Tivoli Endpoint Manager

Core Protection Module

Mahmut Yerlice
Tivoli Endpoint Manager Technical Specialist

Agenda

- Tivoli Endpoint Manager
- Core Protection Module (CPM) 10.6
- Core Protection Module components and features
  - CPM for Windows
  - CPM for MAC
- Basic troubleshooting
- Questions

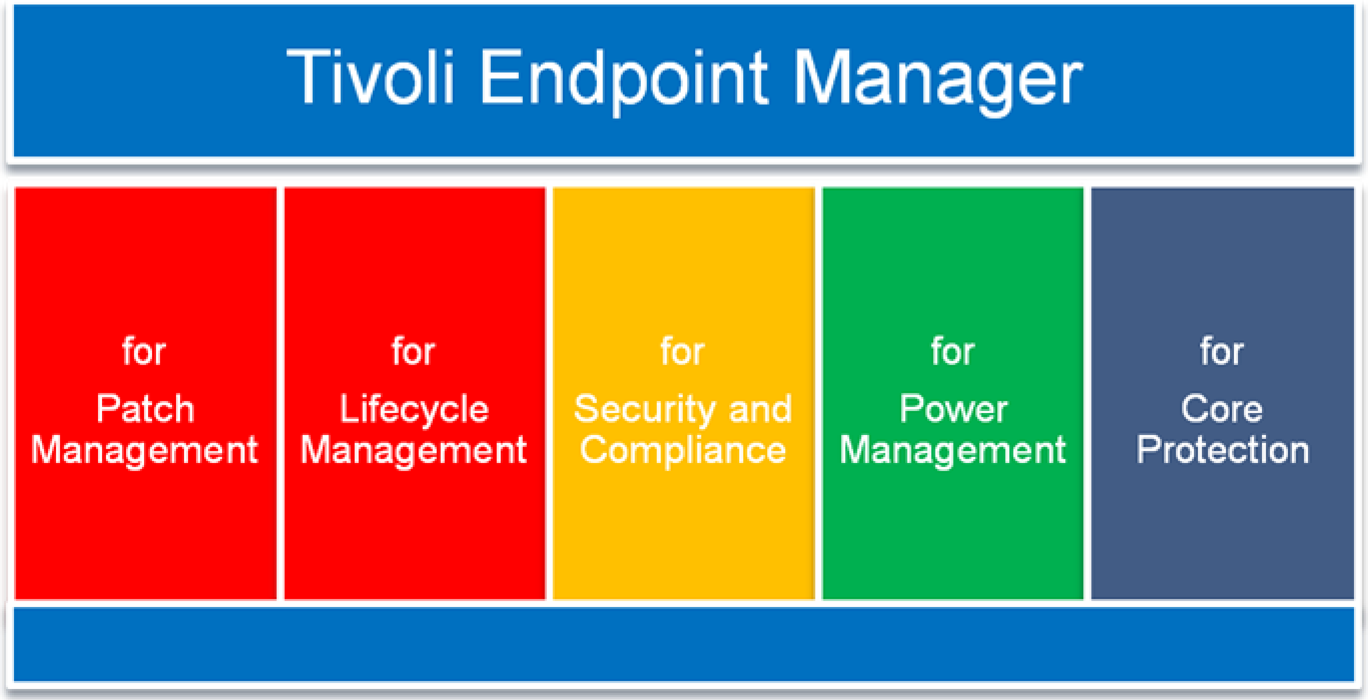
Introduction

Convention	Description
CPM	Core Protection Module
TEM	Tivoli Endpoint Manager
VSAPI	Virus Scanning API (Scan Engine)
TMUFE	Trend Micro URL Filtering Engine
CRC	Cyclic Redundancy Check
VDI	Virtual Desktop Infrastructure
Server	The computer where Security Server is installed.

Introduction

Convention	Description
Smart Server	The Smart Scan Server
Global Smart Scan Server	The Trend Micro Global Smart Scan Server, hosted and maintained by Trend Micro data centers.
Smart Client	A Security Agent that applies smart scanning.
Conventional Scan	The traditional scan implemented by Trend Micro products.
MPM	Mac Protection Module
WRS	Web Reputations Services
AEGiS	Original Name for BM and SP
AU (or iAU)	Intelligent ActiveUpdate

Introducing Tivoli Endpoint Manager
– Based on BigFix Technologies


Tivoli Endpoint Manager

for Patch Management

for Lifecycle Management

for Security and Compliance

for Power Management

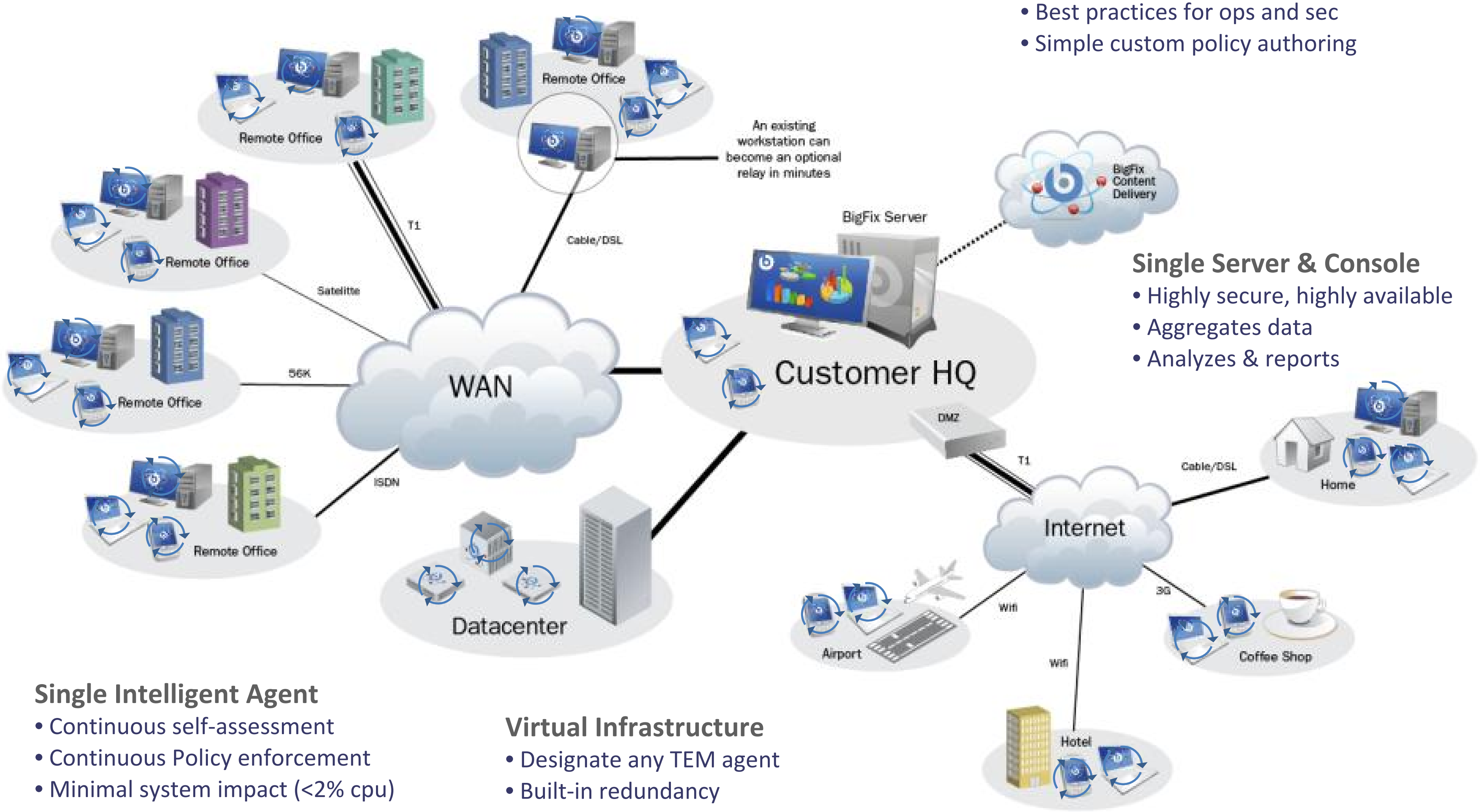
for Core Protection

Using Tivoli Endpoint Manager, Administrators can:

- See all endpoints: physical, virtual, fixed or mobile
- Fix issues anywhere in minutes, regardless of bandwidth or connectivity
- Deploy in days, over any network or geography

The Power of Distributed Intelligence

Fixlet Messages
- Out-of-the-box policies
- Best practices for ops and sec
- Simple custom policy authoring



Single Server & Console
- Highly secure, highly available
- Aggregates data
- Analyzes & reports

Single Intelligent Agent
- Continuous self-assessment
- Continuous Policy enforcement
- Minimal system impact (<2% cpu)

Virtual Infrastructure
- Designate any TEM agent
- Built-in redundancy
- Leverage existing systems

IBM Tivoli Endpoint Manager for Core Protection

Real-time protection from malware and other vulnerabilities

- Protect physical and virtual endpoints from damage caused by viruses, Trojan horses, worms, spyware, rootkits, web threats and their new variants
- Deliver real-time endpoint protection through file and web reputation, behavior monitoring, virtualization awareness and personal firewall
- Fix endpoint vulnerabilities before attacks exploit them and automatically clean endpoints of malware
- Ensure that antivirus services are always installed, running and up to date
- Provides virtualization awareness to reduce resource contention issues on virtual infrastructures
- Leverages industry-leading IBM® and Trend Micro™ technologies with a single-console management infrastructure

By the Numbers

- **$114 billion**
  - **Amount of money spent by enterprises in 2011 cleaning up after a malware attack**
- **$275,000**
  - **Average cost to an enterprise to clean up after a single malware attack excluding the cost of the damage to the reputation**
- **67,000**
  - **Number of new variants of malware PER DAY seen in 2010 – numbers increasing exponentially**
- **1**
  - **Number of attacks/outbreaks it takes for a company to wind up on CNN, MSNBC, etc. joining the illustrious ranks of TJ Maxx, TD Ameritrade, RSA**

Core Protection Module 10.6

Immediate Protection

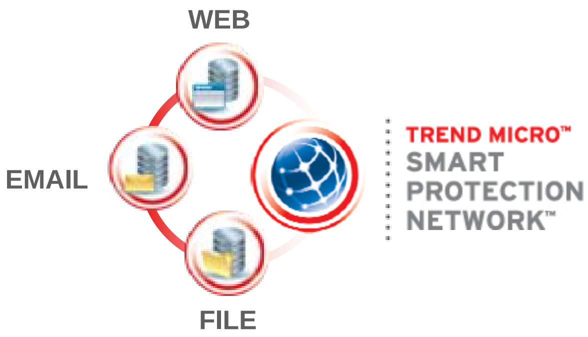
Web Reputation

Blocks Access to Dangerous Web Content

Protects both on and off the network

Supports any application

Limits exposure to today‘s threats



Prevents Users from Opening Infected Files

File Reputation

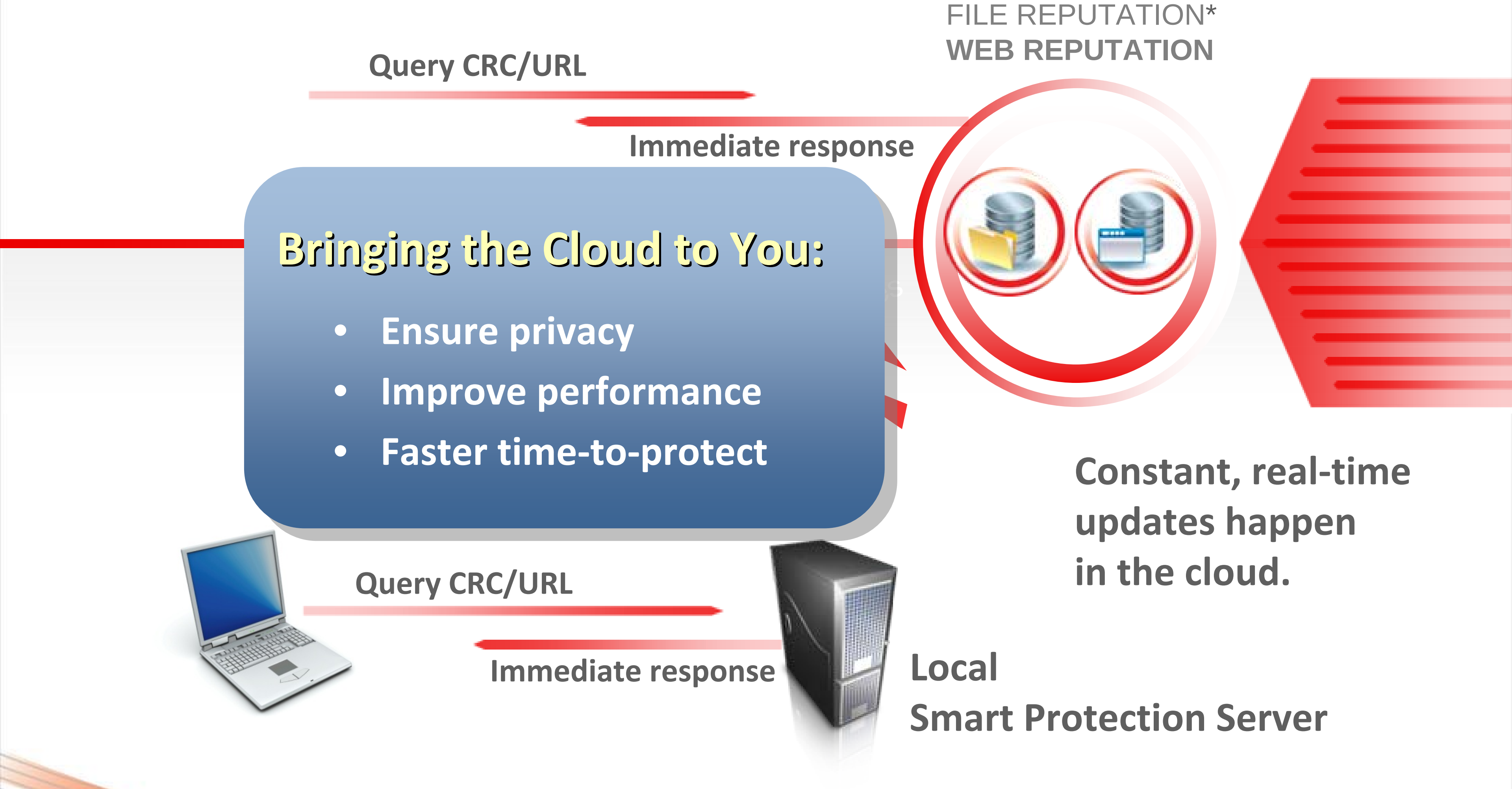
Eliminates signature management effort

Reduces resource impact on endpoints

Enables accurate risk management

Feeds threat information back to the Smart Protection Network

Local File Reputation AND Web Reputation



Query CRC/URL

Immediate response

FILE REPUTATION*
WEB REPUTATION

Bringing the Cloud to You:

- Ensure privacy
- Improve performance
- Faster time-to-protect

Constant, real-time updates happen in the cloud.

Query CRC/URL

Immediate response

Local
Smart Protection Server

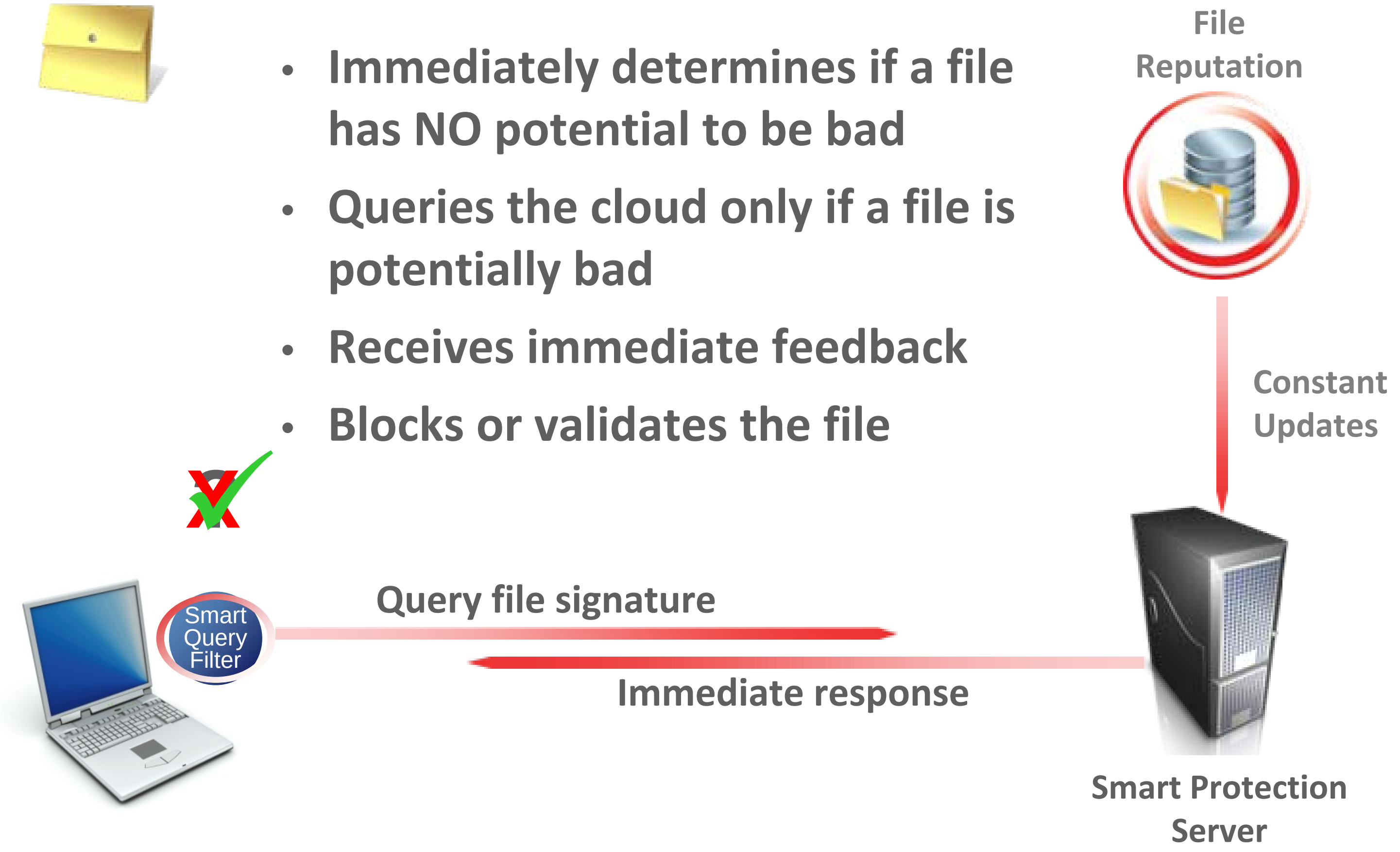
*Available in CPM 10.5, Q2 2011

Smart Query Filter

Core Protection Module 10.6

Ensures safety of most files without querying the cloud

- Immediately determines if a file has NO potential to be bad
- Queries the cloud only if a file is potentially bad
- Receives immediate feedback
- Blocks or validates the file



Understanding File Reputation

Multi-Layer Intrusion Prevention

Application Layer Defense

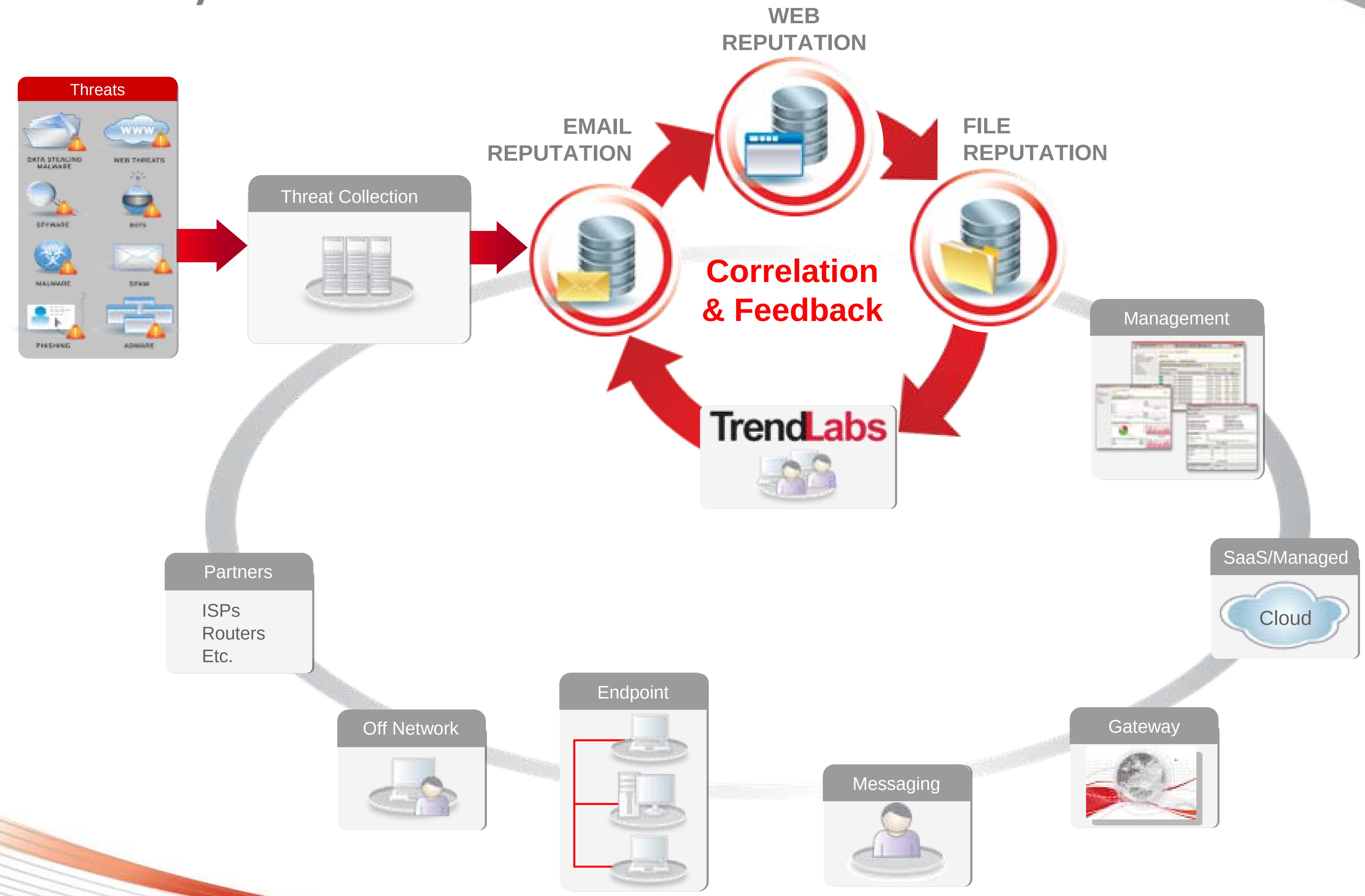
Behavior Monitoring*

- Safeguards the CPM client
- Safeguards other applications
- Monitors processes and applications for suspicious behavior
  - Changes to essential system files
    (including: registry entries, startup files, hosts-file)
  - Changes to Internet Explorer
  - DLL injection, etc.

*Available in CPM 10.5, Q2 2011

Trend Micro Smart Protection Network

Security Made Smarter



Convergence Saves Time and Costs

Endpoint Security Platform

Consolidating endpoint security operations in a single tool increases security while reducing cost and complexity.

Software Distribution

Anti-malware

Security Configuration Management

Patching

- Single agent
- Single server
- Single console

Minimum Complexity

Endpoint Security Platform

Security, visibility, and manageability in a single, highly scalable platform

Single, Intelligent Agent

- Processes continuously
- Consumes < 2% host CPU
- Distributes processing

Single Server, Single Console

- Publishes policies
- Aggregates data
- Analyzes & reports

Virtual Relays

Designate any computer to oversee scanning, patch downloads, and more, with little impact on host.

Fixlets

Simple scripting for policy creation.

Maximum Protection

Endpoint Security Platform

Patch Management Module

Patch management for multiple operating systems and applications

Patch Management Module

- Patches Microsoft, Unix, Linux, and Macintosh
- Centralizes and automates control
- Provides superior flexibility
- Supports low-bandwidth and global networks, with high first-pass success rates
- Boosts service-levels and regulatory compliance

First-pass patch installation success improvement from 65-75% to 95-99+%

Administrator workload lowered by 75% or more

Benefits Summary

Endpoint Security Platform

✓ Safer, Smarter Protection
✓ Ease of Management
✓ Peace of Mind

Safer, Smarter Protection

- Best-in-class* security with Web & File Reputation
- Reduced threat exposure
- Quick, nimble, and reliable updates
- Continuous enforcement and tracking

Ease of Management

- Up to 100,000 users on ONE management server
- More efficient IT/operations teams
- Efficient, cost-avoidant, and robust security posture
- Improved business agility

Peace of Mind

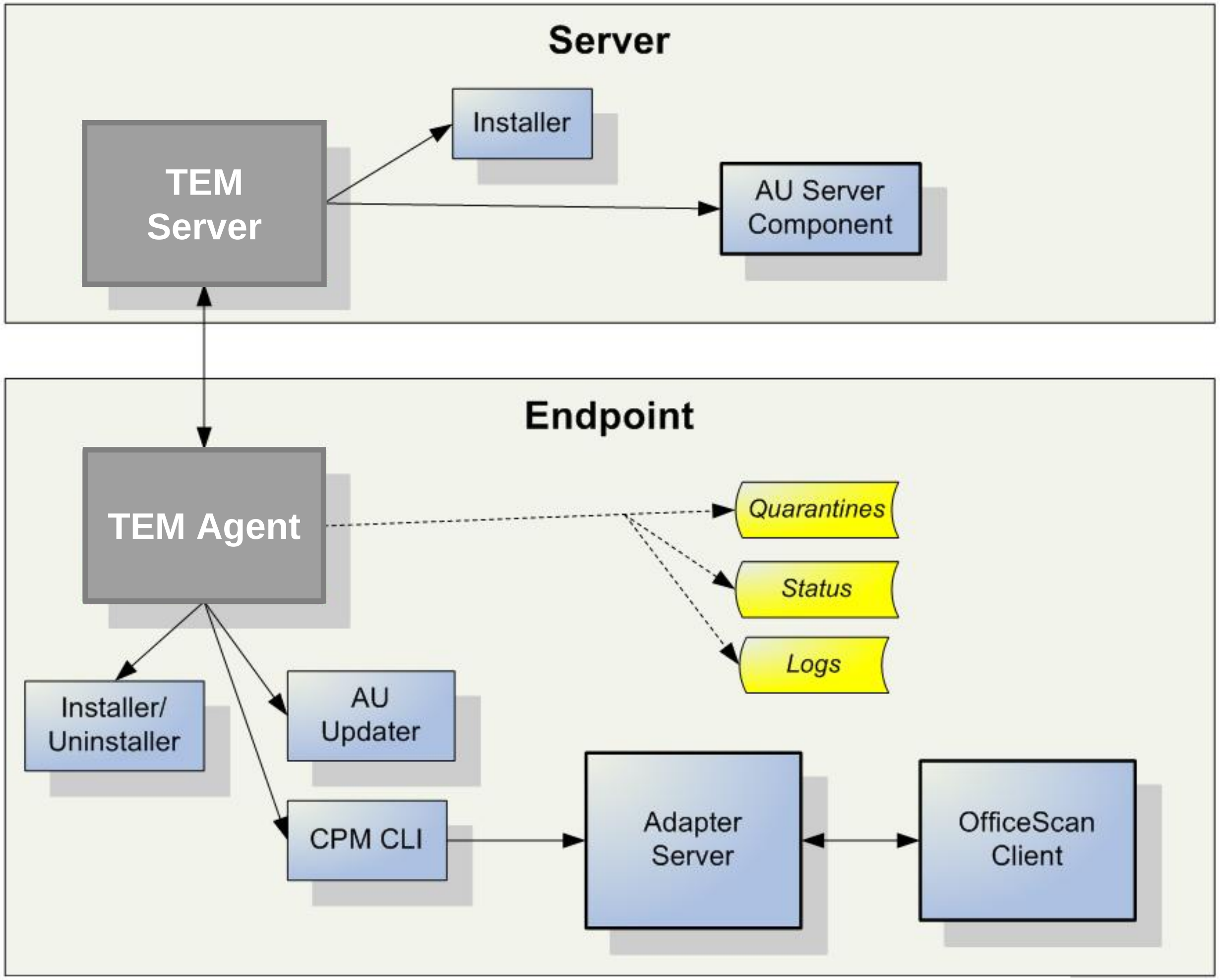
- Full, real-time visibility of endpoint status
- Easy and comprehensive compliance reporting

* NSS Labs, AVTest.org

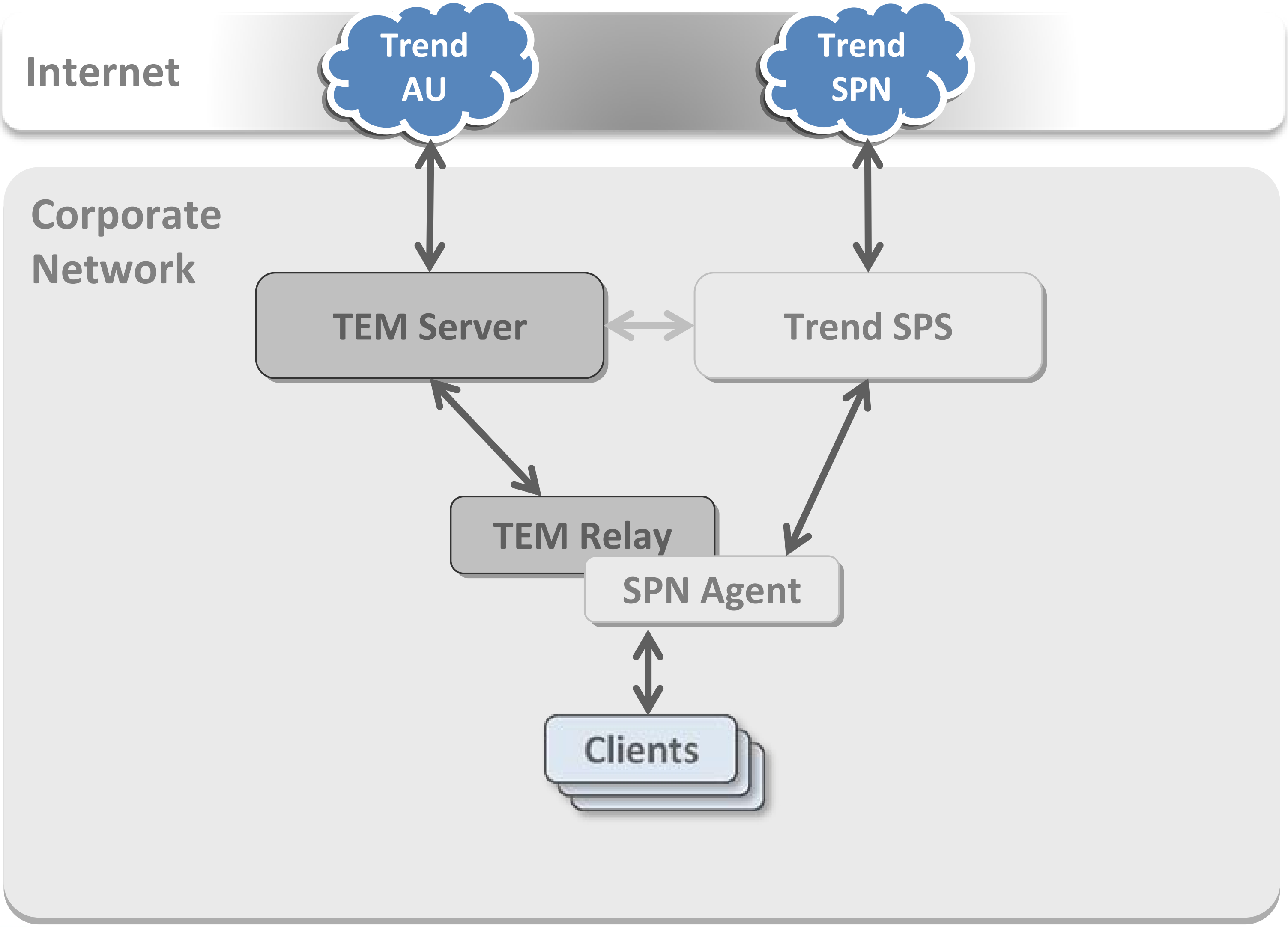
CPM Features

- Uses fixlet technology to identify outdated protection
- Provides these types of scanning
  - On-demand
  - Real-time
  - Scheduled
- Includes the CPM dashboard within the IBM console

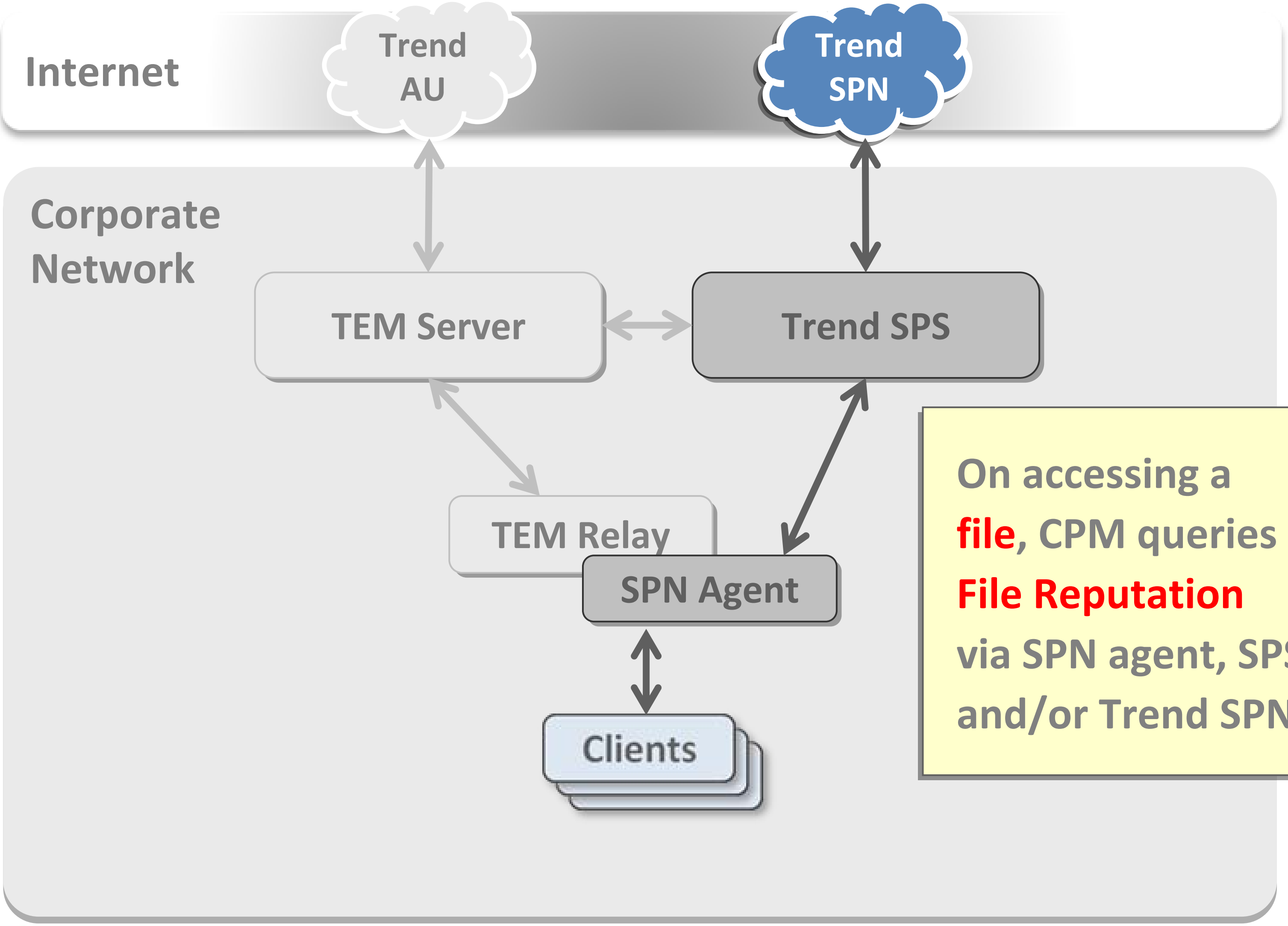
Architecture



CPM 10.5 Smart Protection Architecture

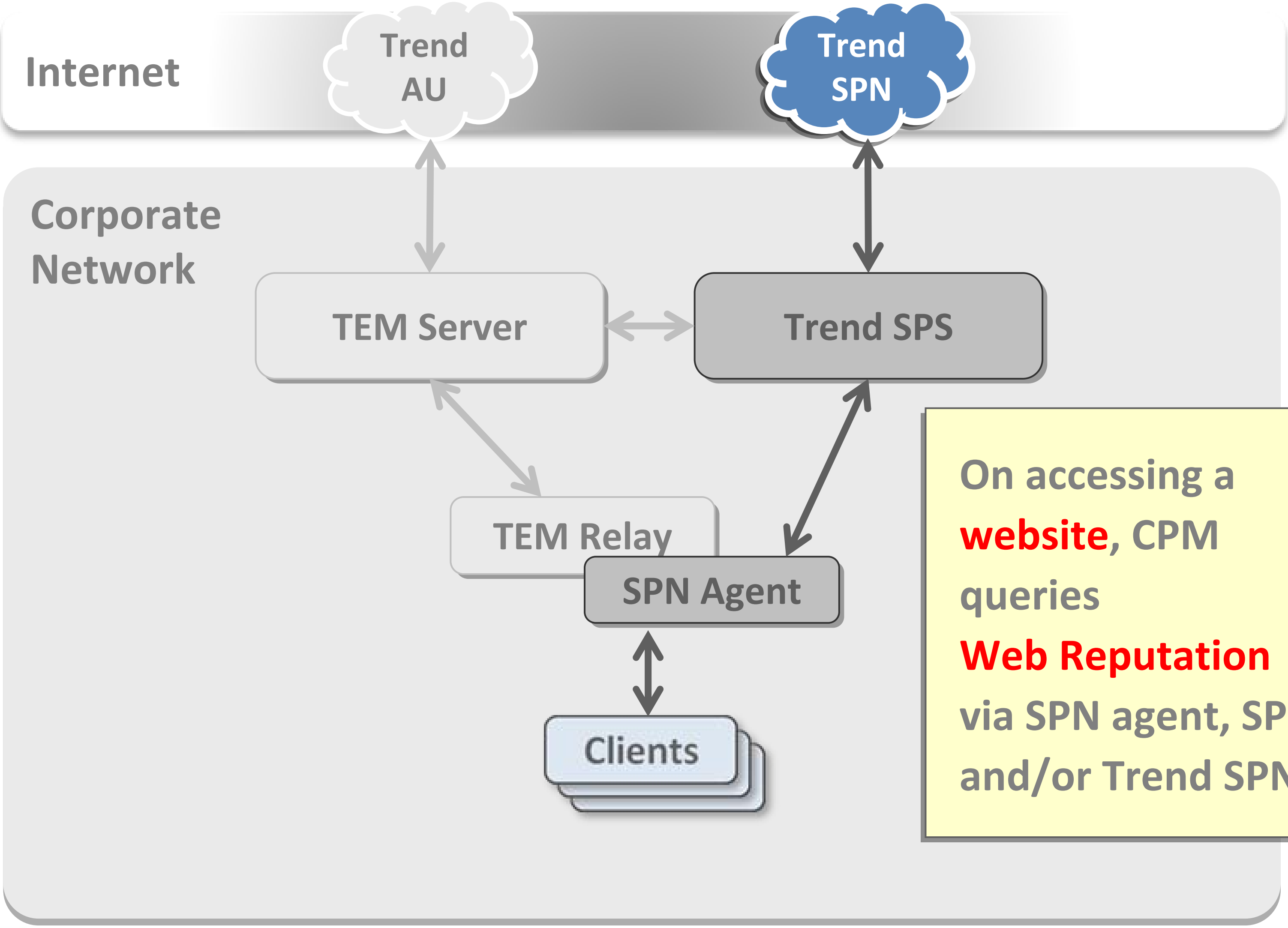


CPM 10.5 Smart Protection Architecture



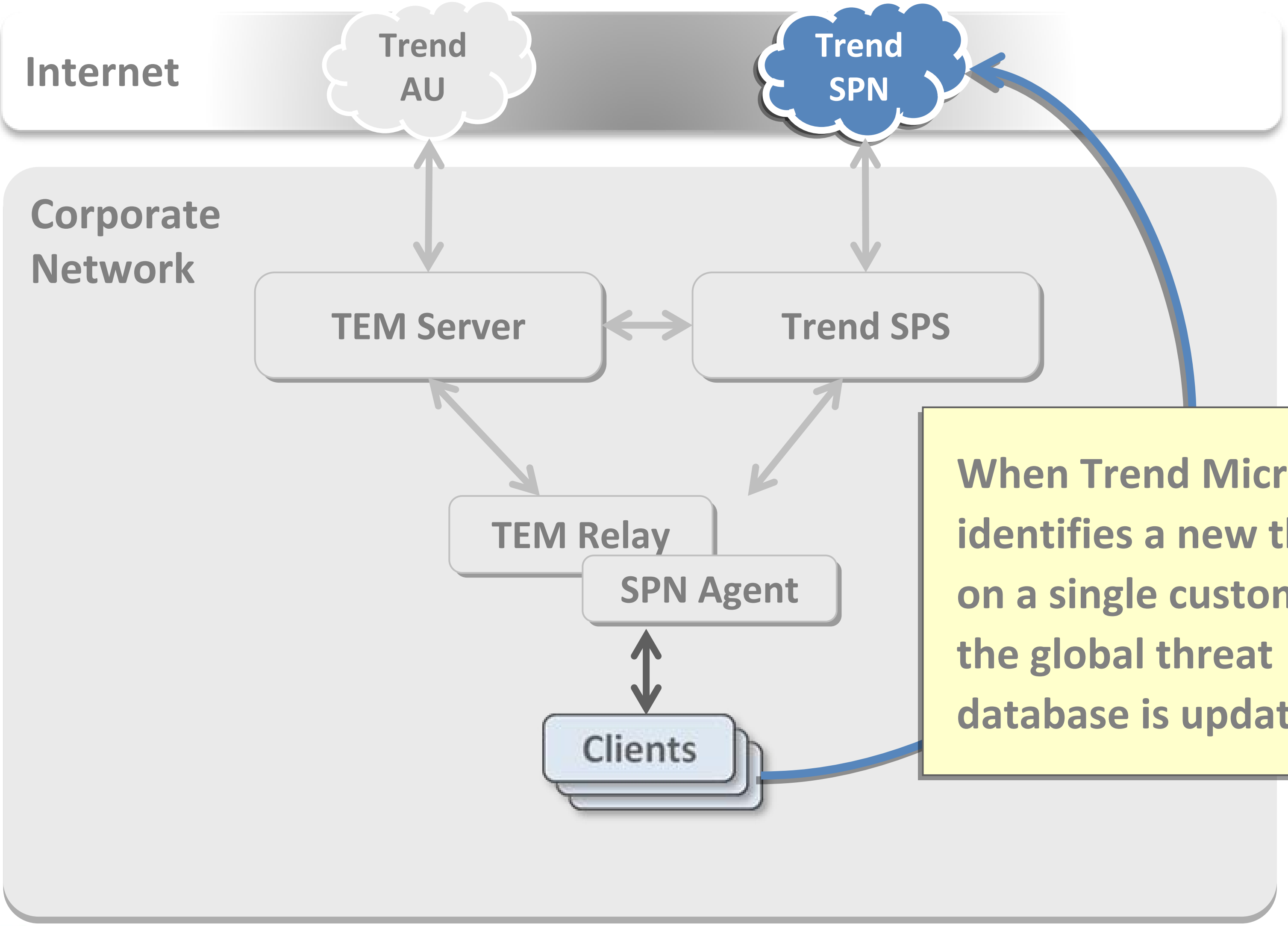
On accessing a **file**, CPM queries **File Reputation** via SPN agent, SPS and/or Trend SPN.

CPM 10.5 Smart Protection Architecture



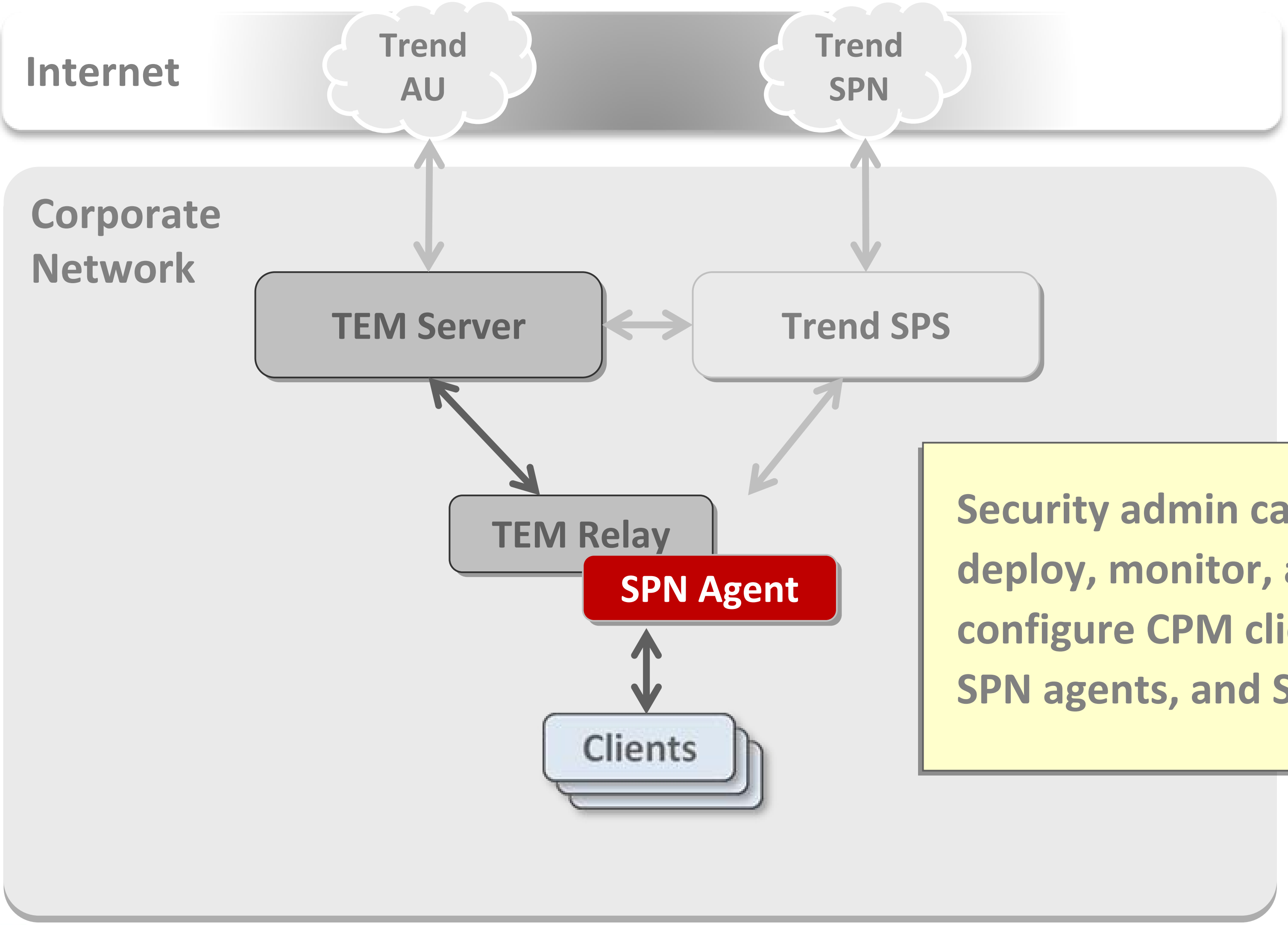
On accessing a **website**, CPM queries **Web Reputation** via SPN agent, SPS and/or Trend SPN.

CPM 10.5 Smart Protection Architecture



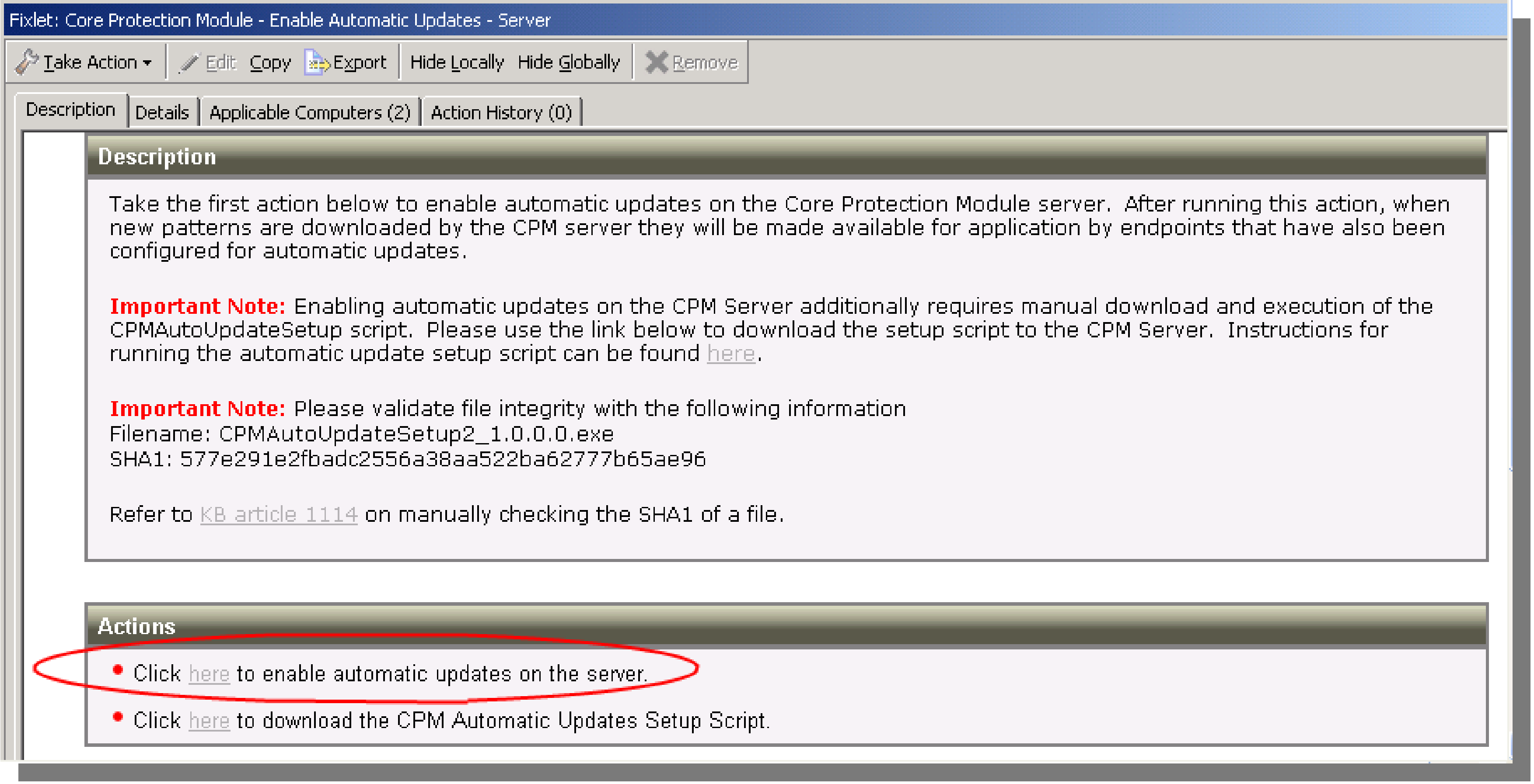
When Trend Micro identifies a new threat on a single customer, the global threat database is updated.

CPM 10.5 Smart Protection Architecture



Security admin can deploy, monitor, and configure CPM clients, SPN agents, and SPS*.

Configuring CPM Server Updates



Description

Take the first action below to enable automatic updates on the Core Protection Module server. After running this action, when new patterns are downloaded by the CPM server they will be made available for application by endpoints that have also been configured for automatic updates.

Important Note: Enabling automatic updates on the CPM Server additionally requires manual download and execution of the CPMAutoUpdateSetup script. Please use the link below to download the setup script to the CPM Server. Instructions for running the automatic update setup script can be found here.

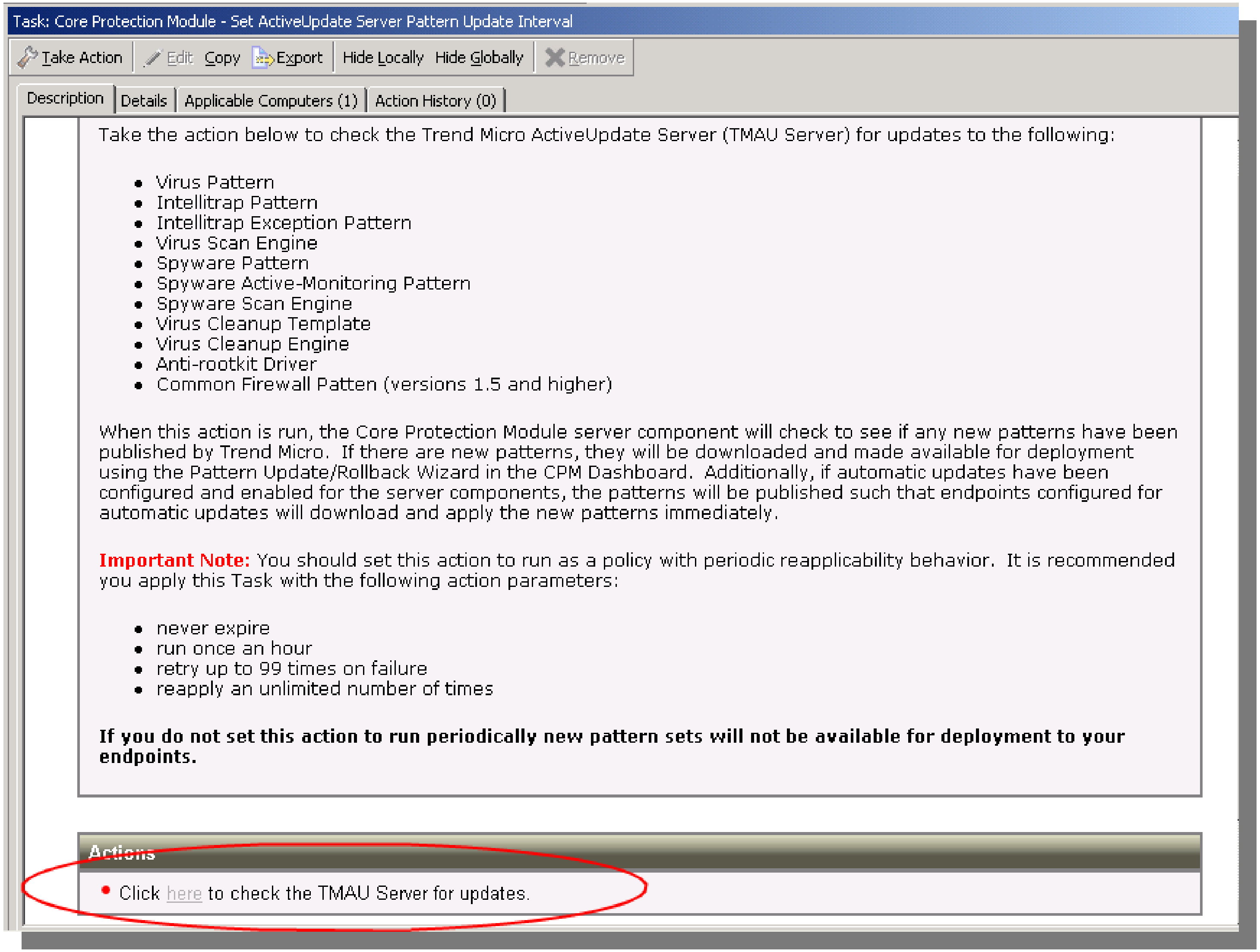
Important Note: Please validate file integrity with the following information
Filename: CPMAutoUpdateSetup2_1.0.0.0.exe
SHA1: 577e291e2fbadc2556a38aa522ba62777b65ae96

Refer to KB article 1114 on manually checking the SHA1 of a file.

Actions

- Click here to enable automatic updates on the server.
- Click here to download the CPM Automatic Updates Setup Script.

Configuring CPM Server Updates



Take the action below to check the Trend Micro ActiveUpdate Server (TMAU Server) for updates to the following:

- Virus Pattern
- Intellitrap Pattern
- Intellitrap Exception Pattern
- Virus Scan Engine
- Spyware Pattern
- Spyware Active-Monitoring Pattern
- Spyware Scan Engine
- Virus Cleanup Template
- Virus Cleanup Engine
- Anti-rootkit Driver
- Common Firewall Patten (versions 1.5 and higher)

When this action is run, the Core Protection Module server component will check to see if any new patterns have been published by Trend Micro. If there are new patterns, they will be downloaded and made available for deployment using the Pattern Update/Rollback Wizard in the CPM Dashboard. Additionally, if automatic updates have been configured and enabled for the server components, the patterns will be published such that endpoints configured for automatic updates will download and apply the new patterns immediately.

Important Note: You should set this action to run as a policy with periodic reapplicability behavior. It is recommended you apply this Task with the following action parameters:

- never expire
- run once an hour
- retry up to 99 times on failure
- reapply an unlimited number of times

If you do not set this action to run periodically new pattern sets will not be available for deployment to your endpoints.

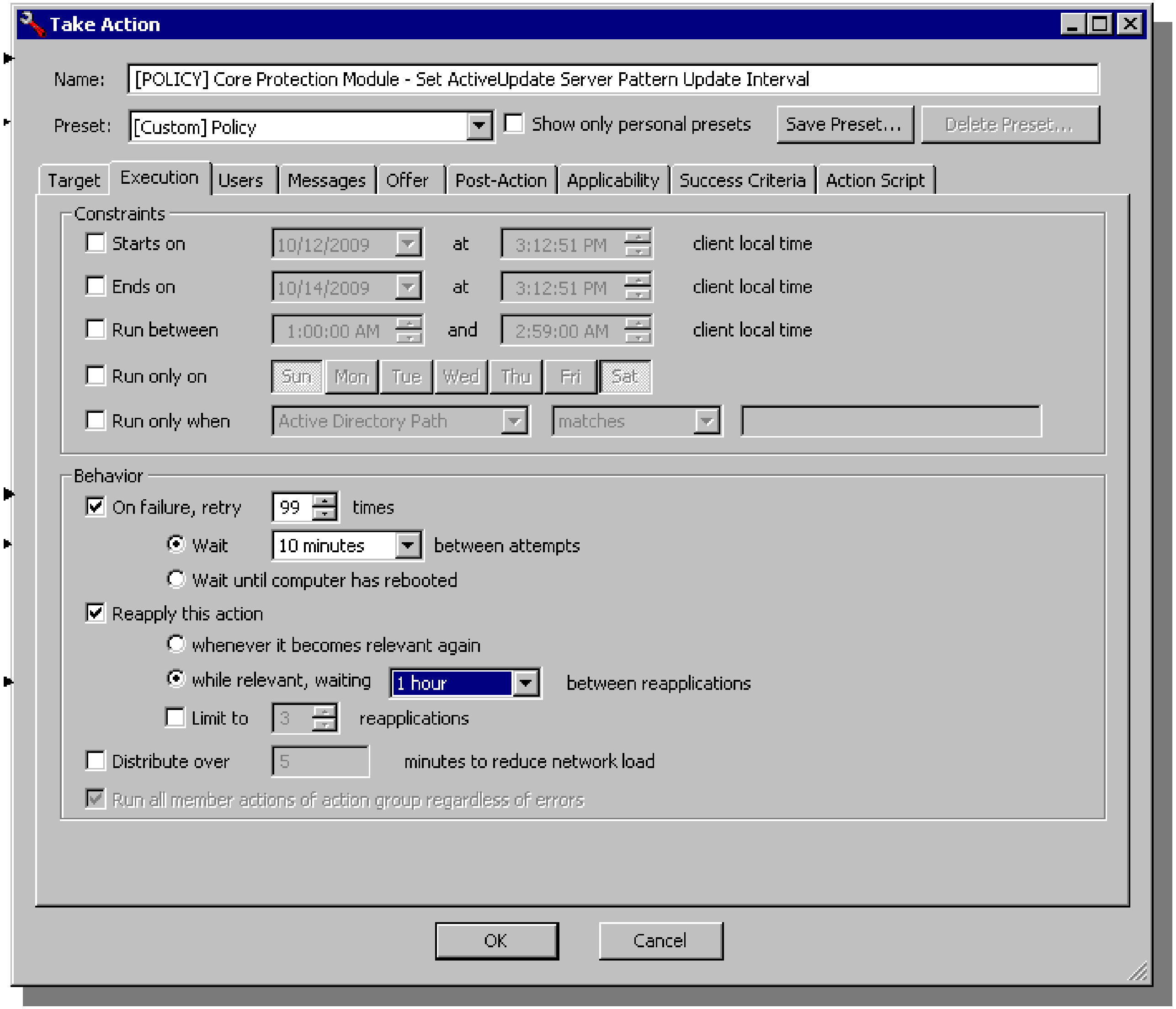
Actions

- Click here to check the TMAU Server for updates.

Configuring CPM Server Updates

- Set ActiveUpdate Server Pattern Update Interval task
  - Deploy the task to the CPM server.
  - Make sure these parameters are set:
    - The task never expires.
    - It is run once per hour.
    - It will retry up to 99 times in 10 minute intervals.
    - There is no limit on the number of times it is reapplied.
- Wait for the task to complete before continuing.

Configuring CPM Server Updates



Take Action

Name: [POLICY] Core Protection Module - Set ActiveUpdate Server Pattern Update Interval

Preset: [Custom] Policy □ Show only personal presets

Constraints

□ Starts on 10/12/2009 at 3:12:51 PM client local time

□ Ends on 10/14/2009 at 3:12:51 PM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat

□ Run only when Active Directory Path matches

Behavior

☑ On failure, retry 99 times

● Wait 10 minutes between attempts

○ Wait until computer has rebooted

☑ Reapply this action

○ whenever it becomes relevant again

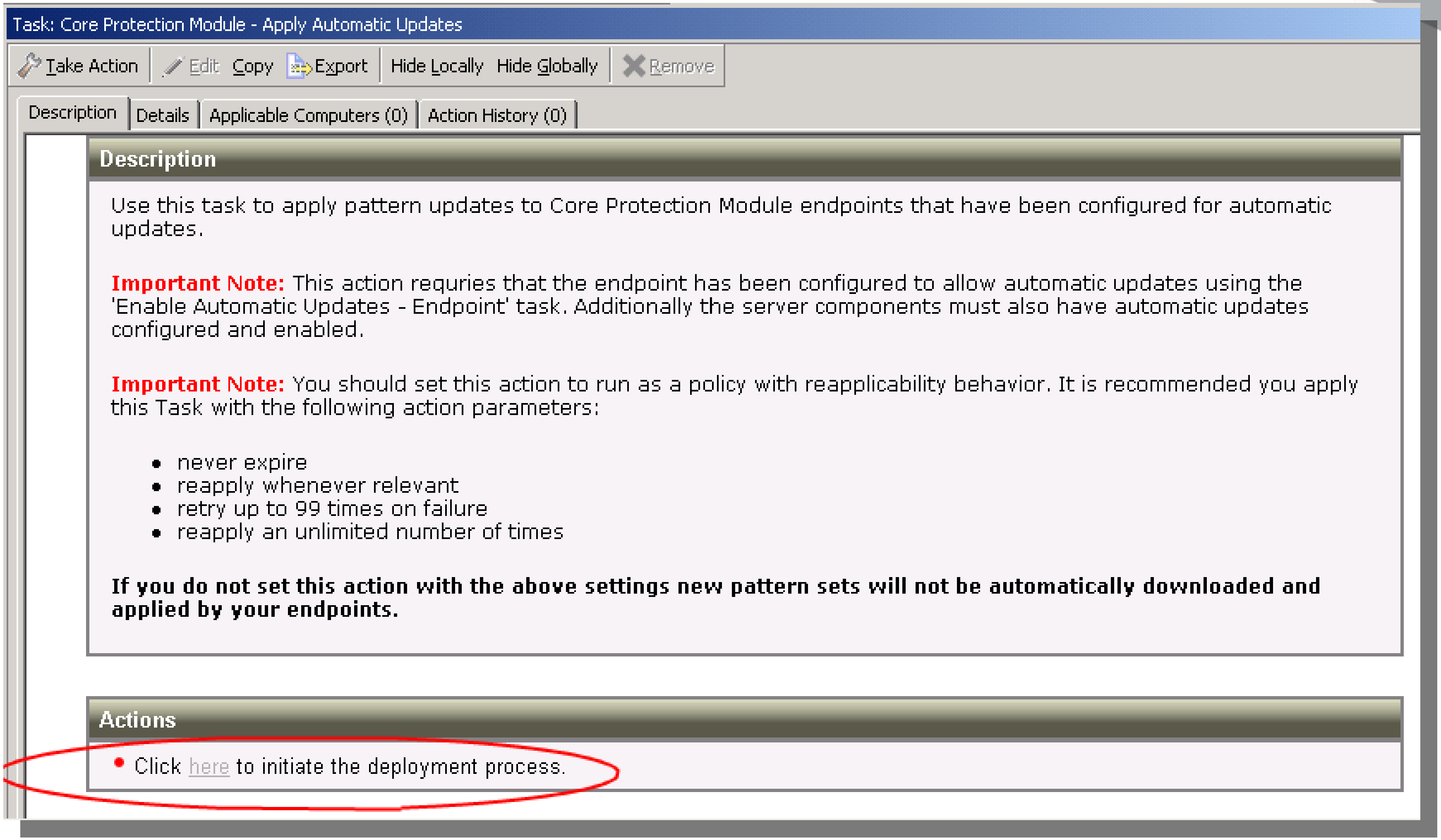
● while relevant, waiting 1 hour between reapplications

□ Limit to 3 reapplications

□ Distribute over 5 minutes to reduce network load

☑ Run all member actions of action group regardless of errors

Configuring CPM Server Updates



Description

Use this task to apply pattern updates to Core Protection Module endpoints that have been configured for automatic updates.

Important Note: This action requries that the endpoint has been configured to allow automatic updates using the 'Enable Automatic Updates - Endpoint' task. Additionally the server components must also have automatic updates configured and enabled.

Important Note: You should set this action to run as a policy with reapplicability behavior. It is recommended you apply this Task with the following action parameters:

- never expire
- reapply whenever relevant
- retry up to 99 times on failure
- reapply an unlimited number of times

If you do not set this action with the above settings new pattern sets will not be automatically downloaded and applied by your endpoints.

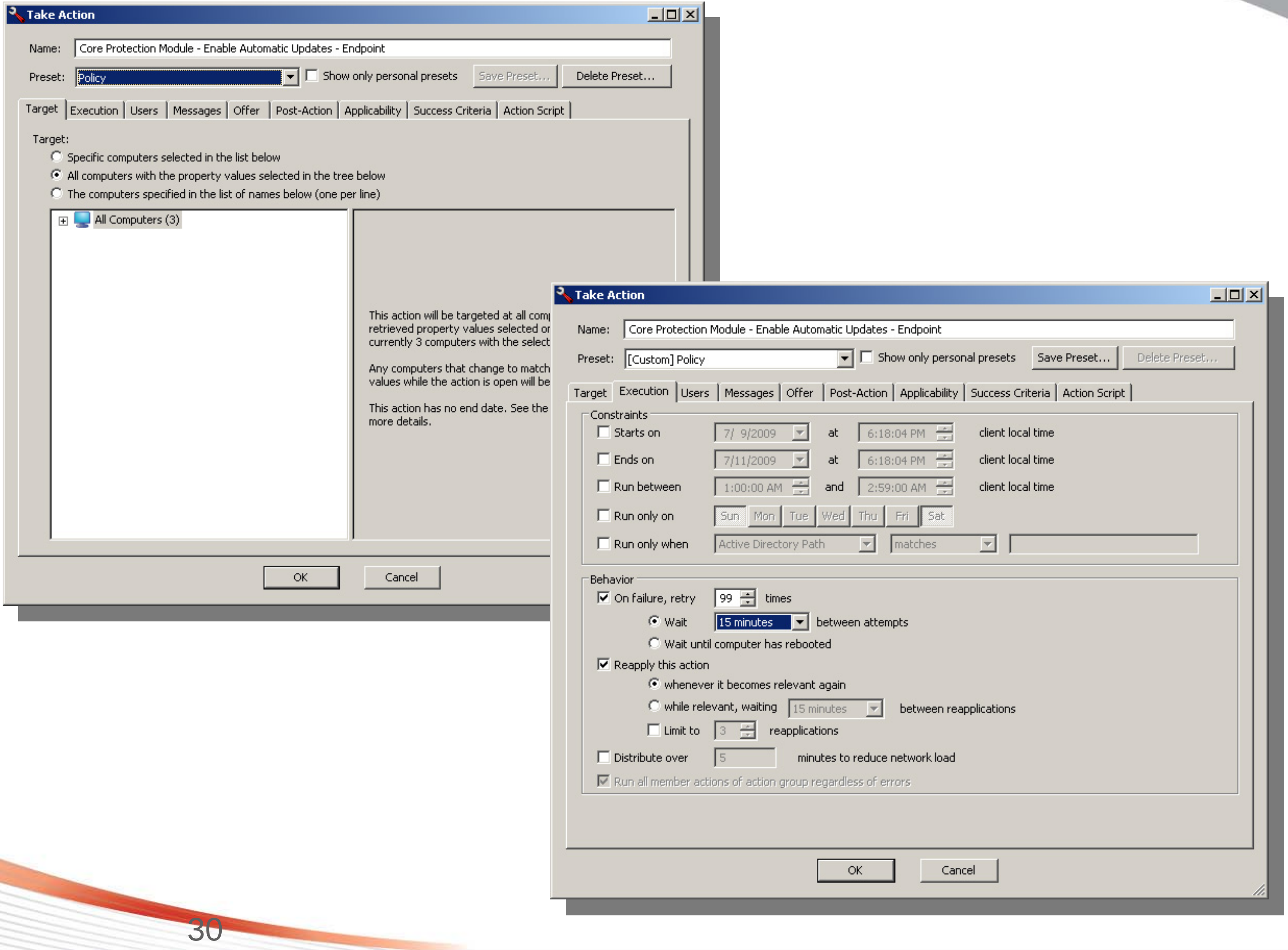
Actions

- Click here to initiate the deployment process.

Configuring CPM Client Updates

- Return to the CPM Dashboard from the Dashboards menu
- Navigate to `Updates > Automatic Update Tasks > Enable Automatic Updates – Endpoint`
  - Deploy the task to all computers
  - Make sure the following parameters are set:
    - The task never expires.
    - Reapply whenever relevant.
    - It will retry up to 99 times in 15 minutes intervals.
    - There should be no limit on the number of times it is reapplied.
- Wait for the task to complete before continuing.

Configuring CPM Client Updates



Take Action

Name: Core Protection Module - Enable Automatic Updates - Endpoint

Preset: Policy □ Show only personal presets

Target:

- ○ Specific computers selected in the list below
- ● All computers with the property values selected in the tree below
- ○ The computers specified in the list of names below (one per line)

All Computers (3)

This action will be targeted at all comp
retrieved property values selected or
currently 3 computers with the select

Any computers that change to match
values while the action is open will be

This action has no end date. See the
more details.

Take Action

Name: Core Protection Module - Enable Automatic Updates - Endpoint

Preset: [Custom] Policy □ Show only personal presets

Constraints

- □ Starts on 7/ 9/2009 at 6:18:04 PM client local time
- □ Ends on 7/11/2009 at 6:18:04 PM client local time
- □ Run between 1:00:00 AM and 2:59:00 AM client local time
- □ Run only on Sun Mon Tue Wed Thu Fri Sat
- □ Run only when Active Directory Path matches

Behavior

- ☑ On failure, retry 99 times
  - ● Wait 15 minutes between attempts
  - ○ Wait until computer has rebooted
- ☑ Reapply this action
  - ● whenever it becomes relevant again
  - ○ while relevant, waiting 15 minutes between reapplications
  - □ Limit to 3 reapplications
- □ Distribute over 5 minutes to reduce network load
- ☑ Run all member actions of action group regardless of errors

Troubleshooting

What do you do if you lost your private key (license.pvk) file?

If you lose your site credential files or password, then no one – not even IBM – can recover your keys or your password. You will need to reinstall the entire system, including all the CPM/BES clients, with a freshly generated key.

Troubleshooting

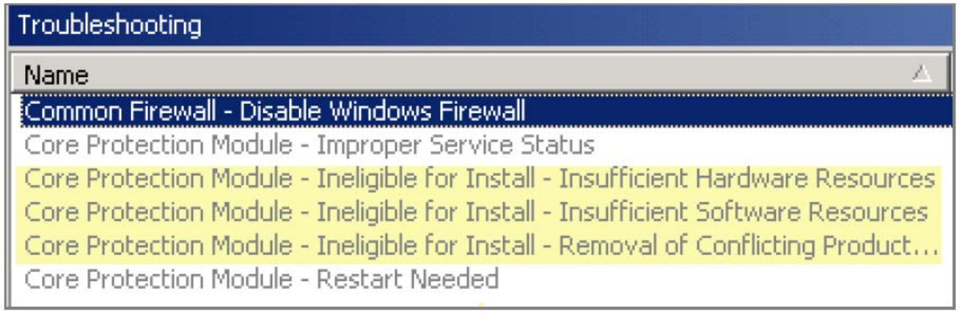
How do you trigger the installation of CPM agent on remote machines?

- **Use the BES Installer and select Install BES Components > Install BES Clients > Install Locally, which will install the client on your local machine in the directory you specify.**
- **Select to Install Remotely which will trigger the BES Client Deploy Tool.**
- **Manually copy `C:\BESInstallers\Client` folder from the BES installation computer to the local hard drive and run `setup.exe`**
- **Use `c:\BESInstallers\ClientMSI\BESClientMSI.msi` to run login script or GPO or other software distribution tool.**

Troubleshooting

Five options in the Troubleshooting node of the navigation tree enable you to resolve issues identified in the Health Status Chart under Deployment/Overview.

- Three audit Fixlets detect machines ineligible for a CPM installation:



Troubleshooting

Name
Common Firewall - Disable Windows Firewall
Core Protection Module - Improper Service Status
Core Protection Module - Ineligible for Install - Insufficient Hardware Resources
Core Protection Module - Ineligible for Install - Insufficient Software Resources
Core Protection Module - Ineligible for Install - Removal of Conflicting Product...
Core Protection Module - Restart Needed

- The remaining two Fixlets identify machines where services are not running or configured correctly, or in need of a reboot.
- A task to disable the Windows Firewall, which may conflict with the Common Firewall component is also included.

Troubleshooting

How do I get notified when my system detects a new spyware or virus infection?

Using Web Reports, configure a Scheduled Report based on the Top 25 spyware and virus reports, and set it to email you anytime it changes

Troubleshooting

How can end users monitor infection information?

By enabling the Client Dashboard.

Troubleshooting

What is the *ActiveUpdate Server and what is it used for?*

The Trend Micro ActiveUpdate (TMAU) server, is Trend’s “in-the-cloud” server from which our CPM server downloads pattern-set files.

Troubleshooting

What information is needed if the installation fails?

If installation fails or other issues are found on the CPM client, please download IBM Client Diagnostics from http://support.bigfix.com/bes/install/downloadutility.html and run it on the client. Send the zip file collected.

THANK YOU!

mahmuty@tr.ibm.com