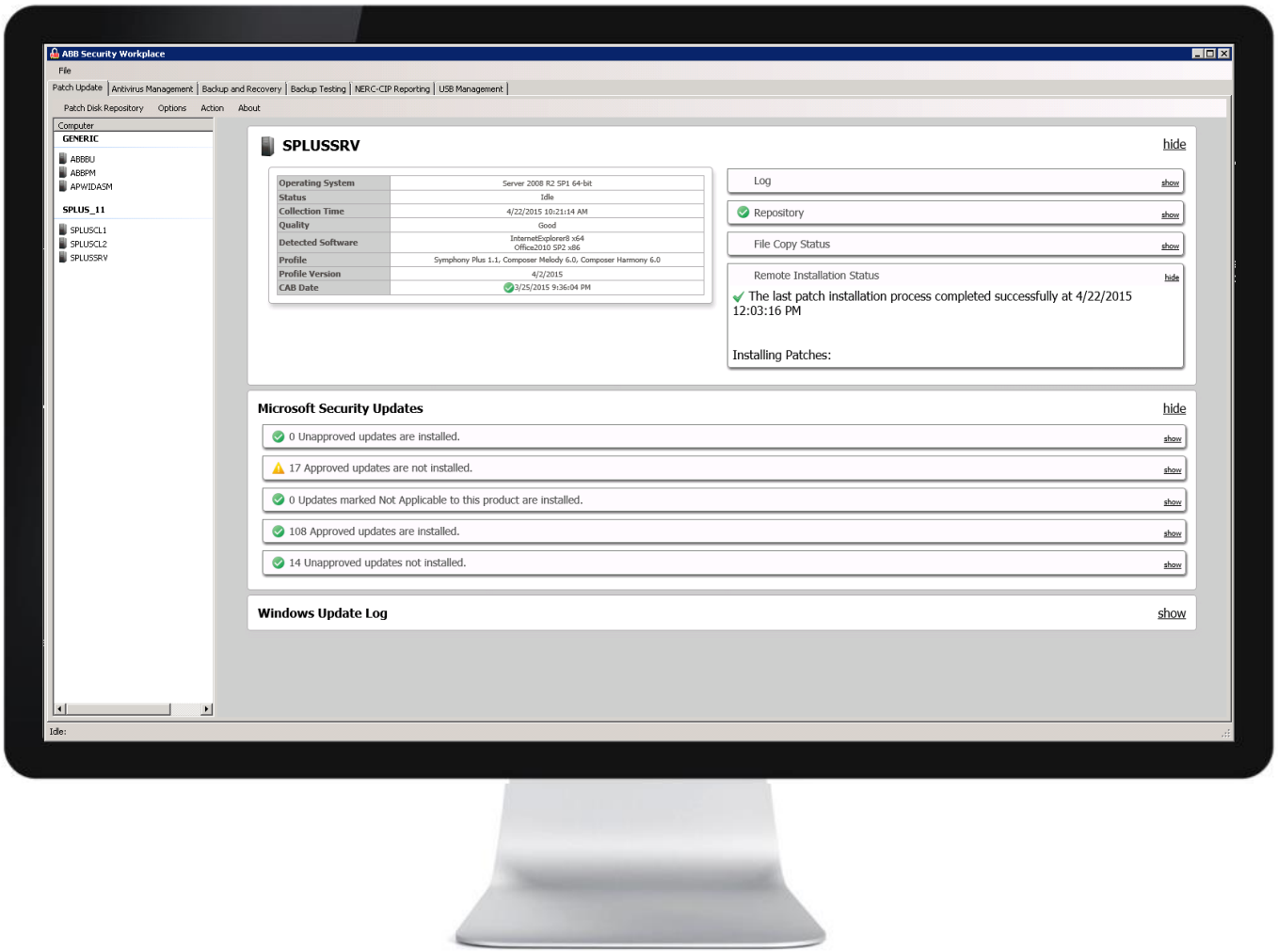


ABB Security Workplace
Maintain - Demonstration

ABB Security Workplace
Maintain - Demonstration

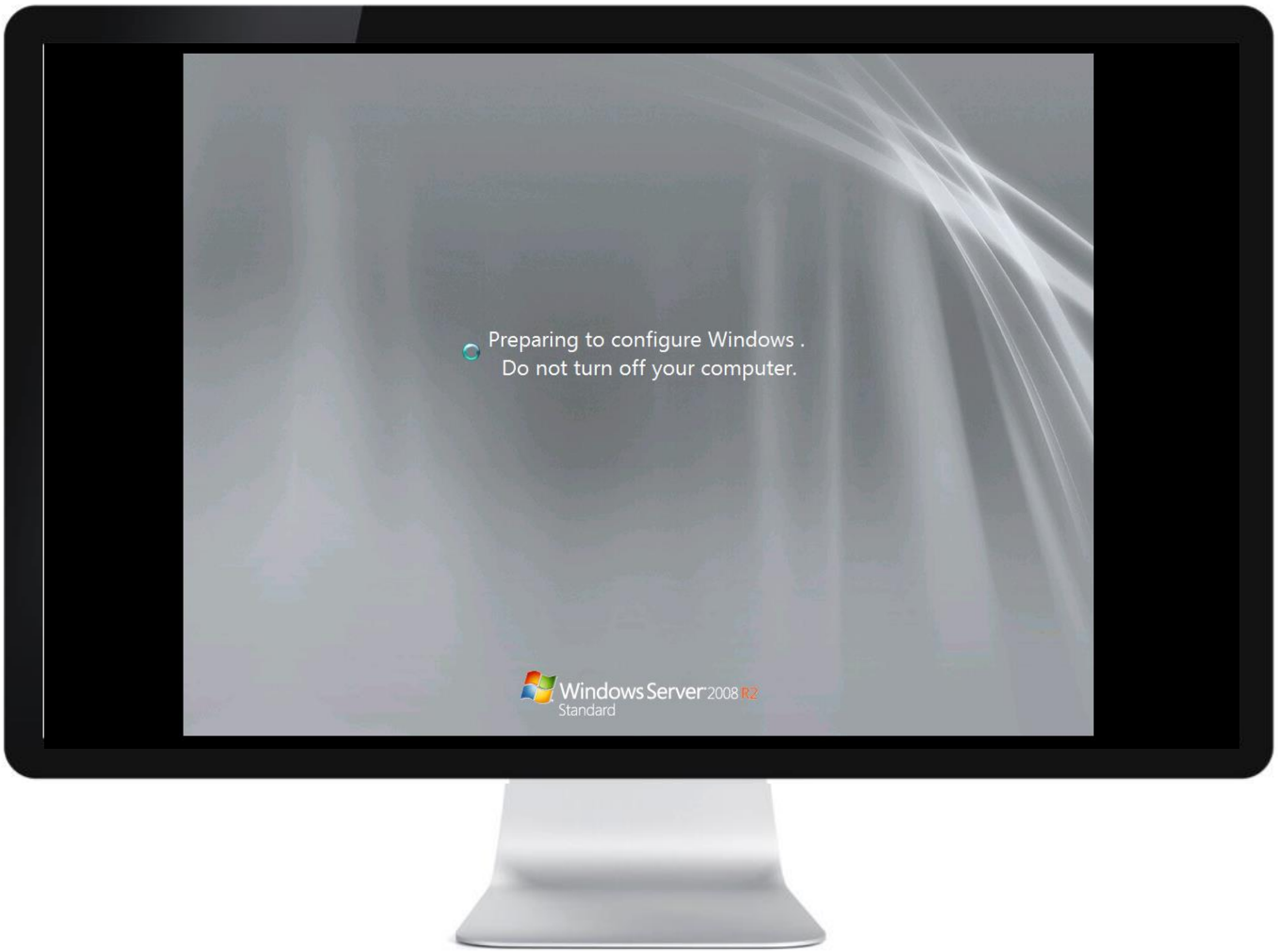


ABB Security Workplace
Maintain - Demonstration

ABB Security Workplace
Maintain - Demonstration

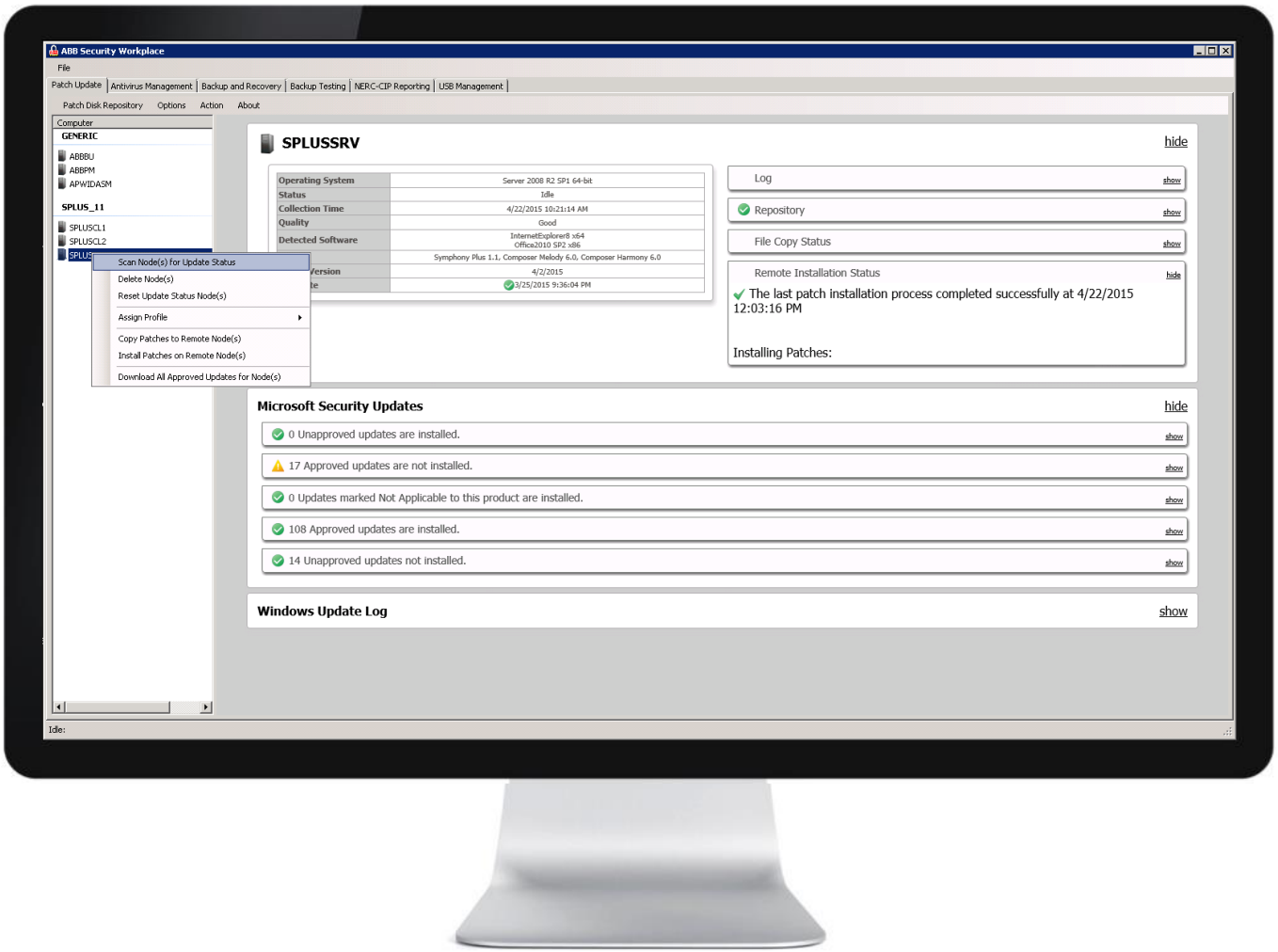


ABB Security Workplace
Maintain - Demonstration

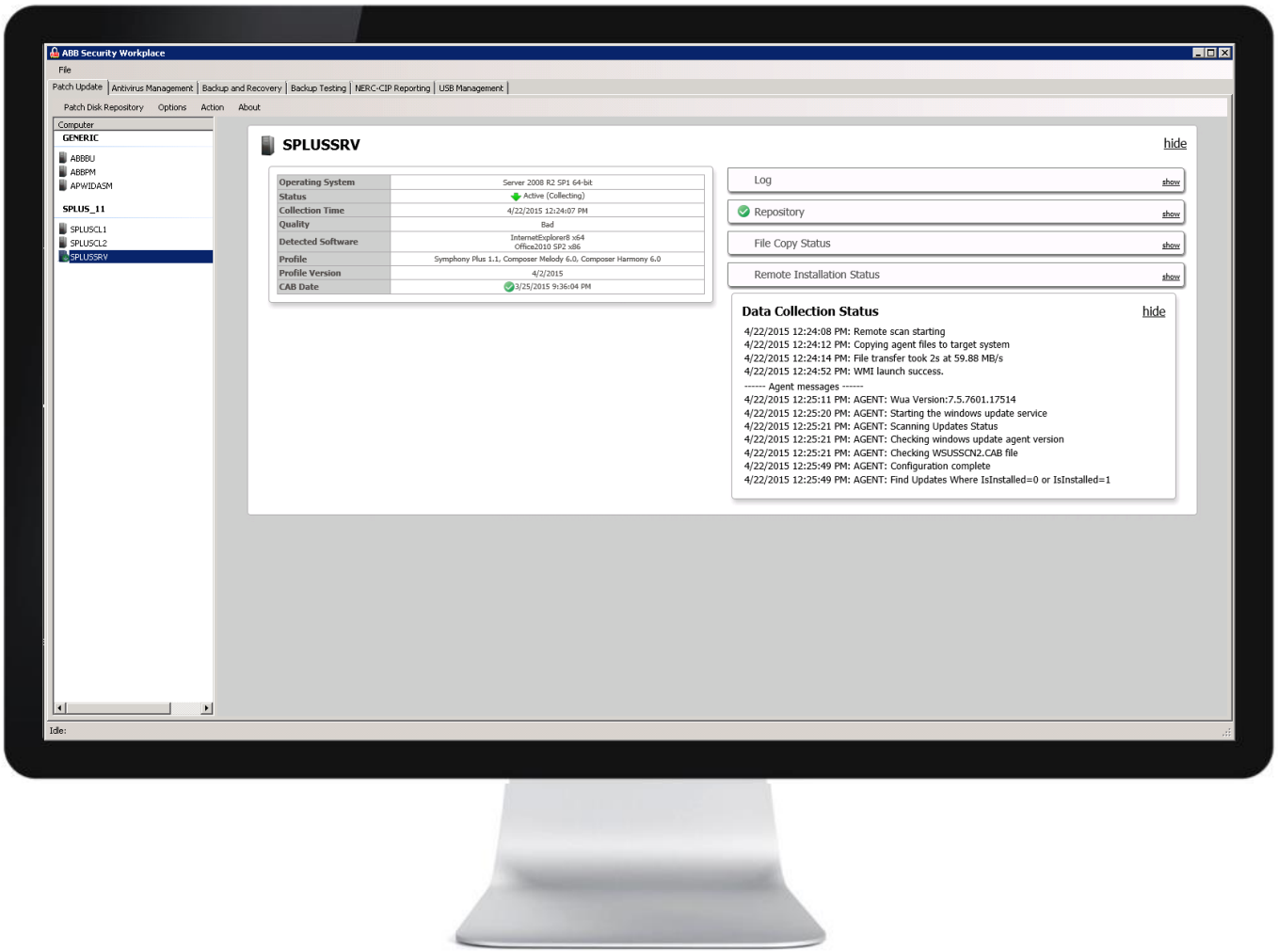


ABB Security Workplace
Maintain - Demonstration

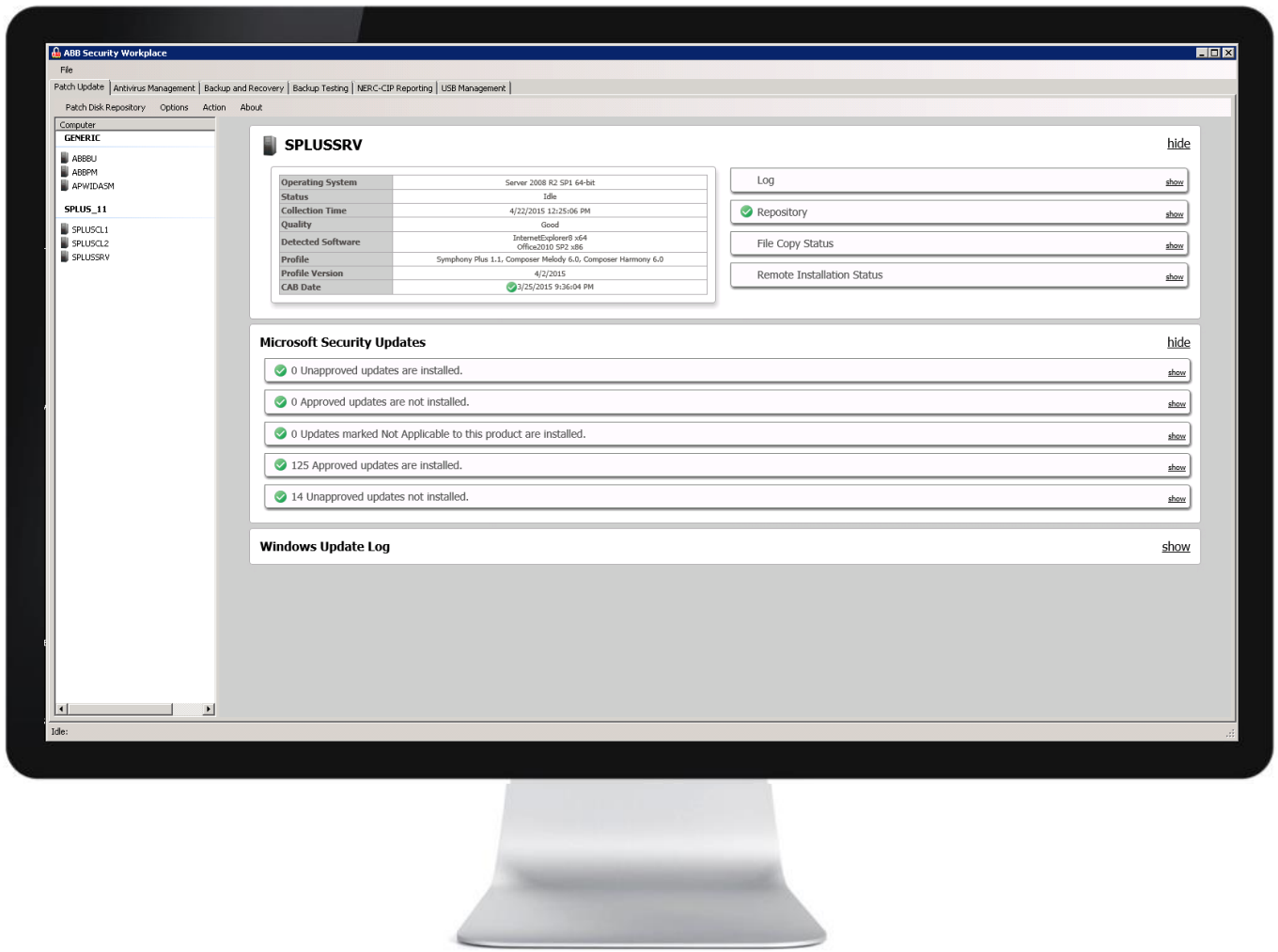


ABB Security Workplace
Maintain - Demonstration

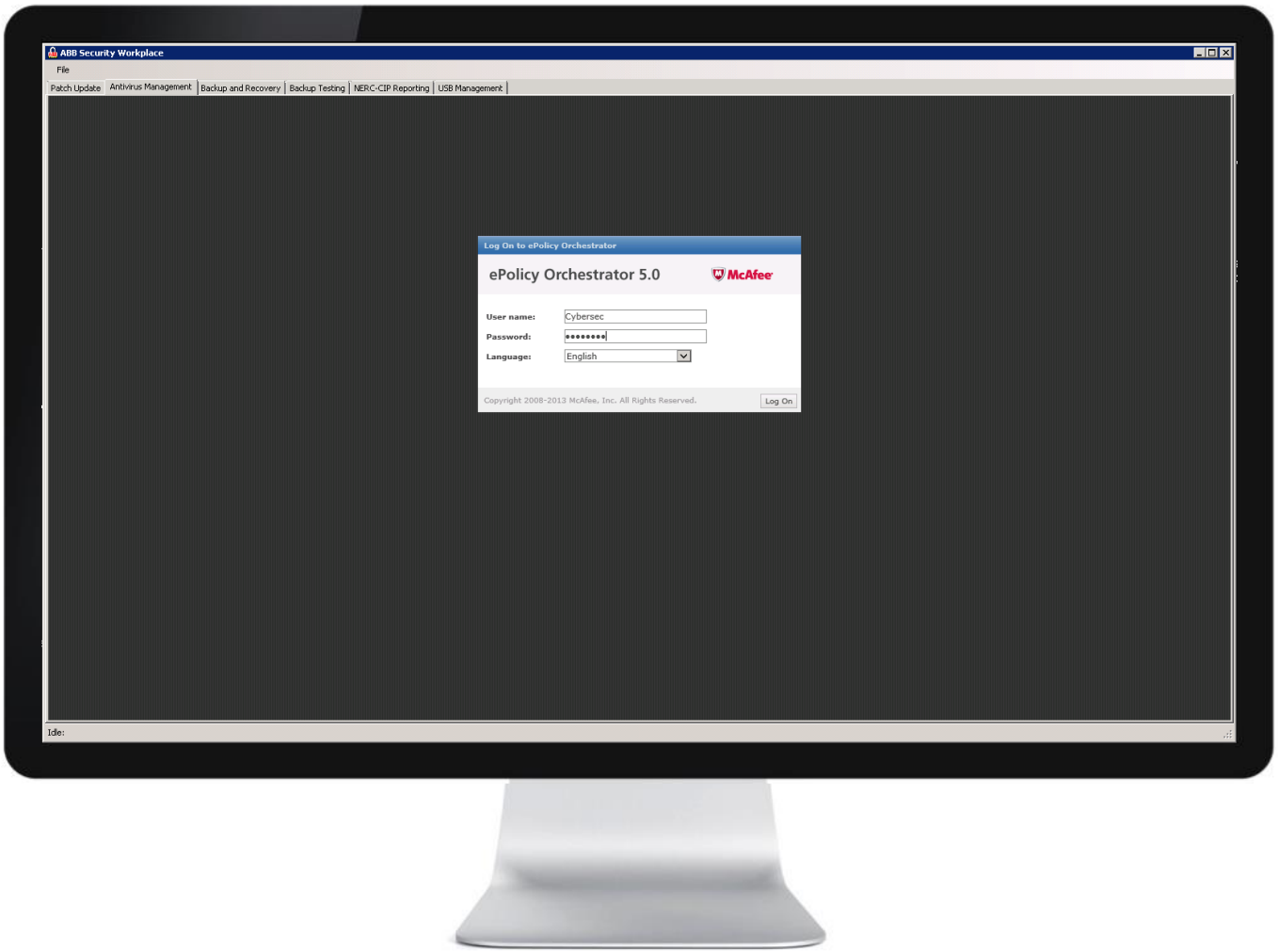


ABB Security Workplace
Maintain - Demonstration

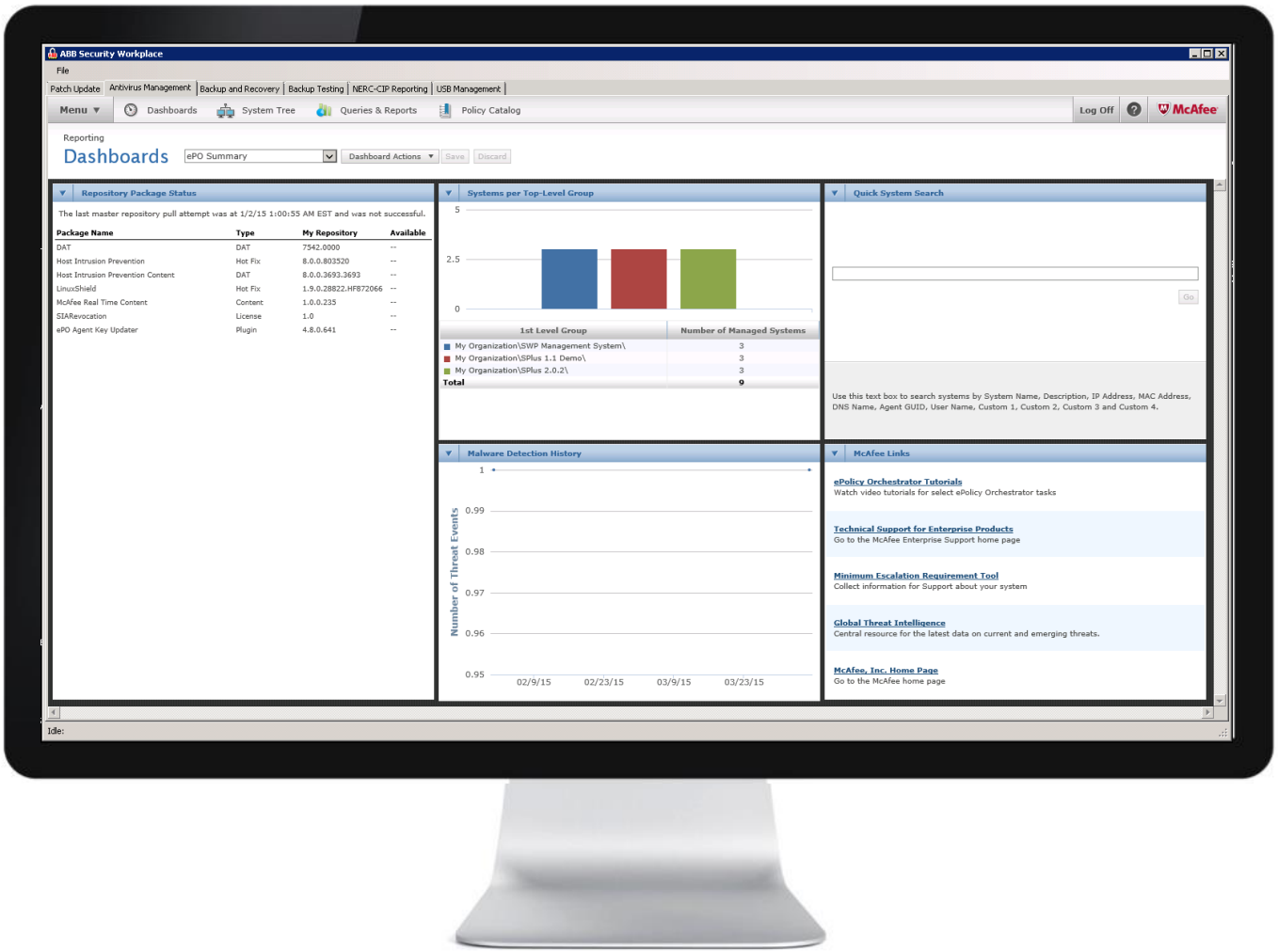


ABB Security Workplace
Maintain - Demonstration

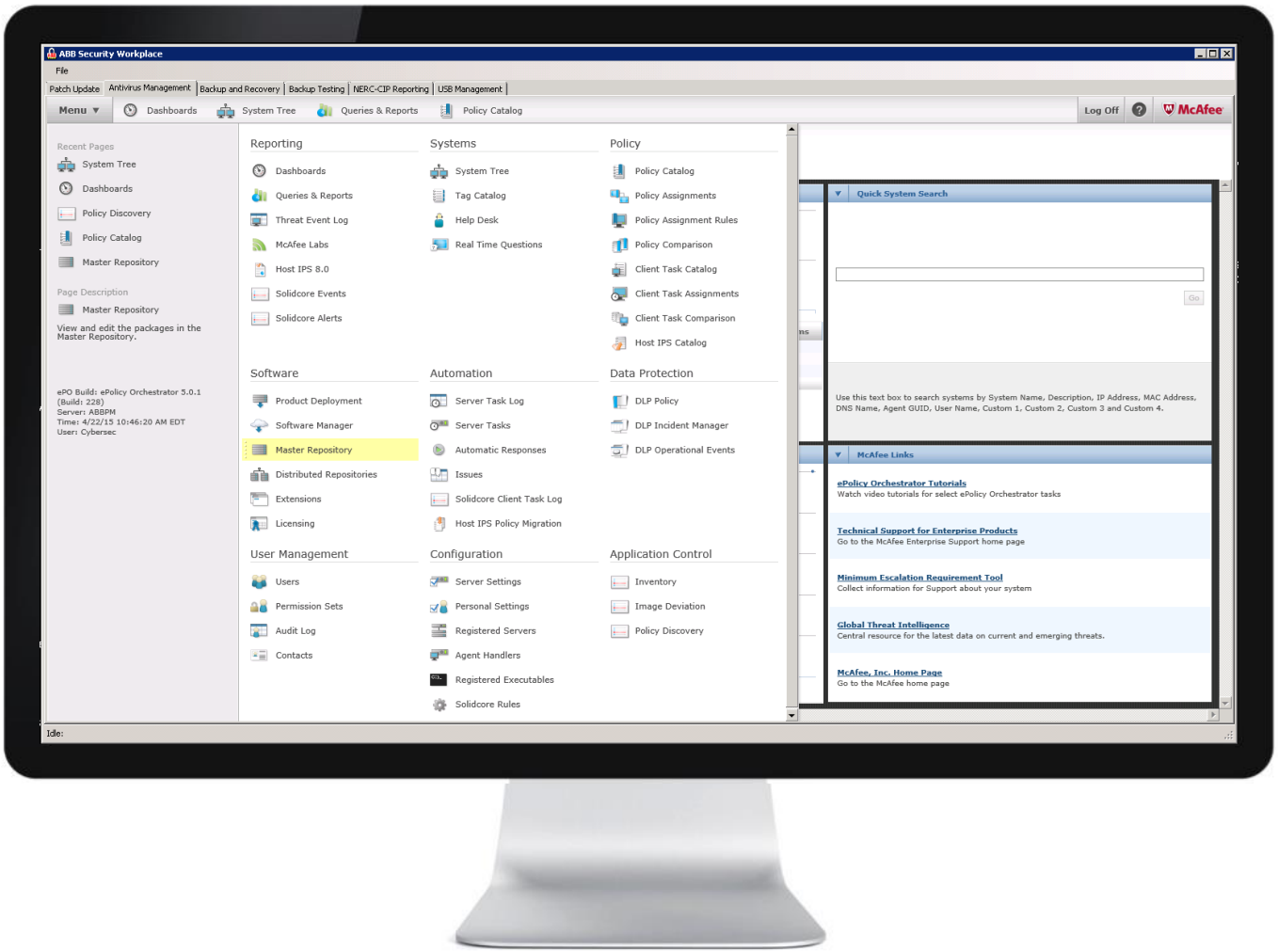


ABB Security Workplace
Maintain - Demonstration

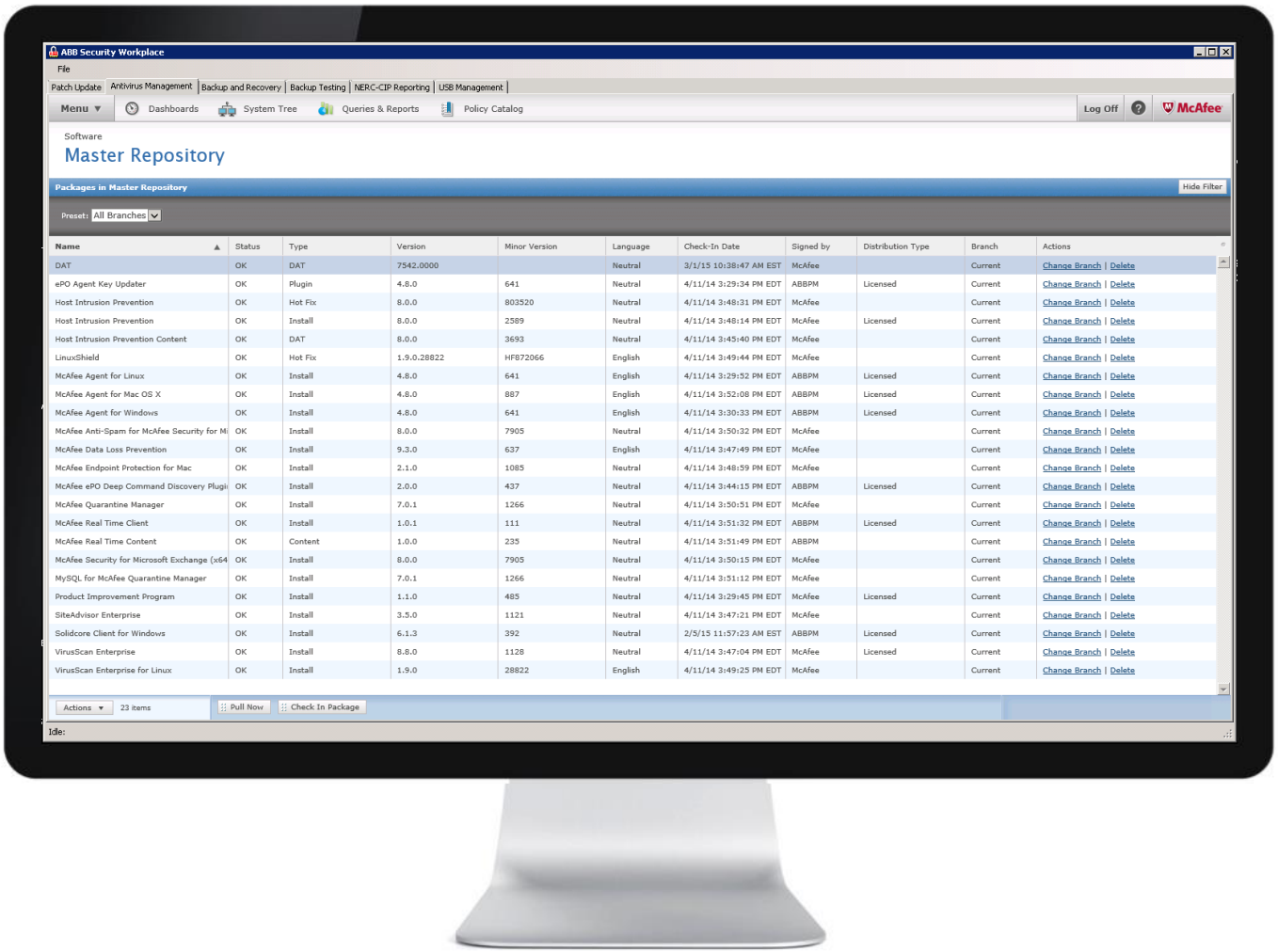


ABB Security Workplace
Maintain - Demonstration

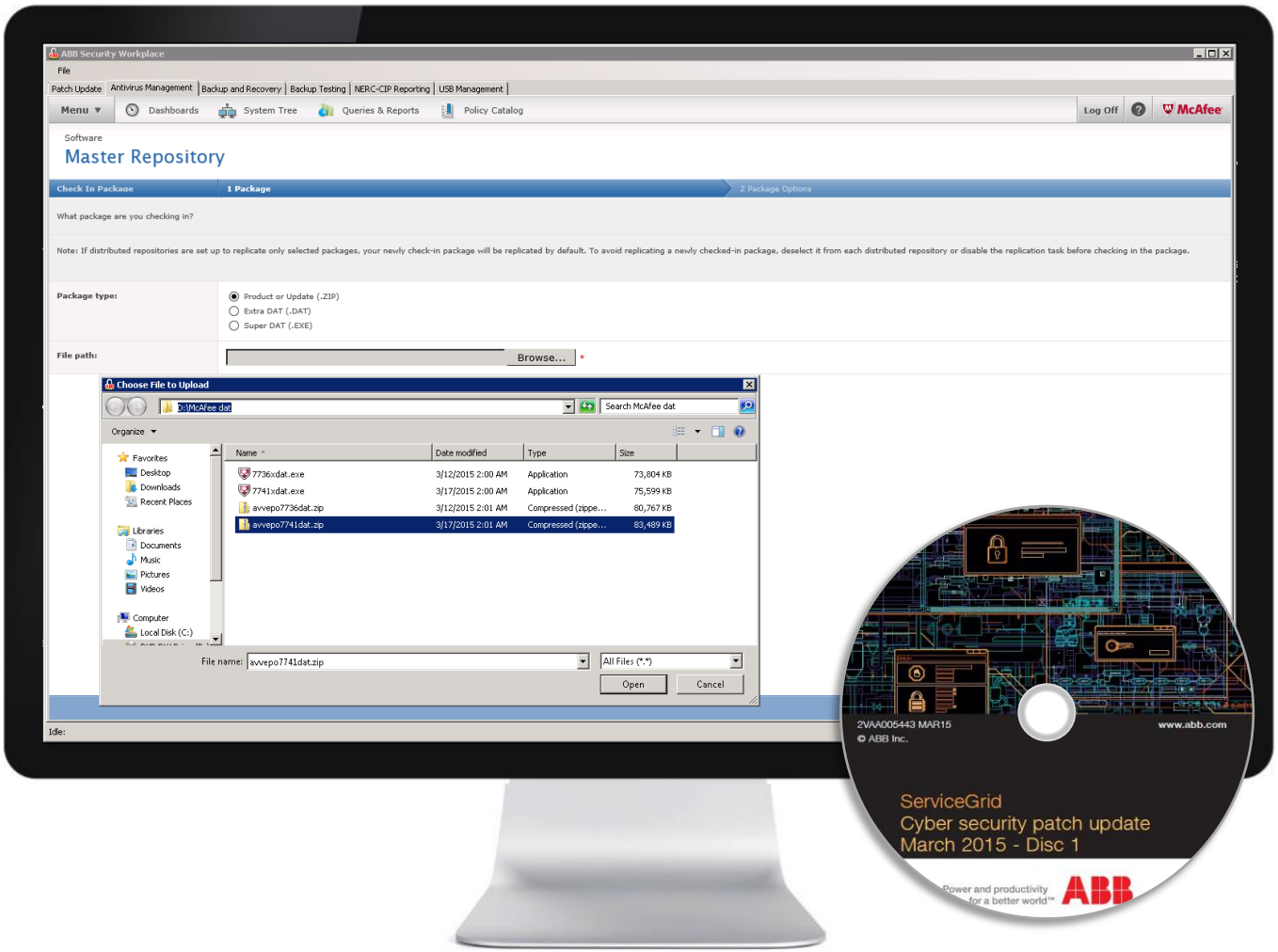


ABB Security Workplace
Maintain - Demonstration

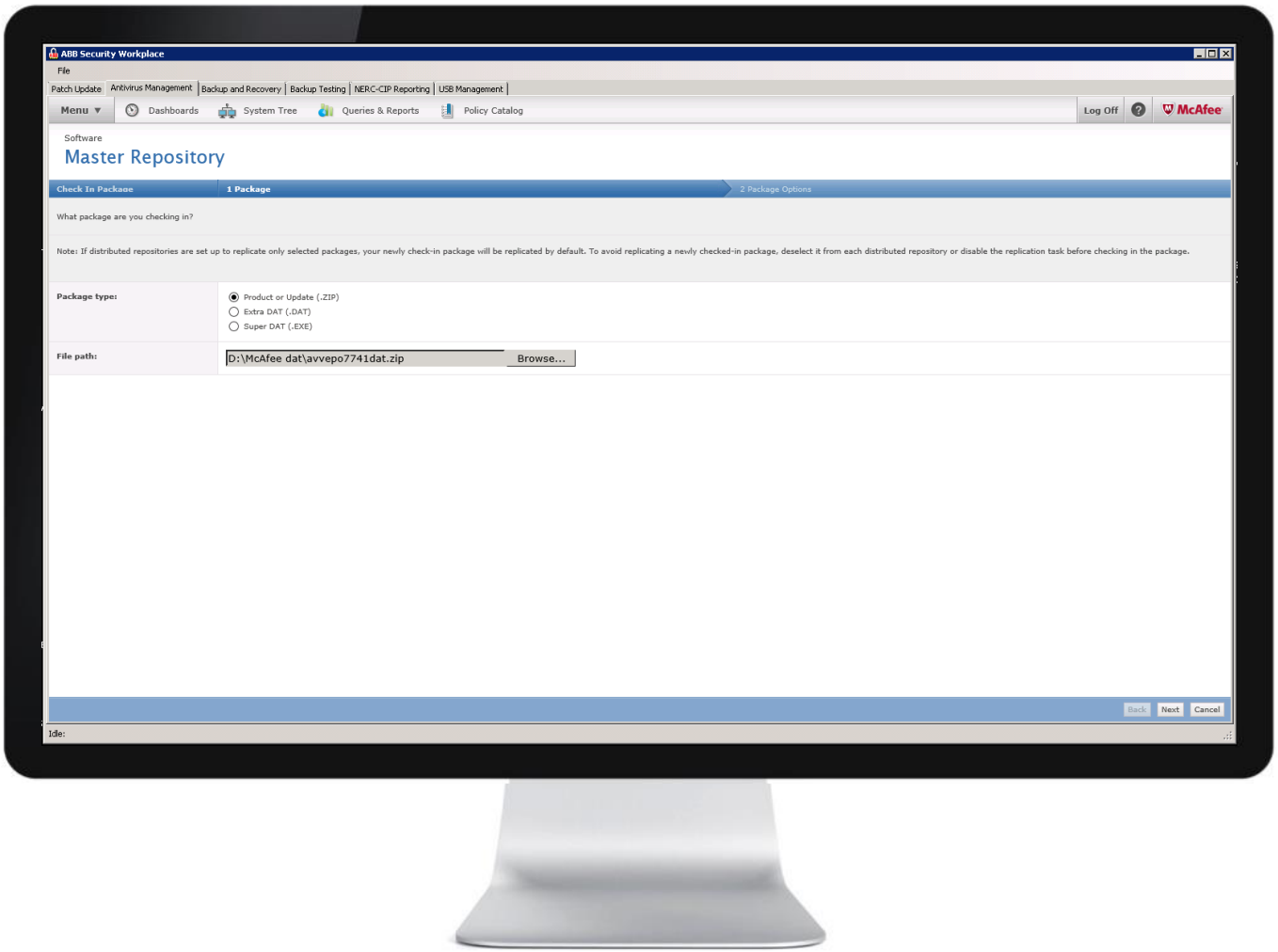


ABB Security Workplace
Maintain - Demonstration

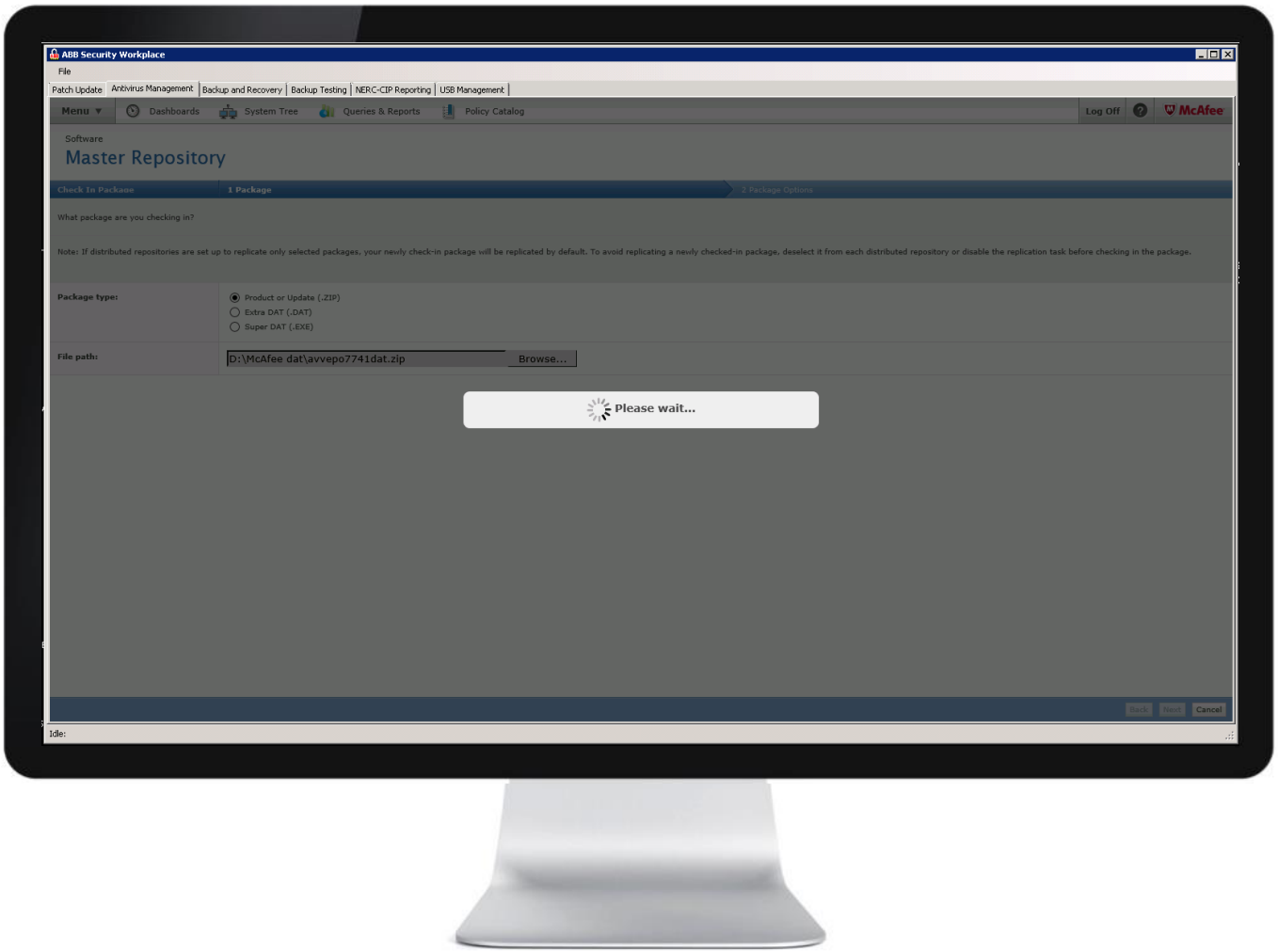


ABB Security Workplace
Maintain - Demonstration

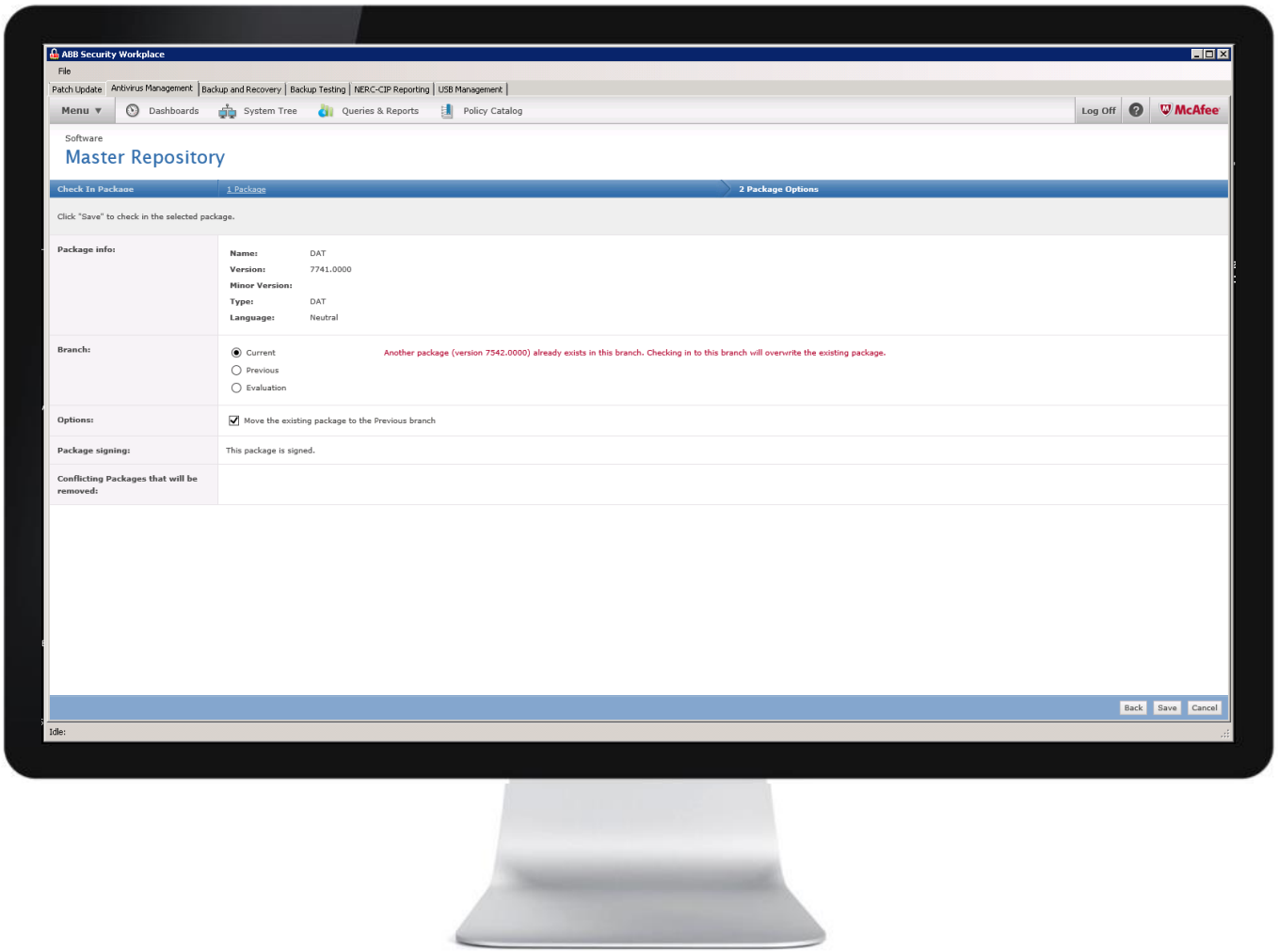


ABB Security Workplace
Maintain - Demonstration

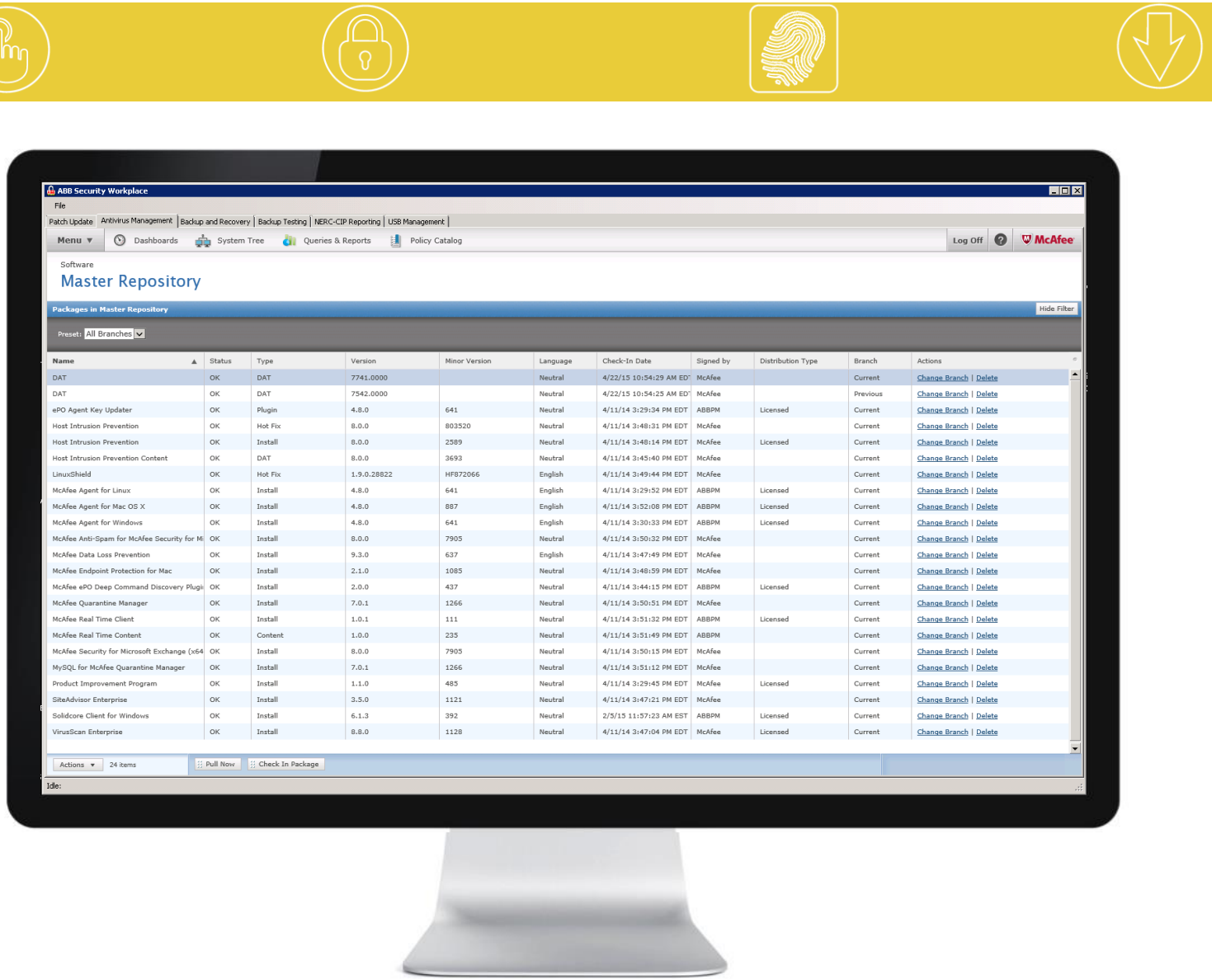


ABB Security Workplace
Maintain - Demonstration

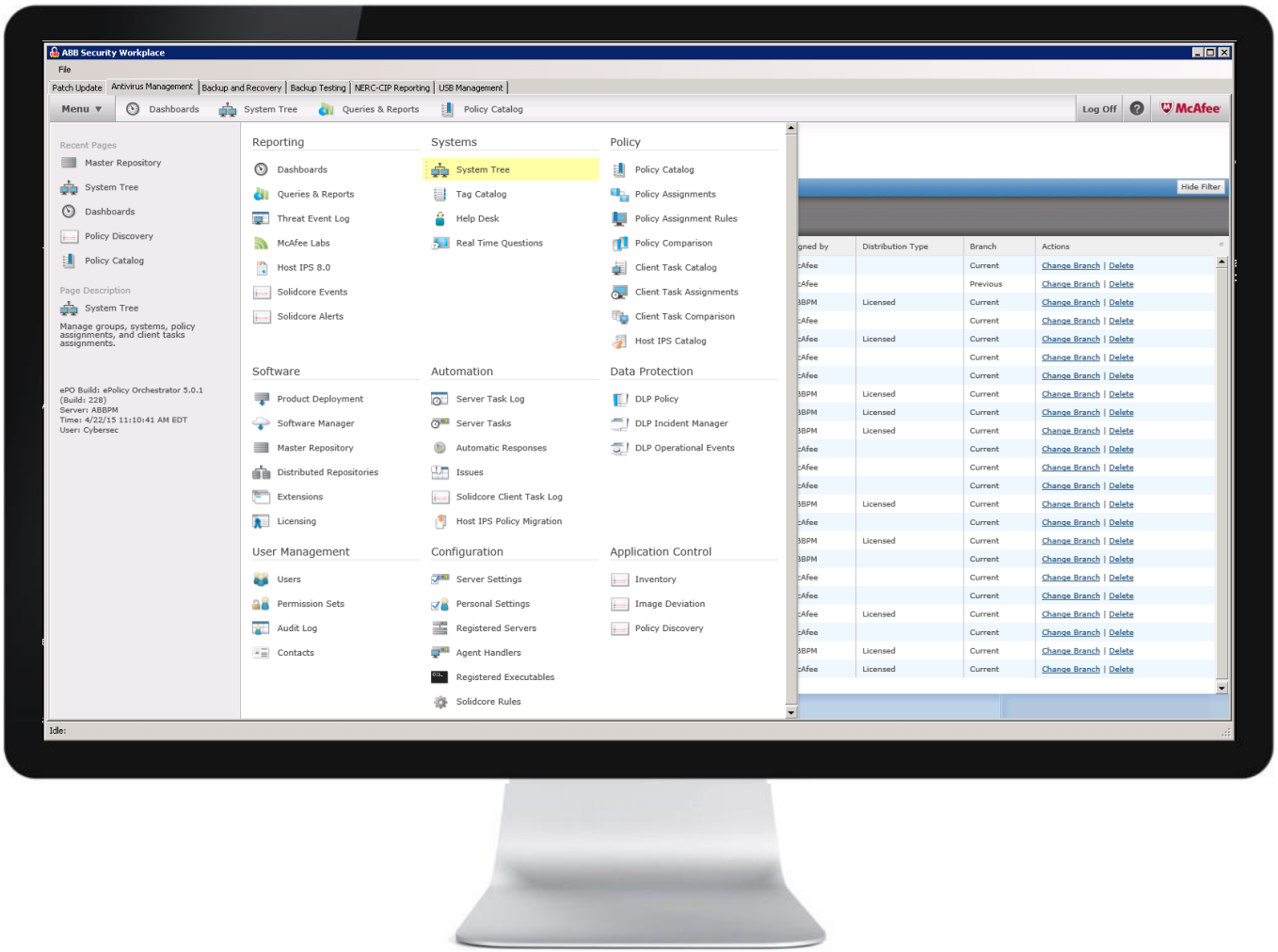


ABB Security Workplace
Maintain - Demonstration

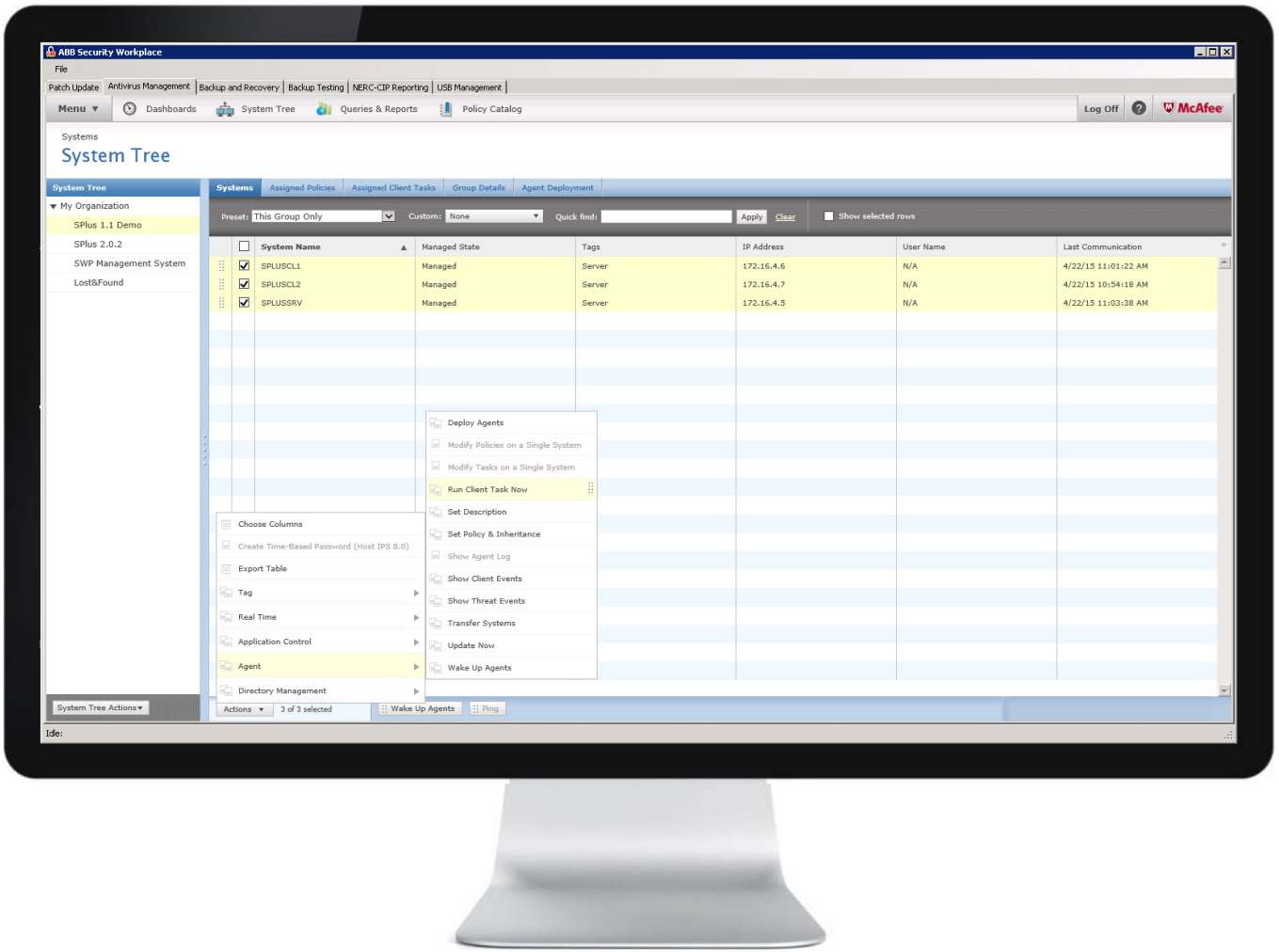


ABB Security Workplace
Maintain - Demonstration

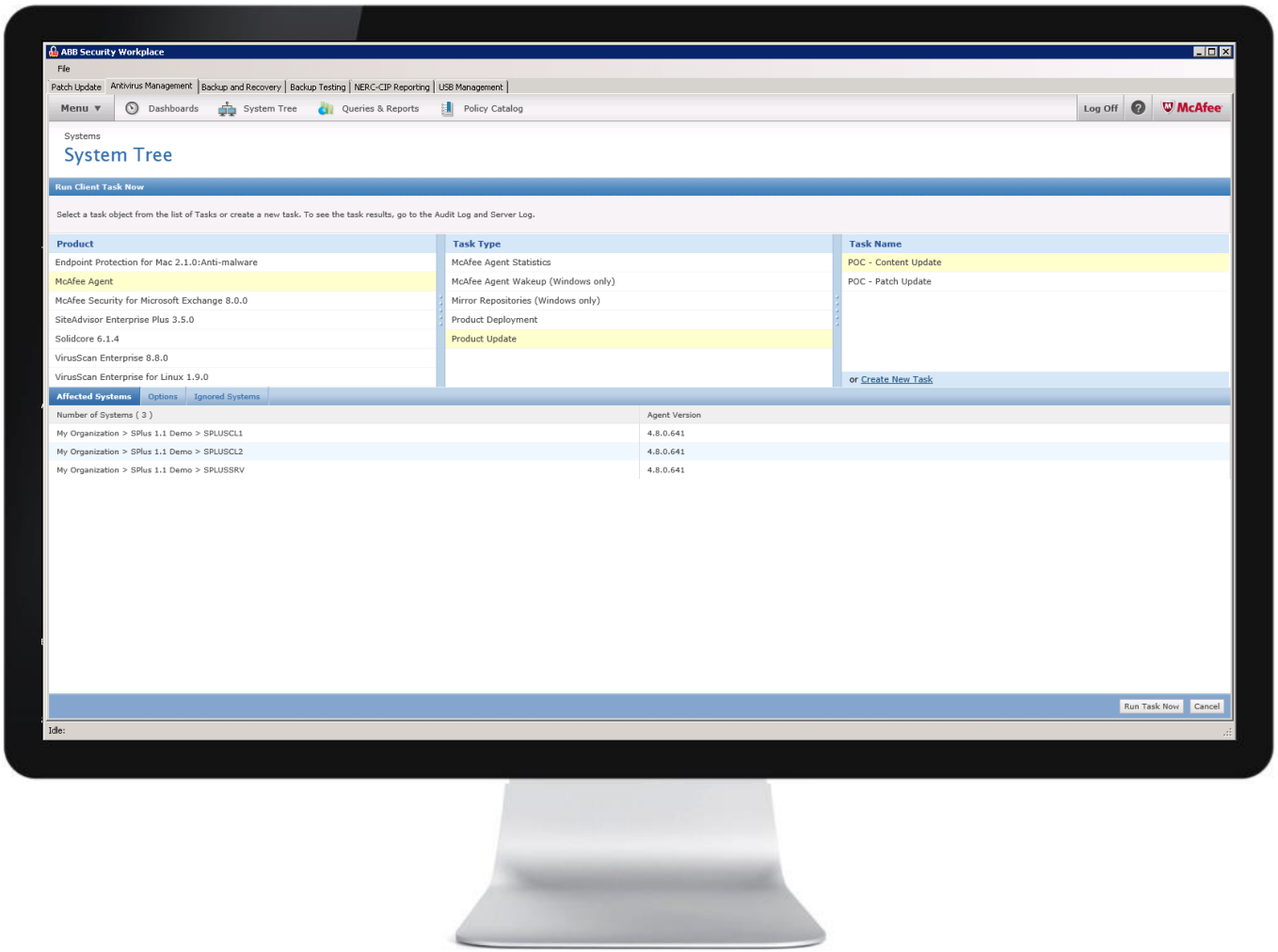


ABB Security Workplace
Maintain - Demonstration

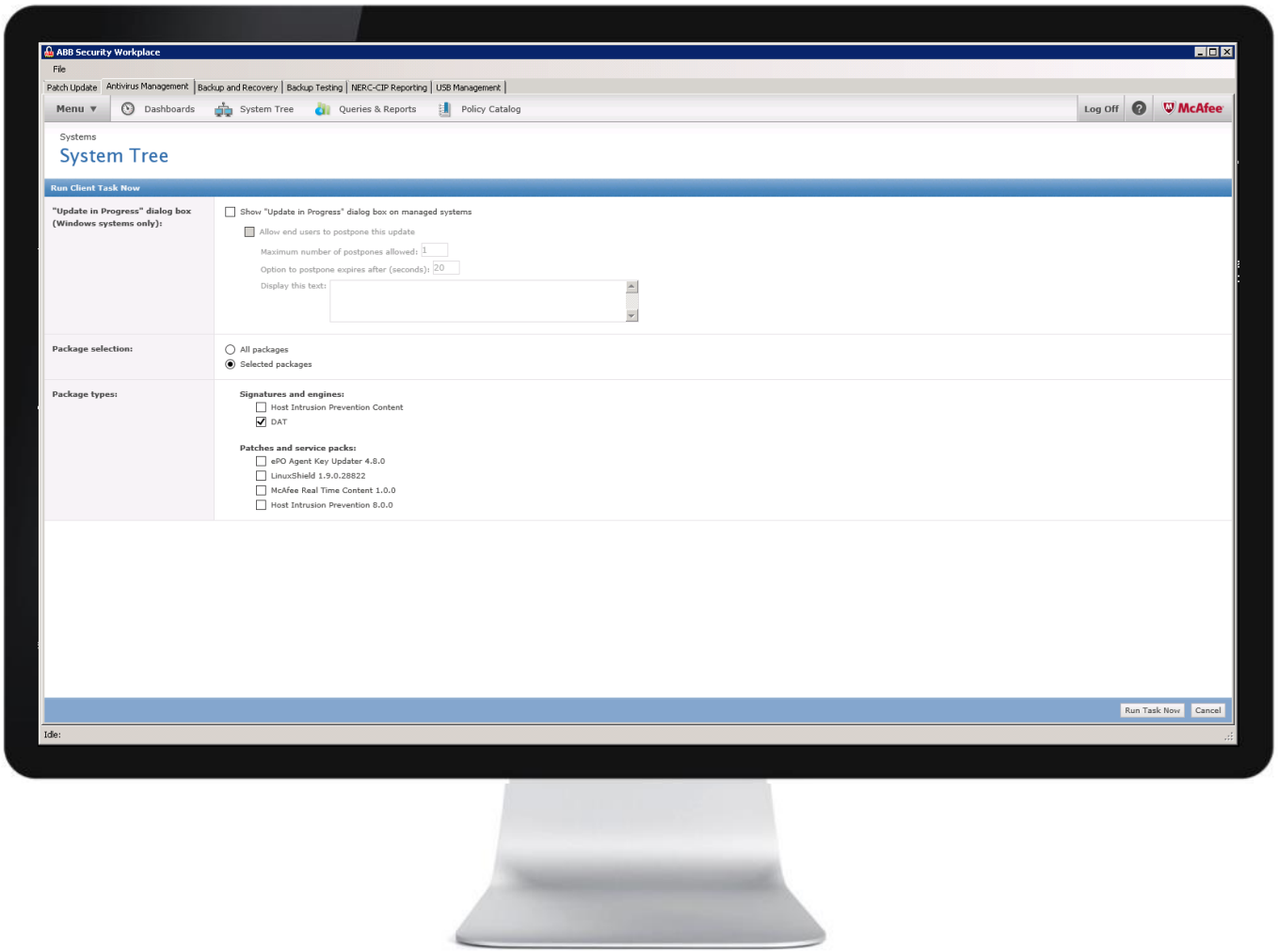


ABB Security Workplace
Maintain - Demonstration

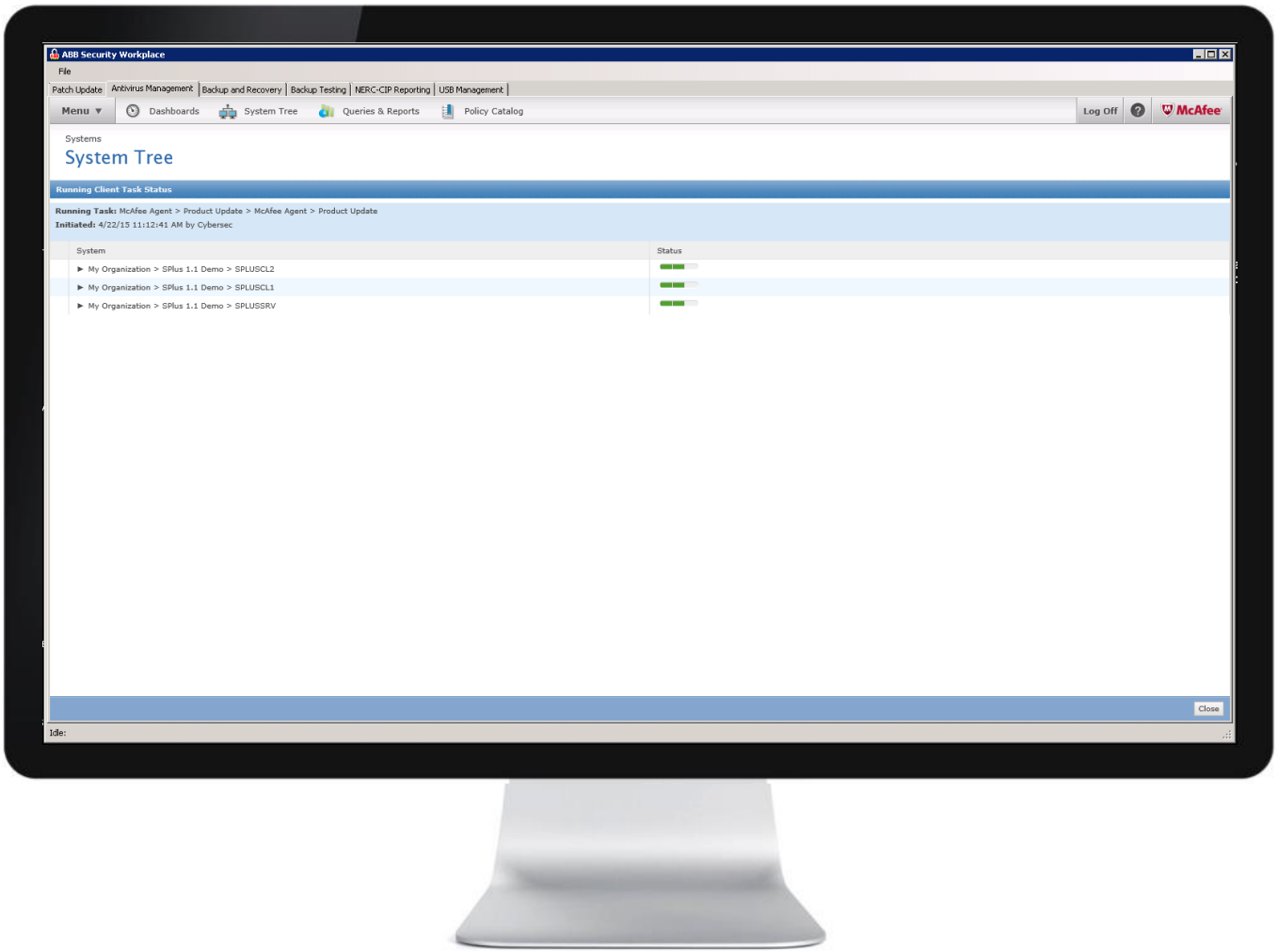


ABB Security Workplace
Maintain - Demonstration

Power and productivity
for a better world™