



Daredevil

- Davor Perat
- Senior Technology Consultant

Agenda

1

Threat landscape and the endpoint

2

Protecting the endpoint

3

Performance or protection, why choose?

4

Virtualized and embedded system optimization

5

Streamlined management and reporting across platforms

6

Symantec product integration and support

7

Architecture overview

8

Additional resources and summary

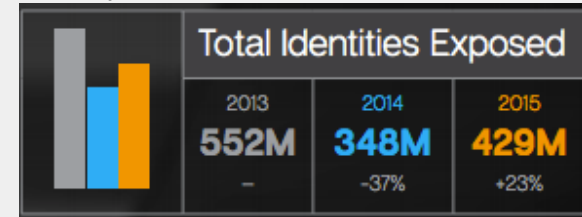
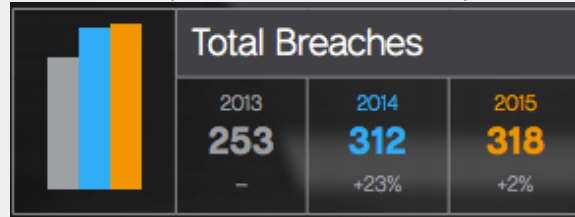
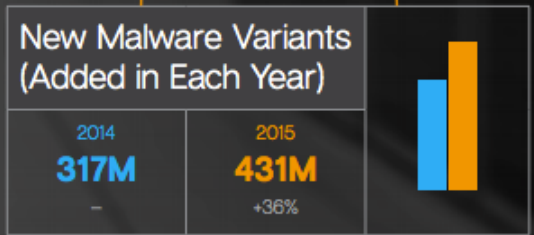
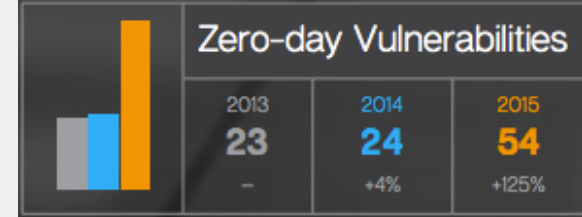


Let's get started!

Threat landscape and the endpoint

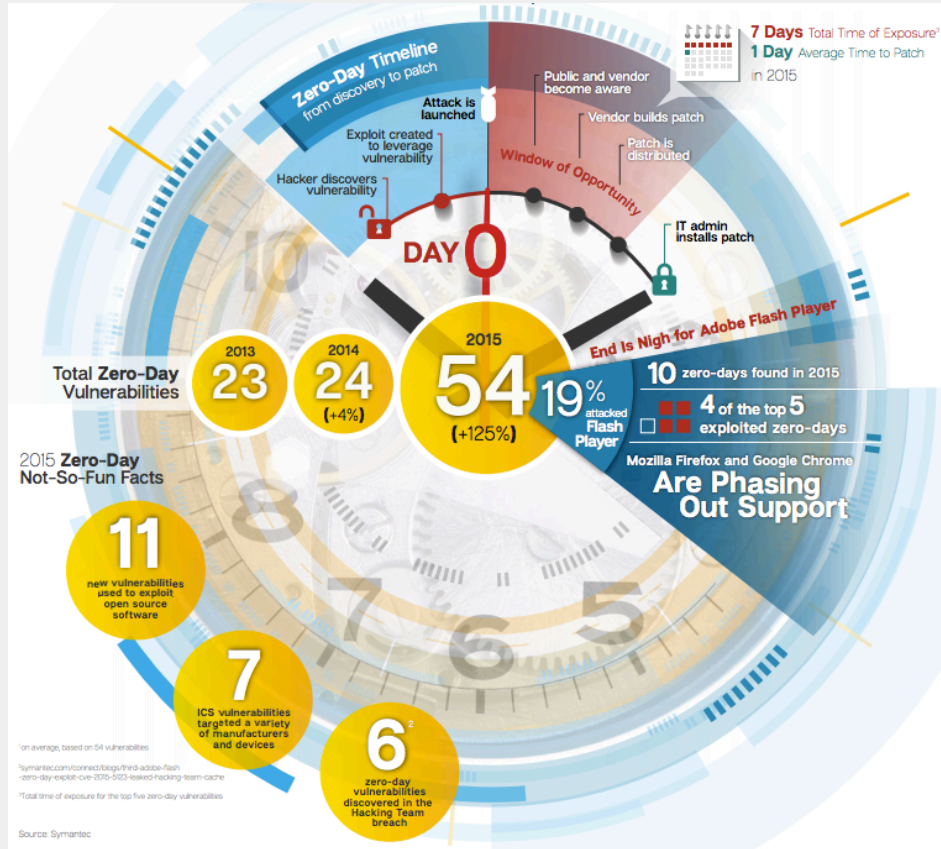
Internet Security Threat Report: ISTR Volume 21

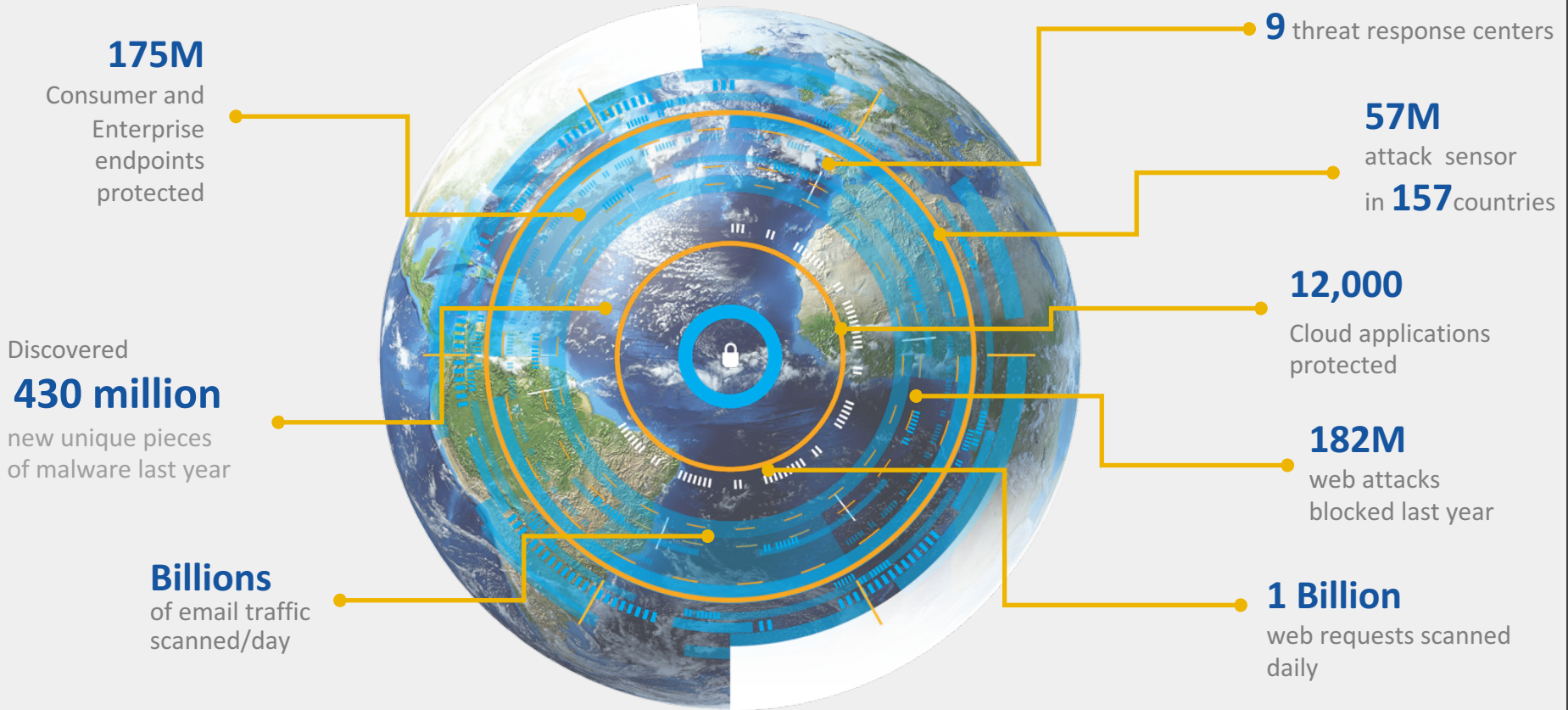
Known Malware New Malware Network Attack Social Engineering System Tampering Data Theft Vulnerabilities



Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36% from the year before.

A new Zero-Day vulnerability discovered every week in 2015





One of the largest civilian cyber intelligence networks
3.7 Trillion rows of security-relevant data

The threat landscape continues to escalate



430M

new pieces of malware were created in 2015



125%

increase of **Zero-Day** vulnerability from 2014 to 2015



35%

increase of **ransomware** in 2015



55%

Increase in **Targeted Attacks**

Inbound Communication

Payload delivery

Payload execution

Outbound Communication

Source: Symantec ISTR 2016

How Symantec can help

Symantec Endpoint Protection 14



UNRIVALED SECURITY

Stops targeted attacks and advanced persistent threats with intelligent security and layered protection that goes beyond antivirus.



BLAZING PERFORMANCE

Performance so fast your users won't even know its there.



SMARTER MANAGEMENT

A single management console across Windows, Mac, Linux, and Virtual platforms with granular policy control.

Inbound
Communication

Payload delivery

Payload execution

Outbound
Communication

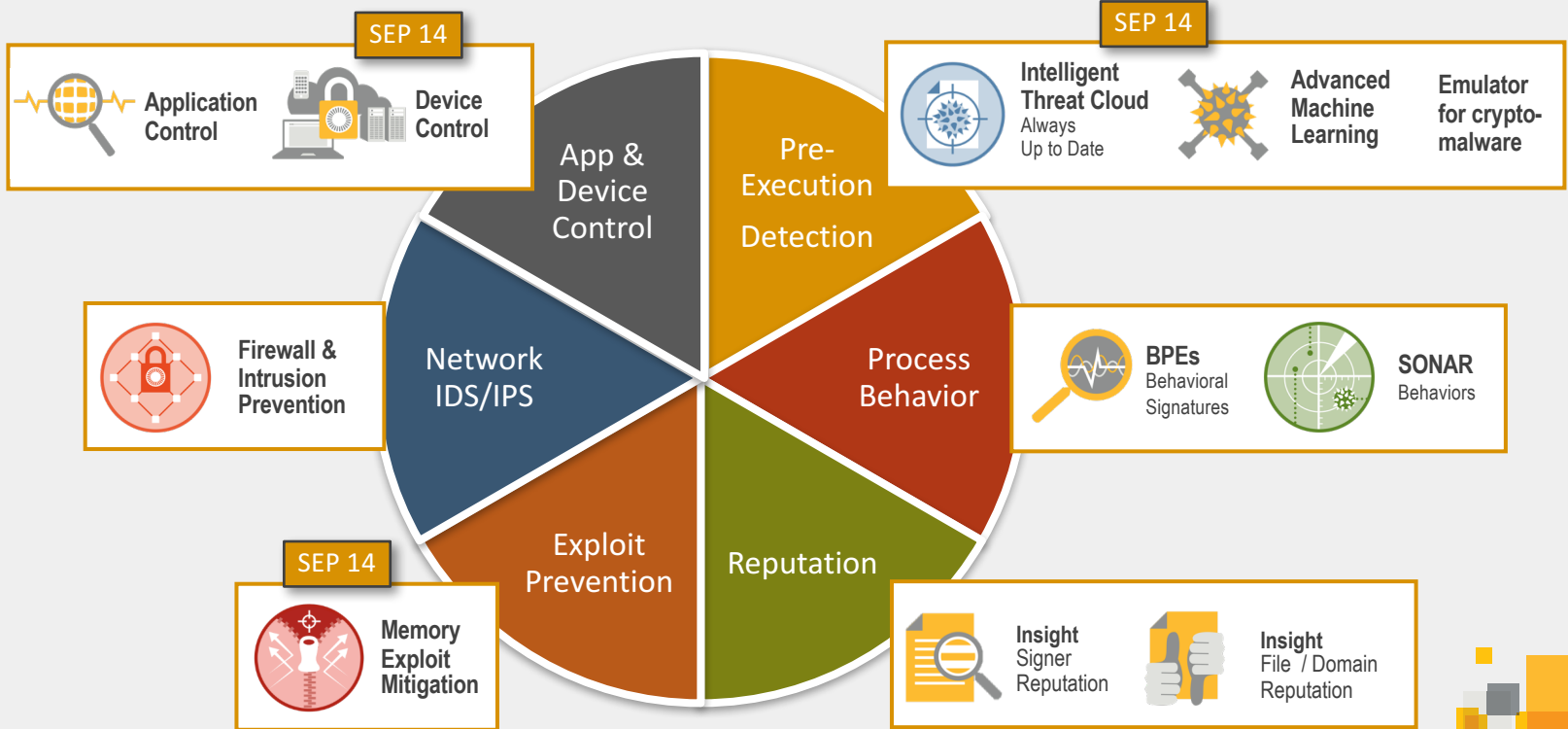
SUPERIOR PROTECTION

BETTER PERFORMANCE

EASY INTEGRATION &
AUTOMATION

SEP protects against all types of threats

SEP 14 combines Core and Next Generation technologies



SEP 14 Next Generation Protection Technologies and Enhancements



Machine Learning

- Pre-execution detection for new and evolving threats

Compete Against Cylance



Application Protection

- Memory Exploit Mitigation

Compete Against Traps



Emulator

- Anti-evasion technique to detect hidden malware

Strong Anti-Evasion



Intelligent Threat Cloud

- Real-time cloud lookup , ~70% reduction in definition size

70% drop in daily updates



Performance Enhancements

- Faster real-time virus detection

Faster and Light Weight



Enabling Integrations

- REST APIs
- Enable BlueCoat integrations

Easy Integrations



Enhanced Automation

- Expanded LiveUpdate to deliver security updates for Windows clients

Automation

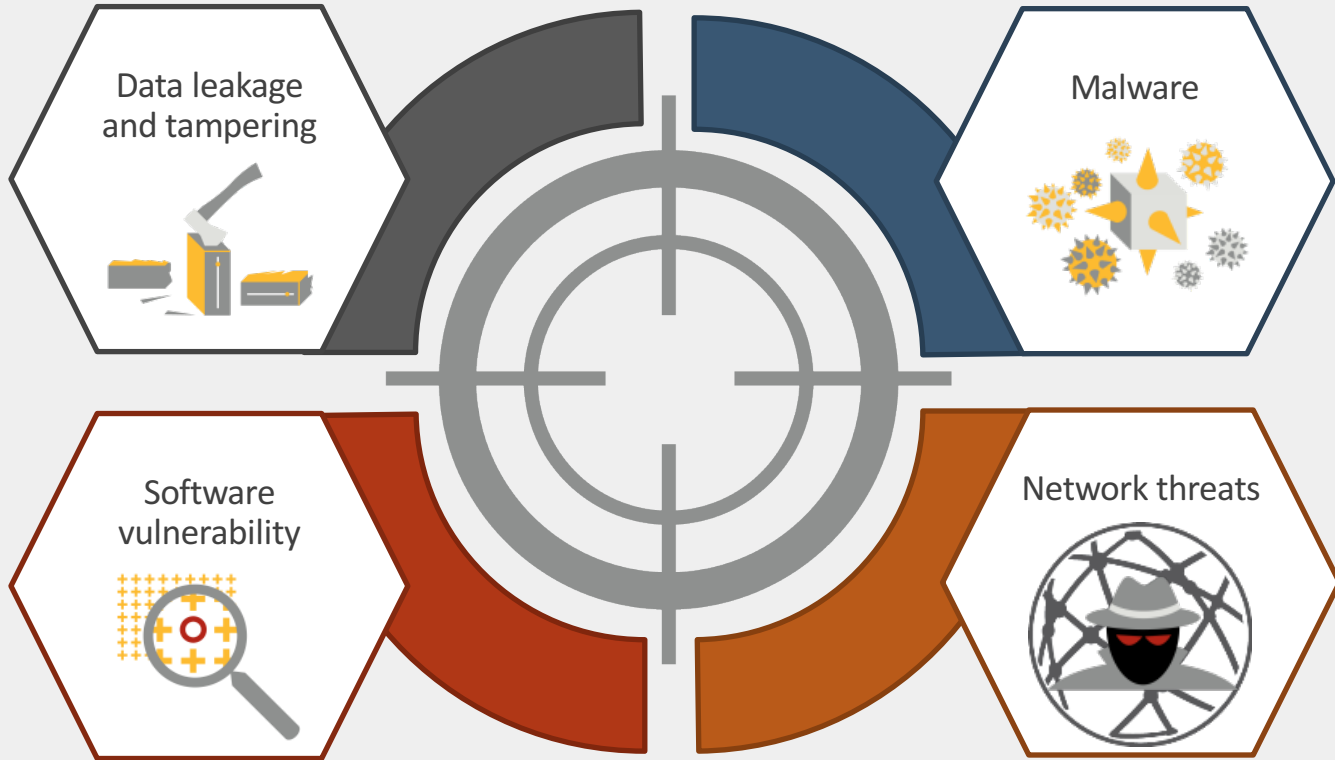
Superior Protection

Better Performance

Easy Integration & Automation

Protecting the endpoint

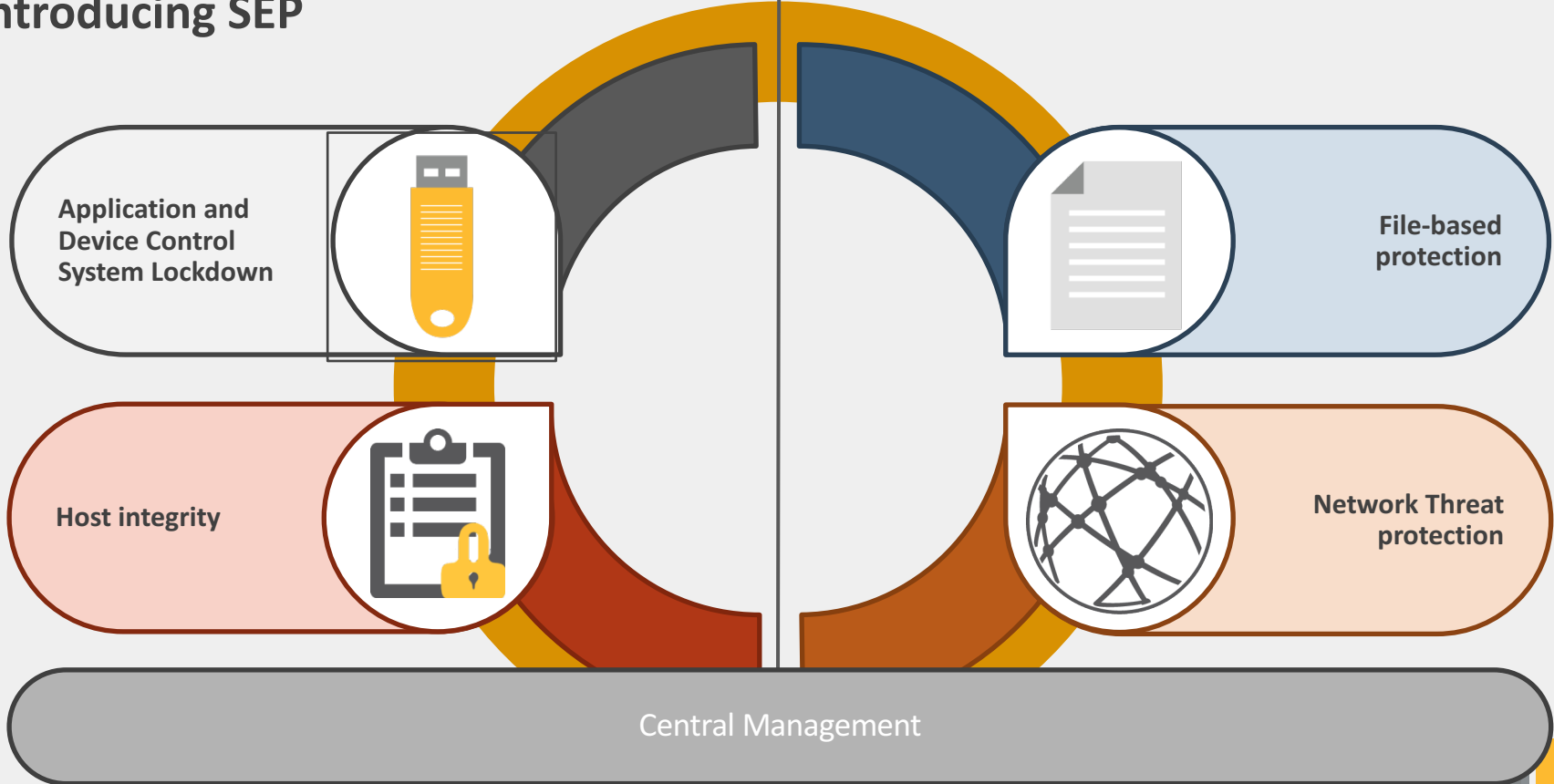
Your endpoints are the target



Introducing SEP

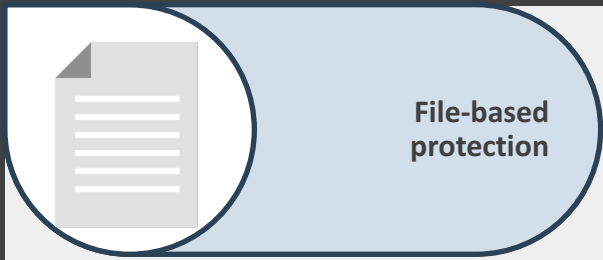
COMPLIANCE

THREAT PROTECTION

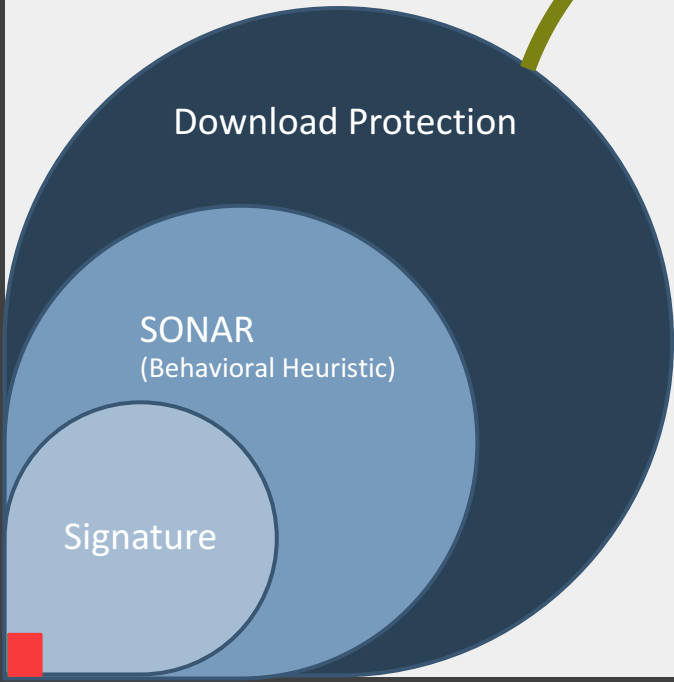


Protection layers | Single agent





Zero-day threats and reduced false positives



Download protection protects against new and unknown files that traditional signature-based security does not detect. Detections are based on the prevalence, age, source and overall reputation given by Insight.

SONAR is a real-time monitoring heuristic system that targets malicious behavior. It leverages Insight to provide zero-day threat protection and signature-less mitigation.

Signature engine is the traditional Antivirus feature matching threats against signatures. It still accounts for 50% of all detections in 2014. The engine also leverages Insight for false positive prevention. Signatures are used for files and emails scans.

Static Data Scanner



SDS Engine



Emulator:
VM for packed
threat



SAPE:
Machine
learning engine



ITCS:
Cloud- based
scanning



CoreDef-3 :
Lightweight AV
Signatures

- Emulator: Analyze the payload by executing a packed threat in a local virtualized sandbox.
- SAPE: Determines if a file is good or bad based on experience, criteria set by analysts, and behavior.
- ITCS: Reduces resource and storage overhead by keeping the most relevant signatures locally and applying small updates when needed. All other signatures are hosted in the cloud.
- CoreDef-3: Traditional antivirus engine that contains a lighter set of definitions.



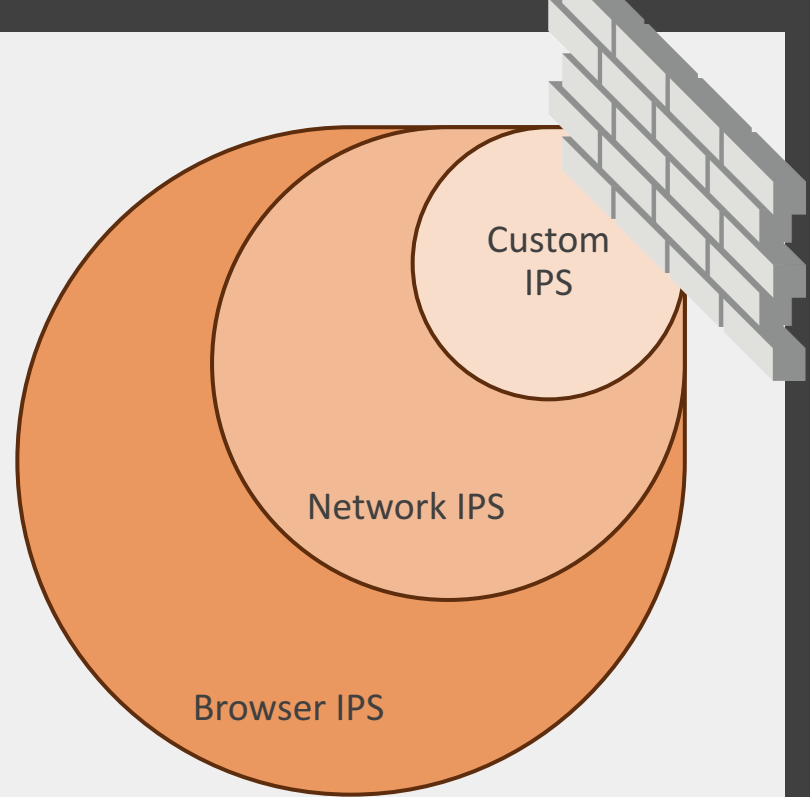
Network Threat Protection

Firewall protects against intrusion and gives control over the data entering and leaving the endpoint.

Custom IPS allows administrators to create SNORT like signatures at the packet level (OSI Layer 2)

Network IPS is stream-based filtering that uses generic exploit blocking (GEM) to block threats using a published vulnerability. (OSI Layer 5)

Browser IPS protects against obfuscated attacks at the browser level. (Encrypted Java, ActiveX, Flash, and more). (OSI Layer 7). Browser Protection works with Firefox and Internet Explorer.





Network Threat Protection

Application

•• Insight, Browser Protection, SONAR, Virus and Spyware Protection and Application Control

Presentation

•• Browser Protection and Insight

Session

•• Firewall and IPS

Transport

•• Firewall

Network

•• Firewall

Data link

•• Firewall and Custom IPS

Physical

•• Device Control



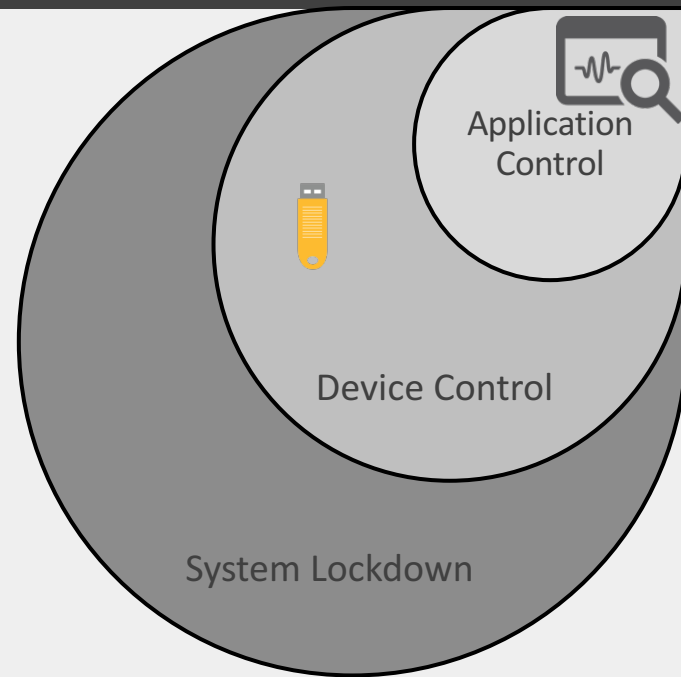


Application and Device Control

Application Control blocks unwanted applications based on hash or filename.

Device Control blocks unauthorized hardware to be connected to the endpoint. Prevents data leakage and dual homing networks.

System Lockdown leverages Application Control to whitelist or blacklist a set of applications. Commonly used in static environments like embedded systems and secure workstations.





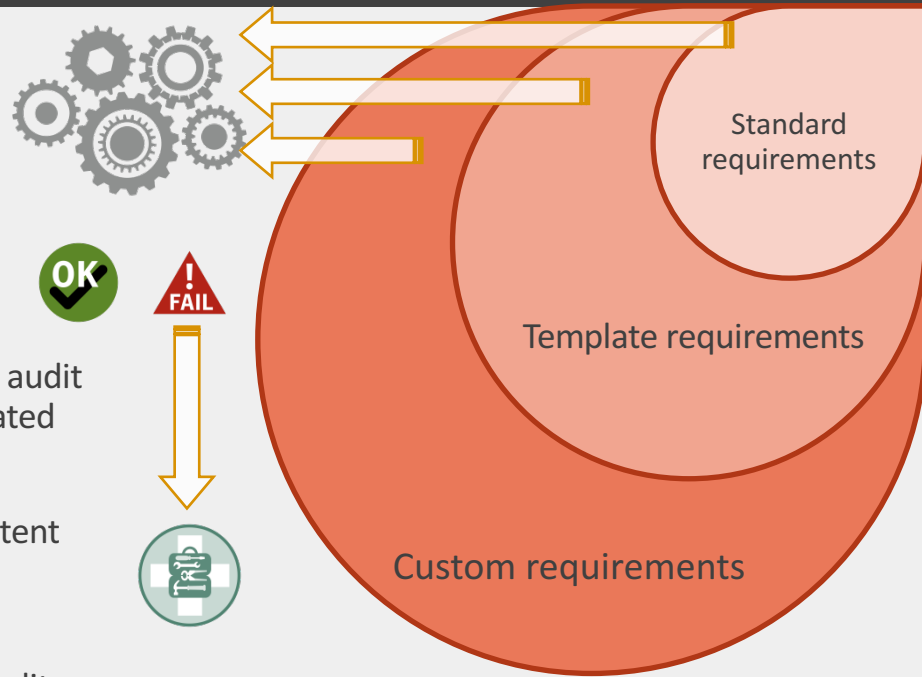
Host integrity

Host integrity audits the endpoint against requirements. The audit gives a **PASS** or **FAIL** result, which is translated into an automated remediation.

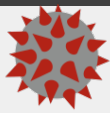
Standard requirements include Endpoint security status, content updates, critical patches, and more.

Template requirements can be retrieved via LiveUpdate to audit advanced requirements, such as password complexity or presence of a second NIC connected to the system.

Custom requirement is a feature that provides a simple method to execute programs and scripts to evaluate and remediate any aspect of the endpoint.



Insight



-127

CALCULATING SCORE

127



Insight is the largest reputation data file system in the world and leverages more than 175 million endpoints to gather information on binary executable files.



Age: Insight looks at how long a file has been created because malware tends to be very new when infecting a system.



Prevalence: Insight keeps count of how many endpoints ran or downloaded a given application.



Source and System Hygiene: Insight uses a rating system: The number of system infections and where the threat came from to determine an accurate reputation score.

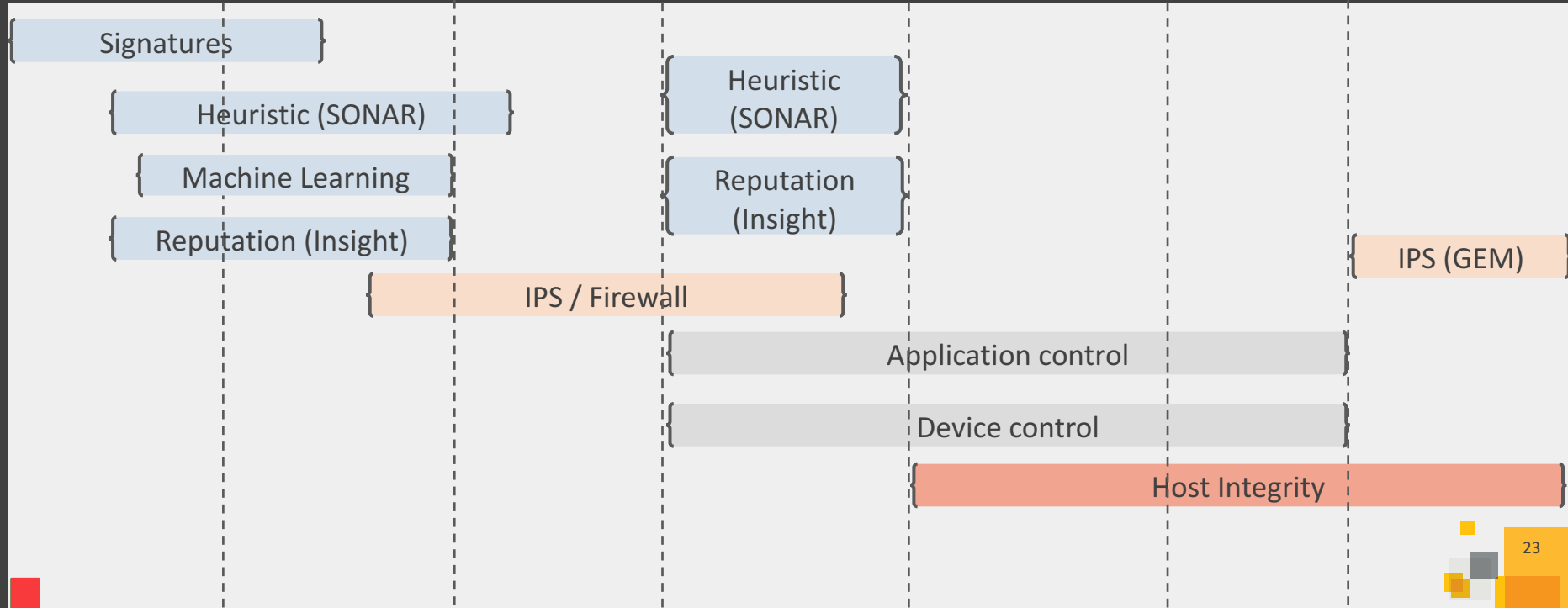


Previous Conviction: Insight leverages telemetry from features like file-based protection, IPS or SONAR to determine if a file already had a malicious behavior on another system.



Threat spectrum vs SEP features

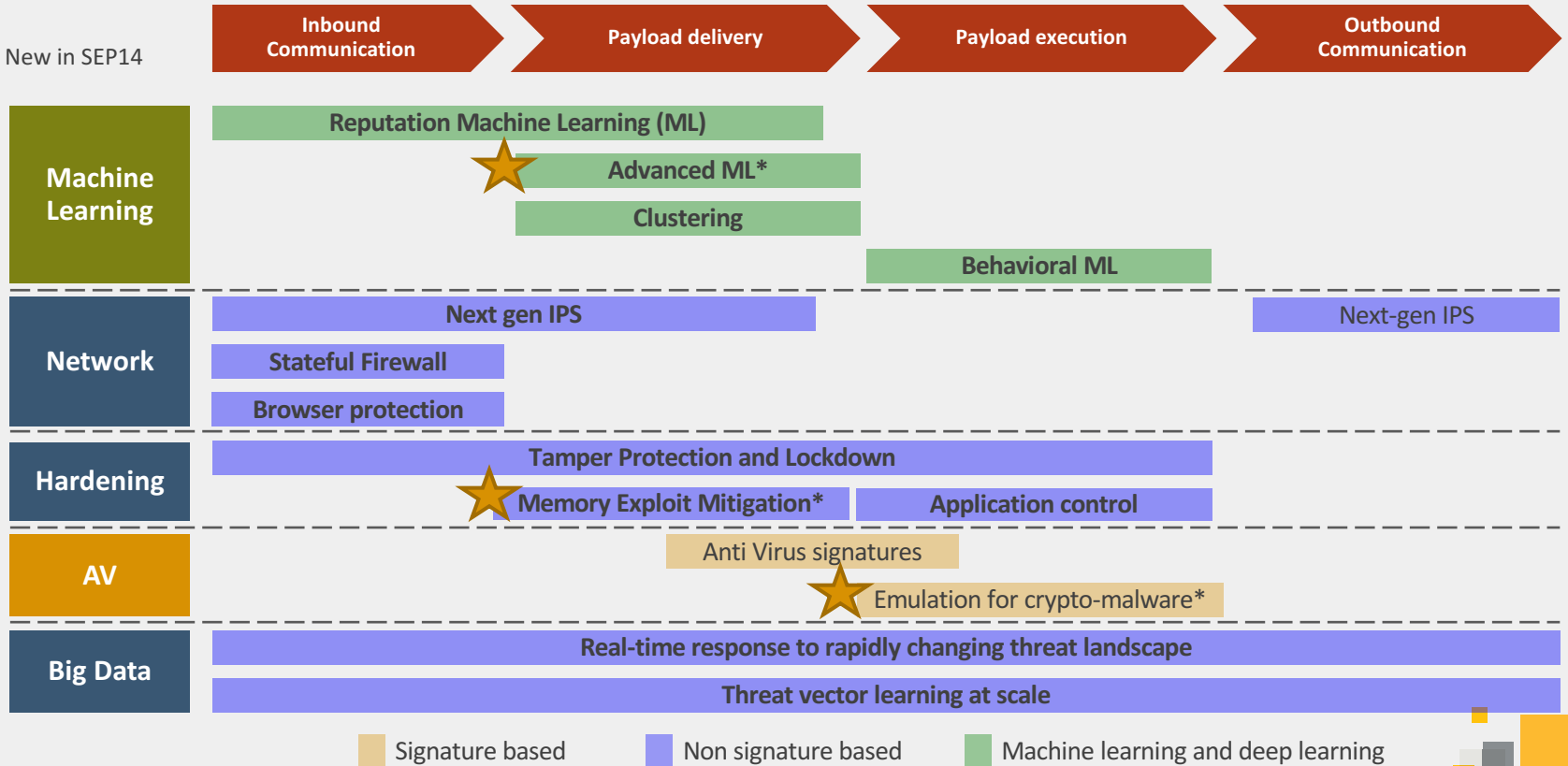
Known Malware New Malware Network Attack Social Engineering System Tampering Data Theft Vulnerabilities



Protection across the attack chain



New in SEP14





Performance or protection. Why choose?

BLAZING PERFORMANCE WITH **INSIGHT**

Up to **70%** reduction in scan overhead by only scanning unknown files



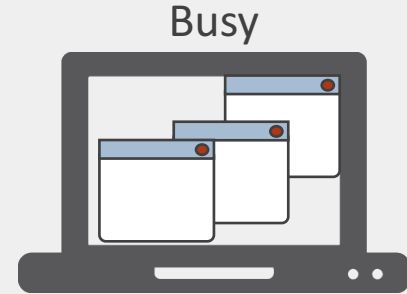
Traditional scan



Scan powered by Insight

Scan throttling

Scheduled scans use less resources when you need your system



SEP
CPU Usage



SEP
Uses up to 75%
resources

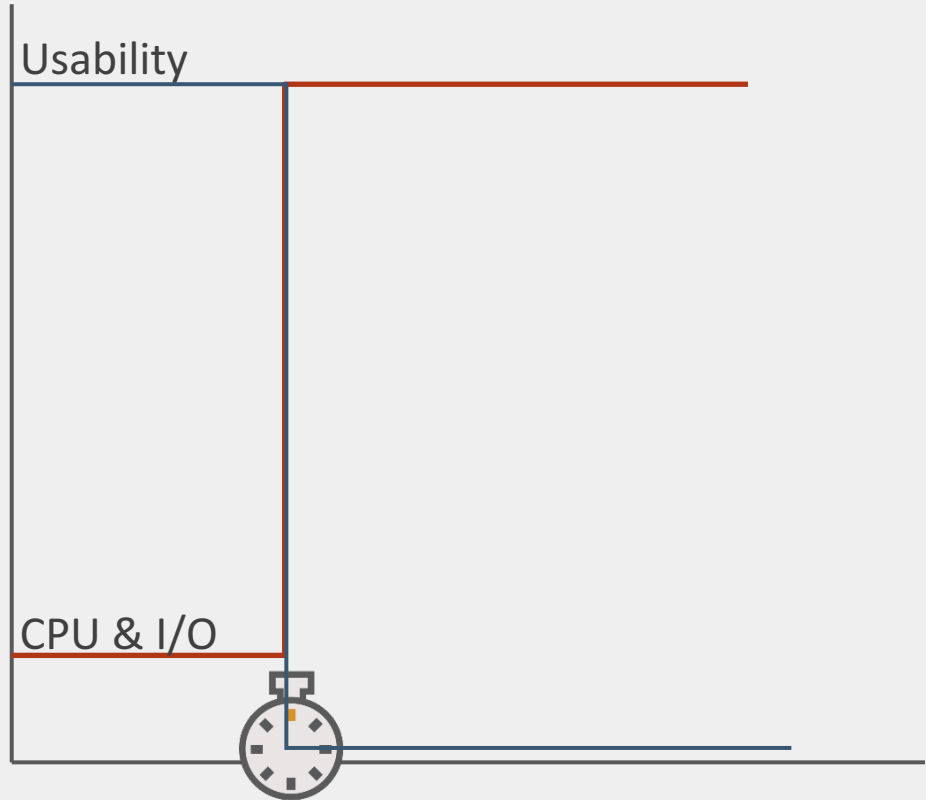
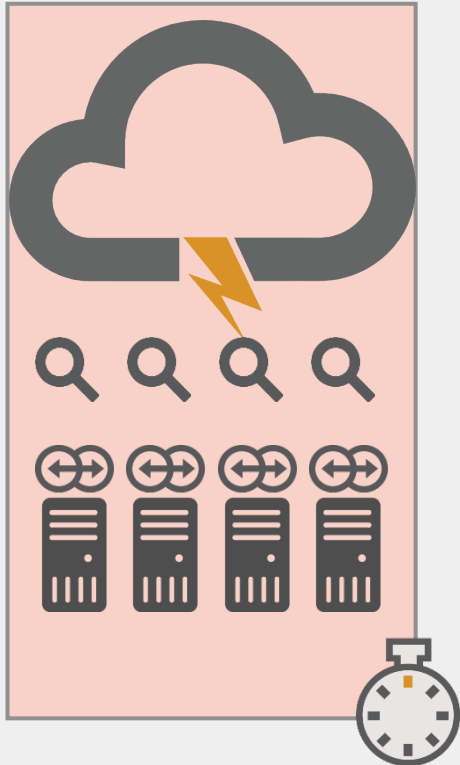
Scenario	CPU/Disk	User	Best App	Balanced	Best Scan
Busy Server	Busy	Idle	Throttled	Throttled	Running
Using PC	Busy	Busy	Paused	Throttled	Running
Moving Mouse	Idle	Busy	Paused	Throttled	Running
Lunchtime	Idle	Idle	Running	Running	Running



SEP
reduces its
resources usage

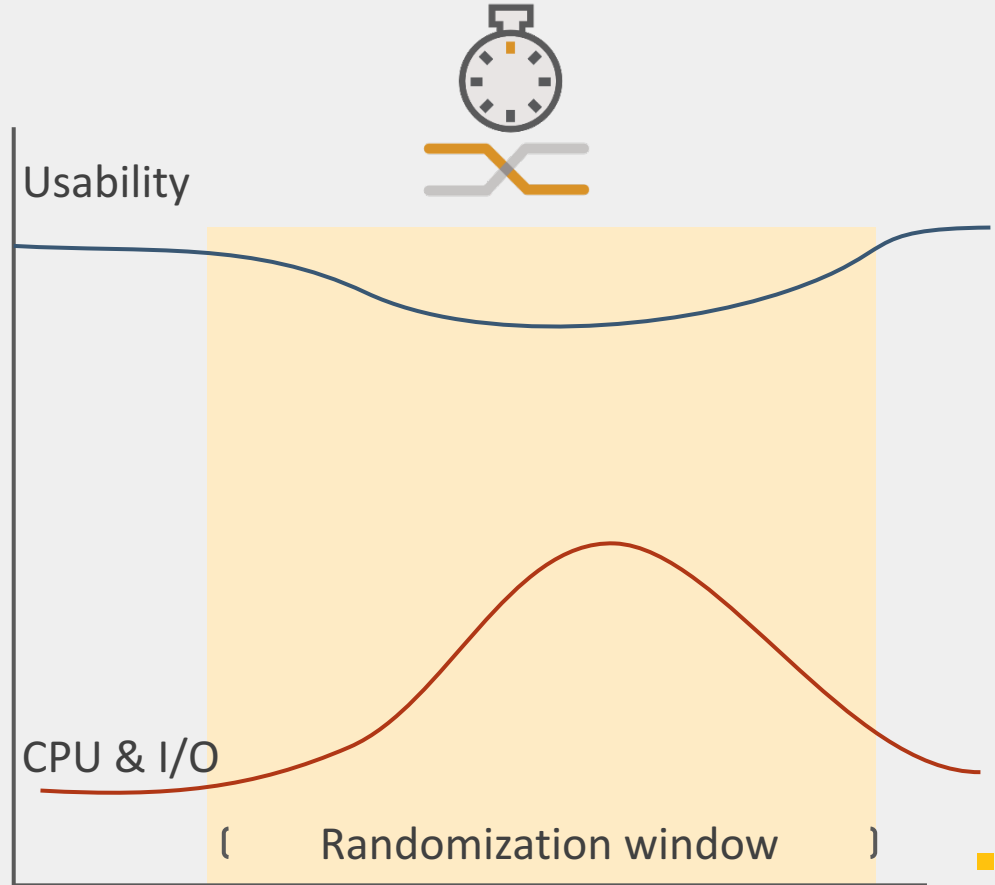
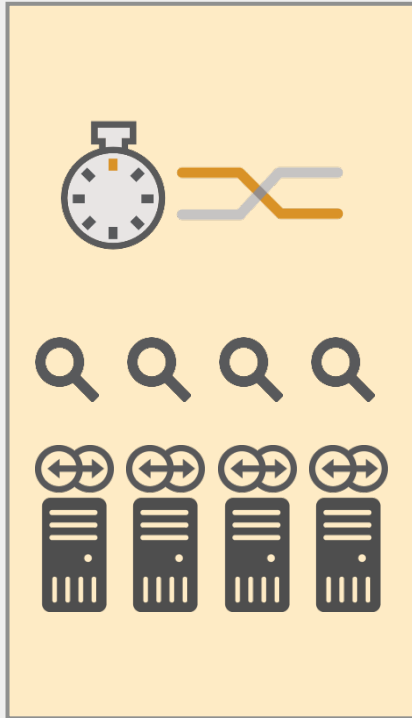
Scan randomization

Preventing the AV storm



Scan randomization

Preventing the AV storm



Virtualized and embedded system optimizations

Built for all endpoints

Limited storage

Reduced-size client: Smaller footprint and lighter content update.

Resource sharing

CoreDef-3 with size enhancement.
ITCS enabled.

License cost

VDI specific settings

Embedded and VDI client installation package

- Contains a smaller set of Virus and Spyware content distribution files
- Contains a reduced-package size that includes all features:
 - Virus and Spyware*
 - Firewall
 - IPS
 - SONAR
 - System Lockdown
 - Application Control, and more
- More NTFS compression where possible
- No installer cache

45 MB



Standard Client

45 MB



Embedded and VDI Client

Estimated definition size: 170 MB

75 MB

Embedded and VDI Virus and Spyware content

- Distributed three times per day on week days and once a day on weekends
- Separate download from the console
- Content specific to the lightweight client
- Contains less signatures than the traditional set



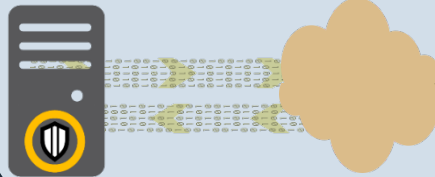
Intelligent Threat Cloud services details

Projected size
range of AV
definitions on the
local disk.



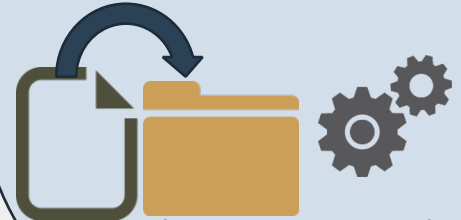
75 MB – 170 MB

Average query
time to the cloud



1.7 seconds

Performance
degradation?



Less than 5% compared
to SEP 12.1.6 scan

Client types and definitions types

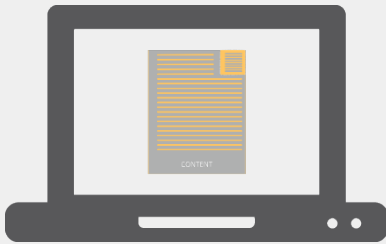


	Standard	Embedded and VDI	Dark network
Definition type	CoreDef-3	CoreDef-3 with size enhancement	CoreDef-1.5
ITCS enabled	Yes	Yes	No
Estimated package size (Network traffic)	~45MB	~45MB	~360MB
Estimated definition size on disk (Full.zip)	~170MB	~75MB	>700MB



The SEP 12.x clients use coreDef-1.5. When you upgrade these clients to SEP 14, they are migrated to CoreDef-3.

Differences between SEP 12.1 and SEP 14 definition sizes



SEP 12.1 Standard

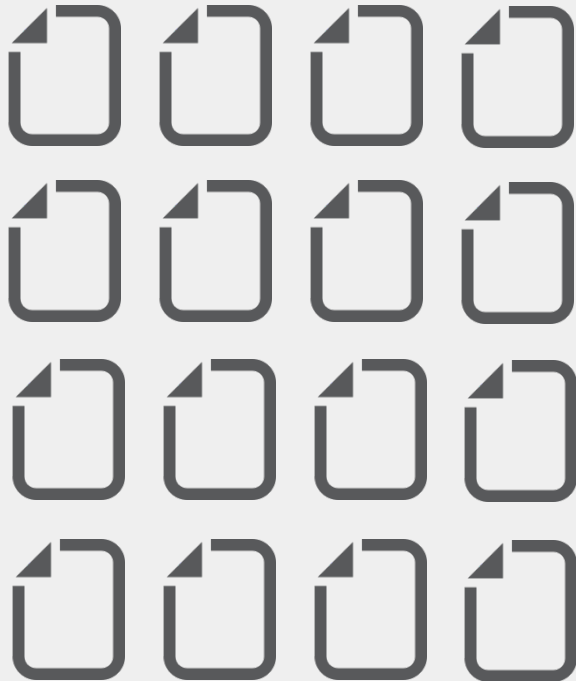
SEP 12.1 Reduced

SEP 14 Standard

SEP 14 Embedded and VDI

	SEP 12.1 Standard	SEP 12.1 Reduced	SEP 14 Standard	SEP 14 Embedded and VDI
Definition type	CoreDef-1.5	CoreDef-3 with size enhancement	CoreDef-3	CoreDef-3 with size enhancement
ITCS enabled	No	No	Yes	Yes
Estimated package size (Network traffic)	~360 MB	~45 MB	~45MB	~45MB
Estimated definition size on disk (Full.zip)	~700 MB	~75 mb	~170MB	~75MB

What if you can skip all the *standard* files in a VM ?



By default, SEP 14.x trusts and skips most of the OS and some applications.

There are still some files present in the VM template that are not a threat and those files are scanned over and over.

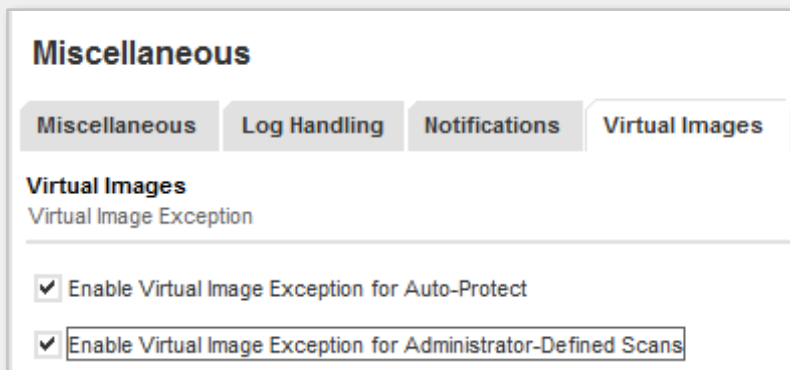
Virtual Image Exception VIE sets all the files present on the VM template as trusted by adding them to the local SEP reputation store.

When a VIE enabled template is cloned... We scan very little



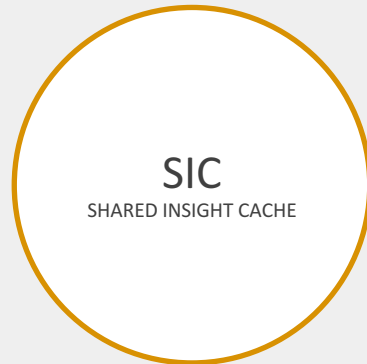
When the new VM is based on the VIE trusted image, only new documents and applications are scanned.

This reduced I/O applies to both real-time, on-demand, and scheduled scans.



Shared Insight Cache

- Shared Insight Cache (SIC) is a server application which caches known clean files in order to optimize **scheduled scan** performances.
- The SIC server is mainly designed for virtual environments, but usage on physical system is supported given that network latency is kept at an absolute low.
- The SIC server keeps a record in memory (RAM) of files which are voted clean by system performing scans.



SEP for VDI

Agent

- Features
 - SONAR Behavior
 - Intrusion Prevention
 - Browser Protection
 - Firewall
 - Network IPS
 - Application Device Control
 - Insight Reputation
 - Console to manage SEP

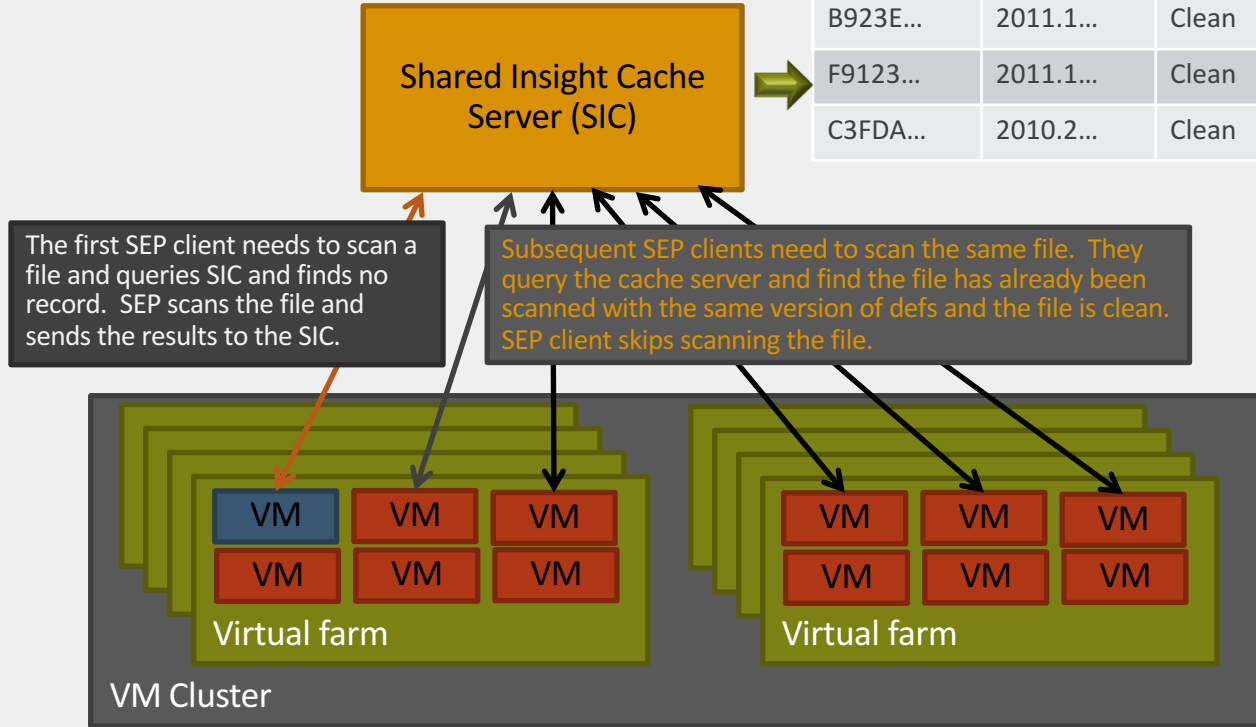
Agentless

- Features
 - Agentless Anti-Malware
 - Insight file reputation
 - Agentless Network IPS (requires NSX)
 - Console to manage DCS

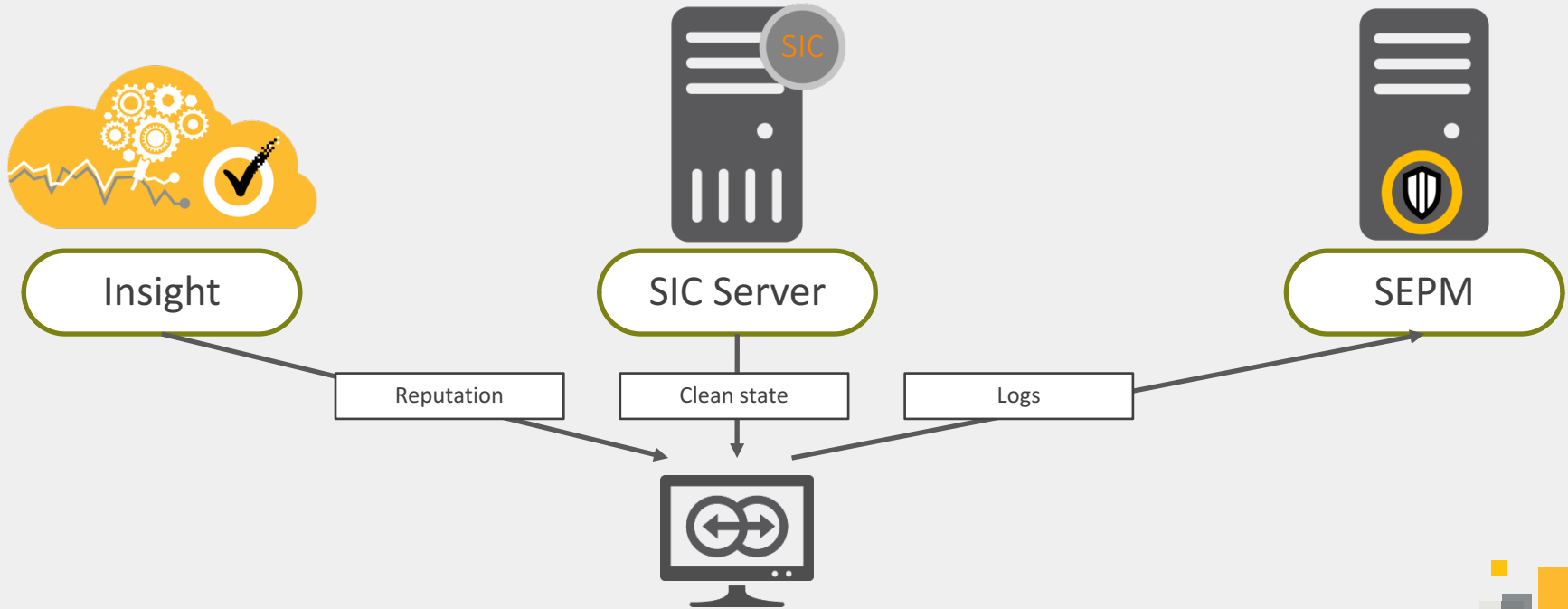
- Windows Desktop Supportability: Windows 7/Windows 8
- System Requirements: VMware NSX/VMware ESXi 5.5 and VMware vShield/ESXi 5.1+

Shared Insight Cache: High Level

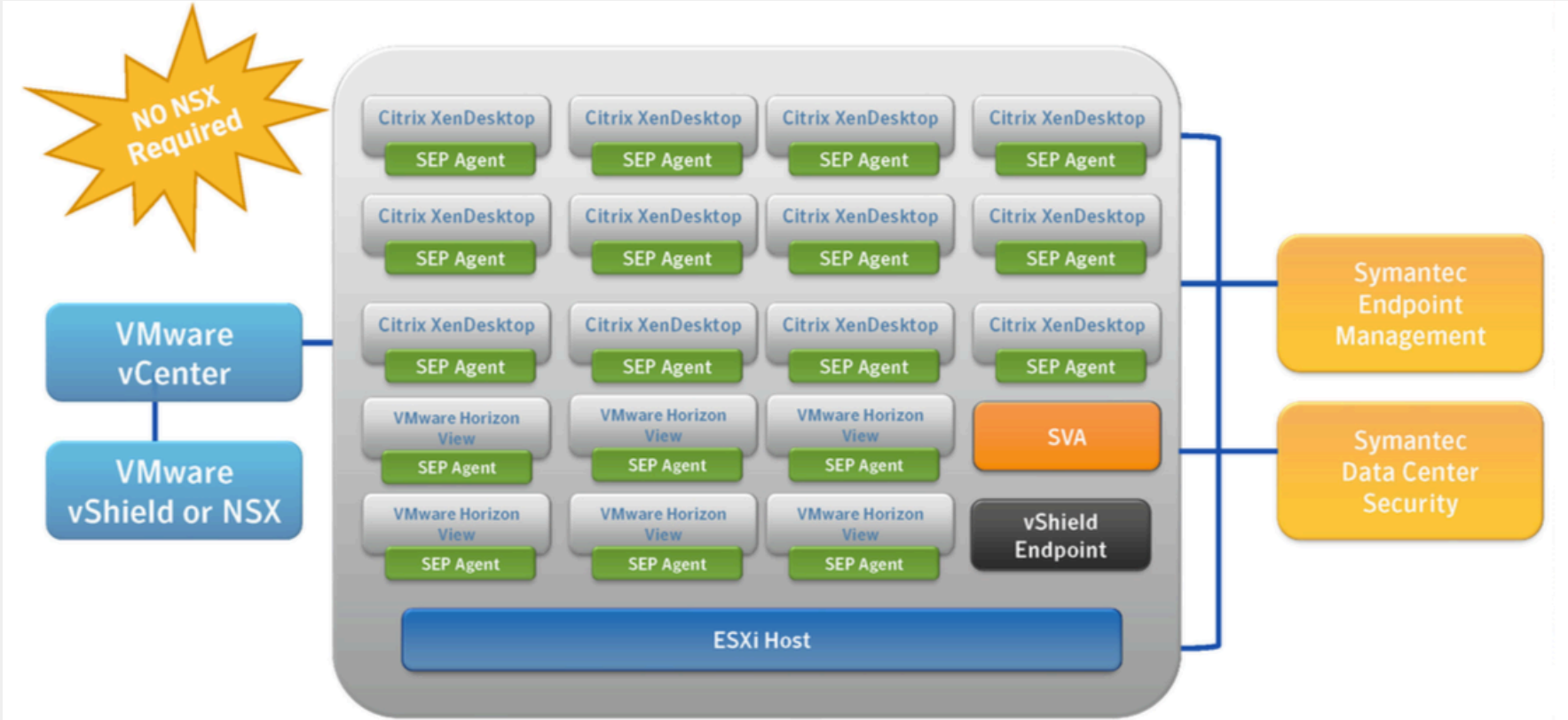
File Hash	Def Ver	Result
AE32D...	2011.1...	Clean
B923E...	2011.1...	Clean
F9123...	2011.1...	Clean
C3FDA...	2010.2...	Clean



Shared insight cache architecture



Symantec Endpoint Protection for Virtual Desktop Infrastructure (VDI)



Non-persistent VDI refinements

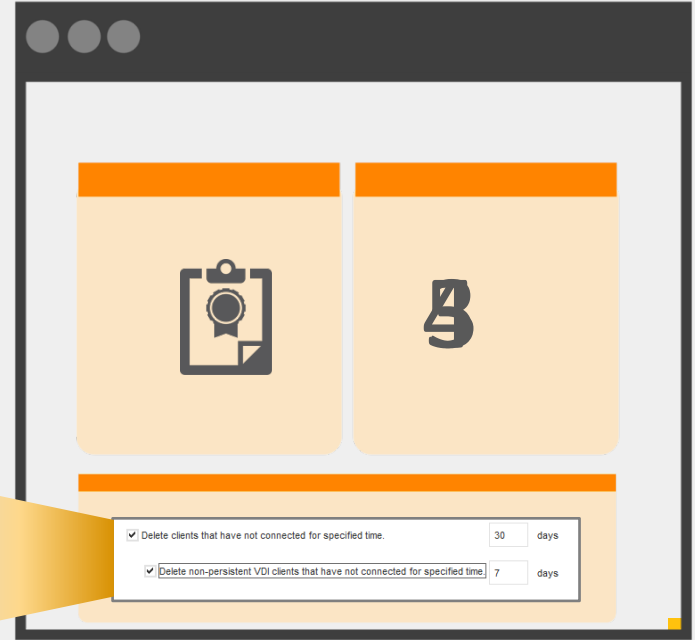


- VDI licensing scheme
 - Shorter retention time equals more licenses available
 - Set the client as VDI in the template
 - Configure the Manager to set the separate retention scheme

– Select Admin > Domain properties

Delete clients that have not connected for specified time. days

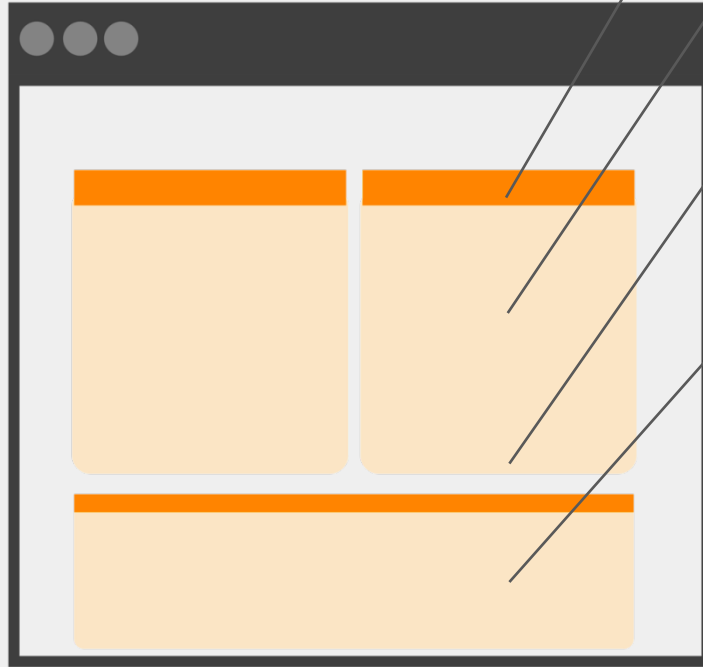
Delete non-persistent VDI clients that have not connected for specified time. days





Streamlined management and reporting across platform

Single console Multiples agents



Policies

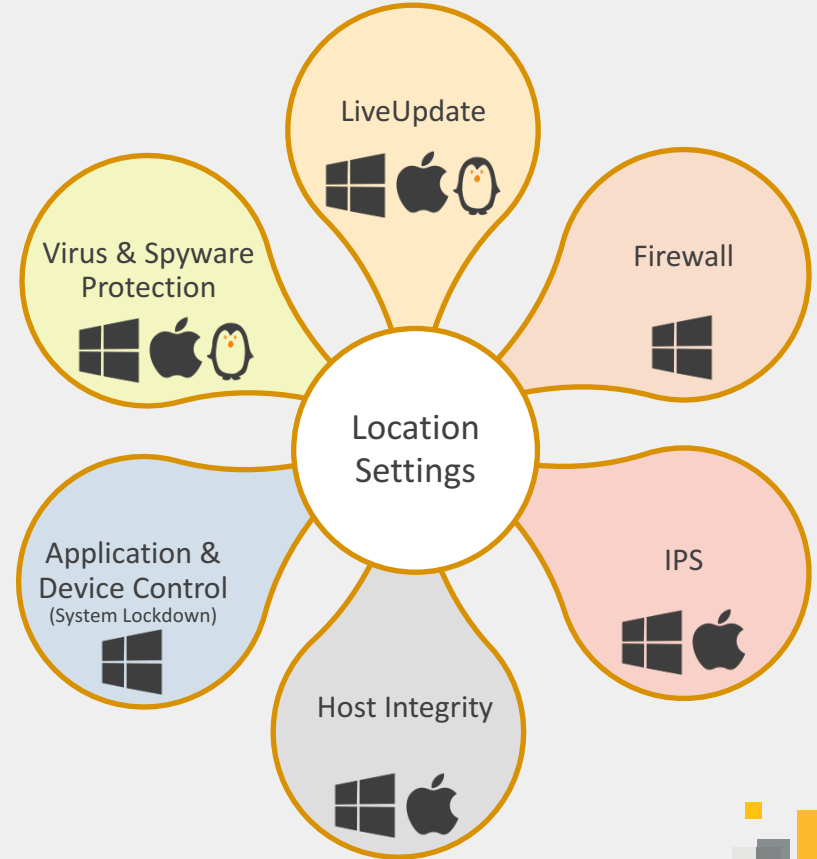
Reporting

Alerting

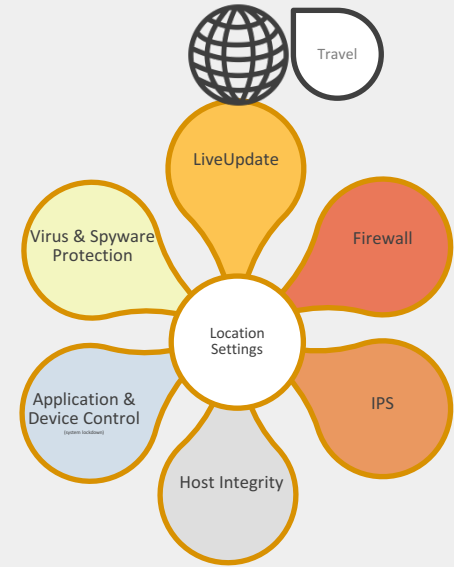
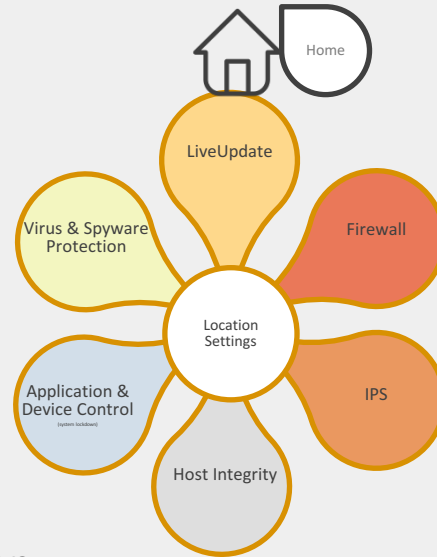
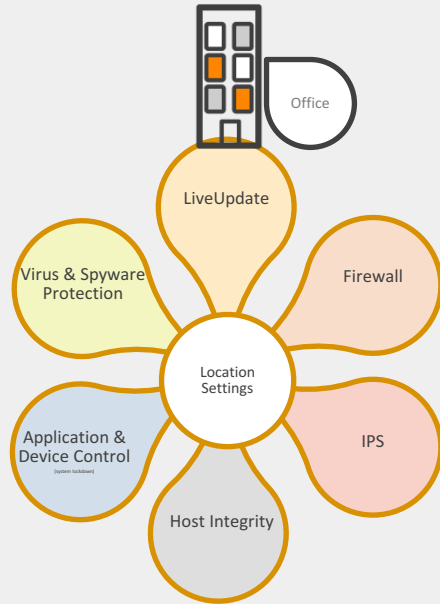
Management

Policies

- Central configuration
- Location aware settings
- Manual grouping or Active Directory import
- Tree structure inheritance



Location awareness



- Adapts all policies based on location
- Location determination uses Boolean logic and multiple criteria making impossible to “fake” a location:

Office location = Gateway mac address + Connected to SEPM + Resolve intranet site to a given IP

Reporting

- Three views:
 - Dashboard: Overview
 - Monitors: Tables and logs
 - Reports: Graphs
- Exports:
 - CSV, MHTML (alerts)
- Actionable reports:
 - Launch scan, update, and remediate
- Alerts:
 - Console
 - Email

The screenshot shows the Symantec Endpoint Protection Manager interface. The top navigation bar includes 'Home', 'Monitors', 'Reports', 'Policies', 'Clients', and 'Admin'. The main content area is titled 'Reporting - Comprehensive Risk Report' and displays a 'Risk Distribution by Risk Type' section. This section includes a donut chart showing the distribution of risk types and a corresponding histogram table.

Risk Distribution by Risk Type
2 entries
Top Risk Types as Pie Chart

Risk Type	Number	%
Security Assessment Tool	3	60
Application Heuristic	2	40

Risk Type as Histogram

Risk Type	Number	%
Security Assessment Tool	3	60
Application Heuristic	2	40

Risk Distribution by Computer
1 entries

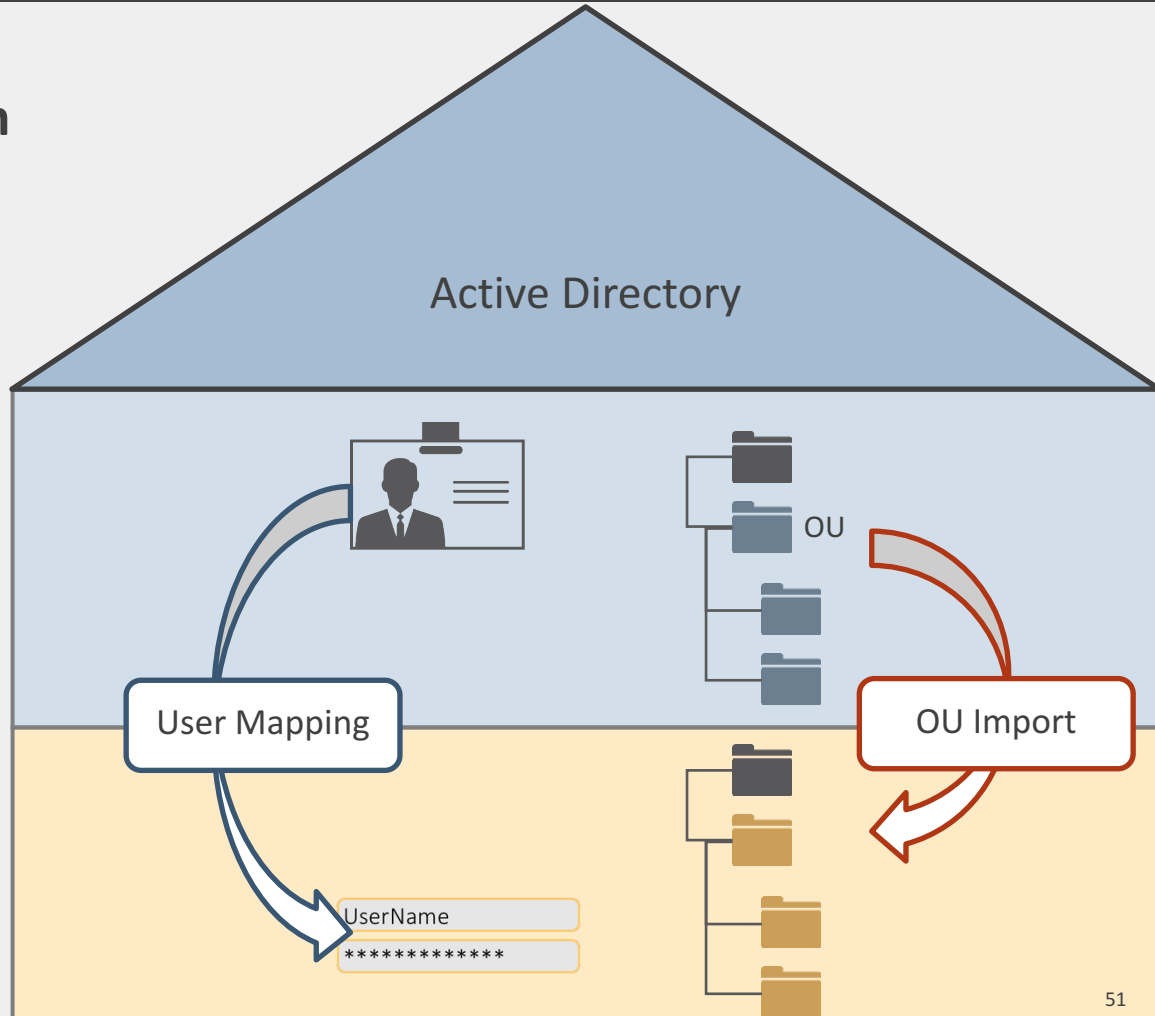
Alerting and scheduled reports

- Email or Console
- Preconfigured conditions
- You can create your own alerts for a selected number of events
- Alert equals live data that can change over time
- Scheduled report equals Static data at a given point

Authentication failure
Client list changed
Client security alert
Download Protection content out-of-date
File reputation lookup alert
Forced application detected
Generic Exploit Mitigation Detection
IPS signature out-of-date
Licensing issue
Network load alert: requests for virus and spyware full definitions
New learned application
New risk detected
New software package
New user-allowed download
Power Eraser recommended
Risk outbreak
Server health
Single risk event
SONAR definitions out-of-date
System event
Unmanaged computers
Virus definitions out-of-date

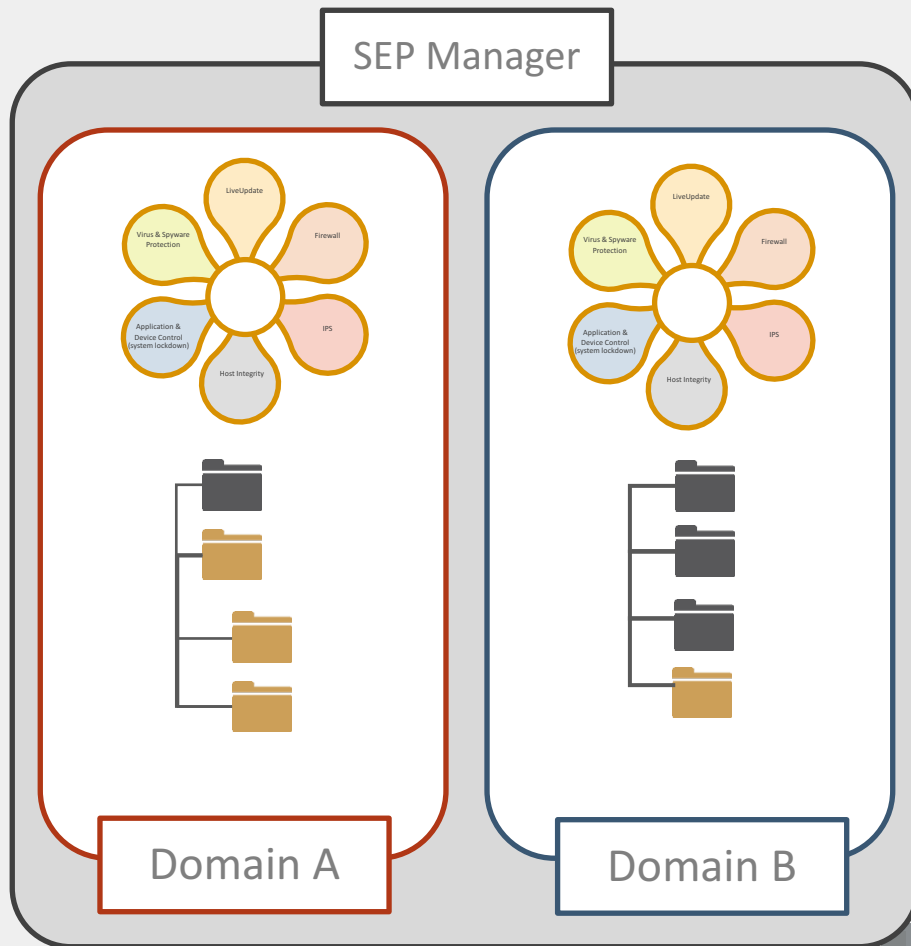
Active Directory integration

- Organizational unit synchronization
 - Client grouping matching Active Directory
 - No support for Active Directory groups
- Console login SSO
Password changes when the Windows account changes




Domains


- Can separate entities while using the same management server.
- Separate:
 - Policies
 - Groups structure
 - Reporting and alerting settings
- Mostly used by service providers or large environment with multiple IT teams




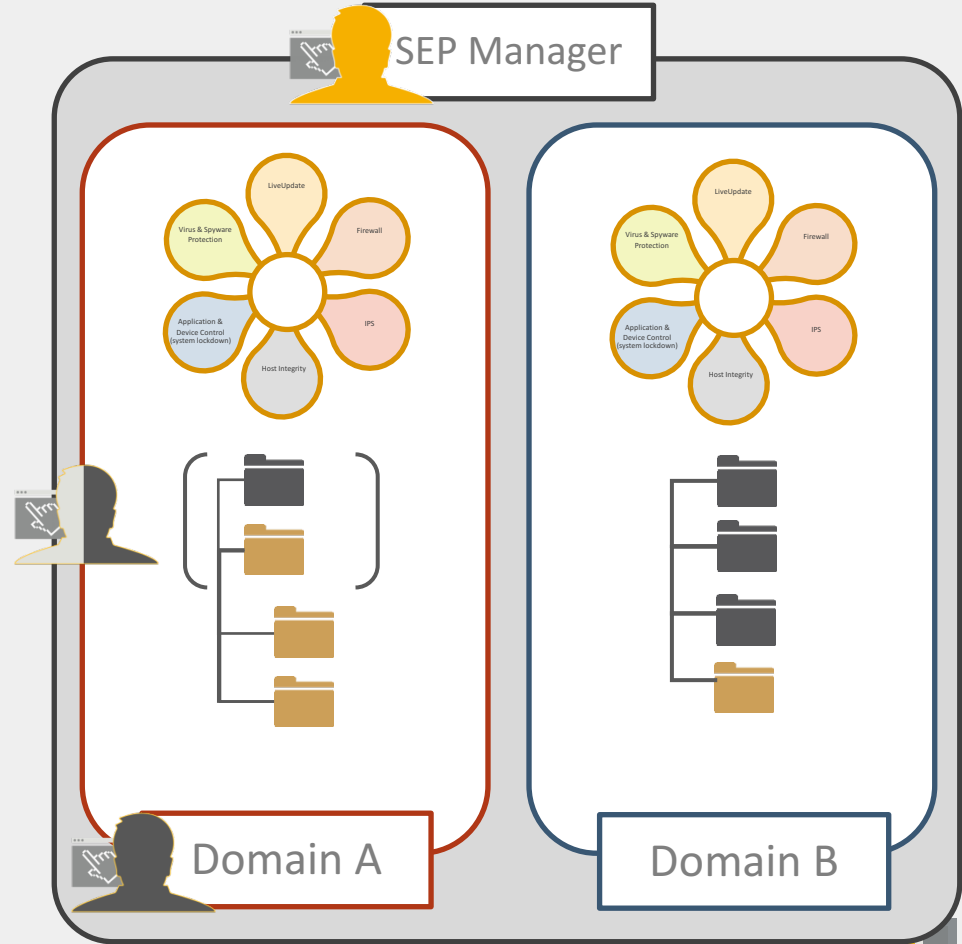
Account delegation

Console with multiple access levels:

 System Admin has access to all settings.

 Domain Admin has access to settings for a single domain.

 Limited Admin has limited access to some settings for a single domain



Product Integration

Symantec Endpoint Protection integration

Advanced reporting

Syslog Server

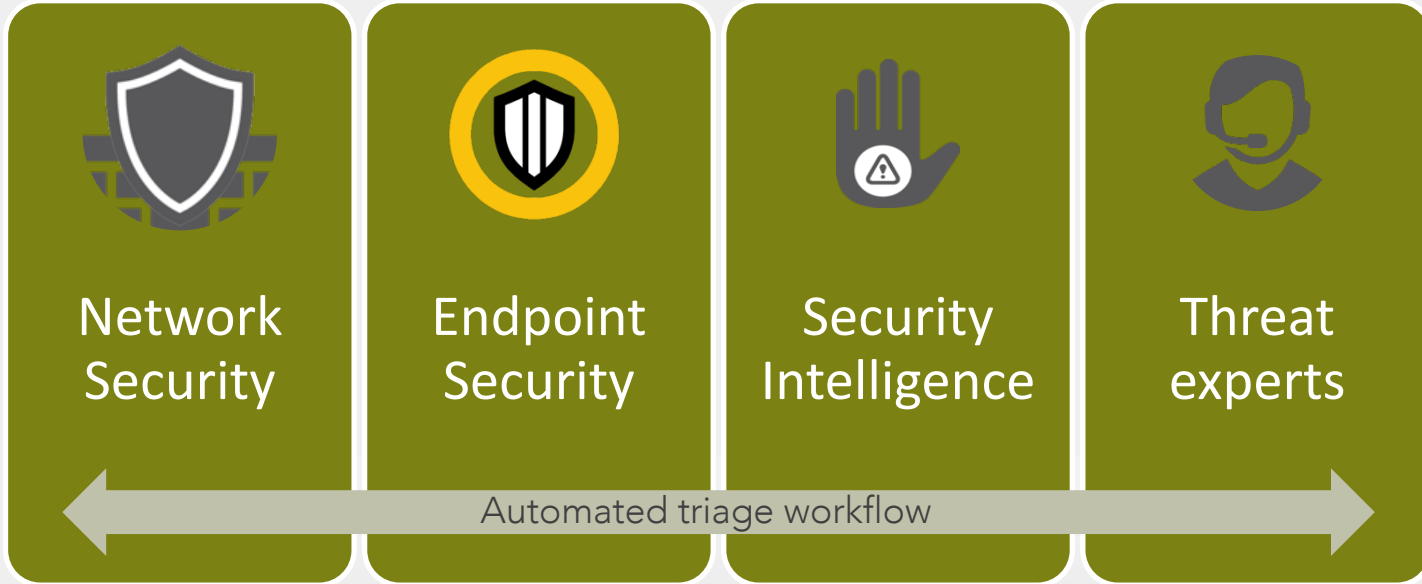
IT Analytics

Threat detection

Managed Services Agent

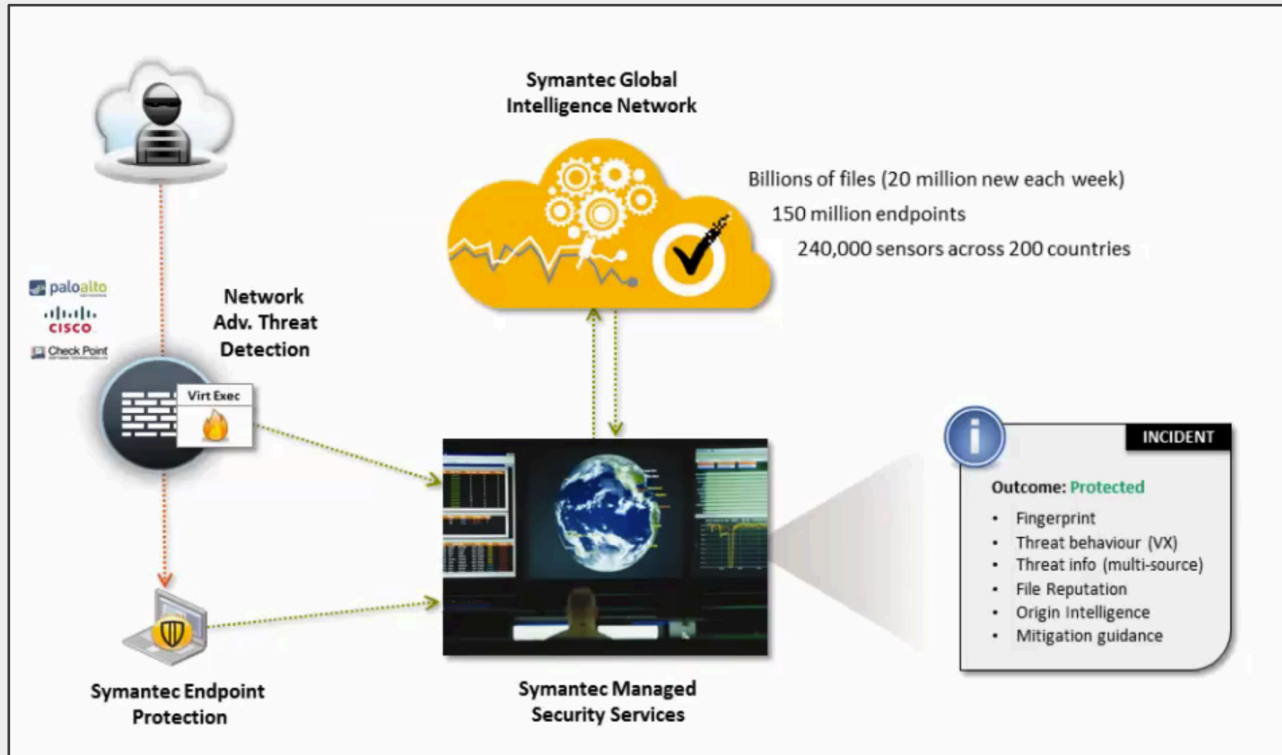


Managed Security Services



Rapid Response | Operational Efficiency | Attack Visibility

MSS overview



IT Analytics benefits



Syslog

External Logging for Local Site (My Site)

General Log Filter

Send logs to a Syslog Server or export to a file.

Update Frequency: 30 seconds Master Logging Server: wsepm

Enable Transmission of Logs to a Syslog Server

Syslog Server: 10.10.2.1

Destination Port: TCP 1468

Log Facility: 6

Log Line Separator: CR

Export Logs to a Dump File

Limit Dump File Records

Management Server Logs		Client Logs	
System Administrative Log Limit:	1000 entries	Client Activity Log Limit:	1000 entries
System Client-Server Activity Log Limit:	1000 entries	Security Log Limit:	1000 entries
Audit Log Limit:	1000 entries	Traffic Log Limit:	1000 entries
System Server Activity Log Limit:	1000 entries	Packet Log Limit:	1000 entries
		Control Log Limit:	1000 entries
		Scan Log Limit:	1000 entries
		Risk Log Limit:	1000 entries
		SONAR Protection Log Limit:	1000 entries

OK Cancel Help

- SEPM can send events to a Syslog server.
- Events can be parsed and generate alerts and tickets with third-party Event management solutions.

Extend SEP capabilities with the SEPM API Service

Symantec Endpoint Protection Manager

Client Management	Application & Device Control	Policy Control	Reports & Analytics
-------------------	------------------------------	----------------	---------------------

REST API's

SEP14 - API's

Login & Logout of SEPM

Obtain a list of groups

Assign a fingerprint list to a group for system lockdown.

Retrieve the Symantec Endpoint Manager version information

Add or delete a blacklist as a file fingerprint list

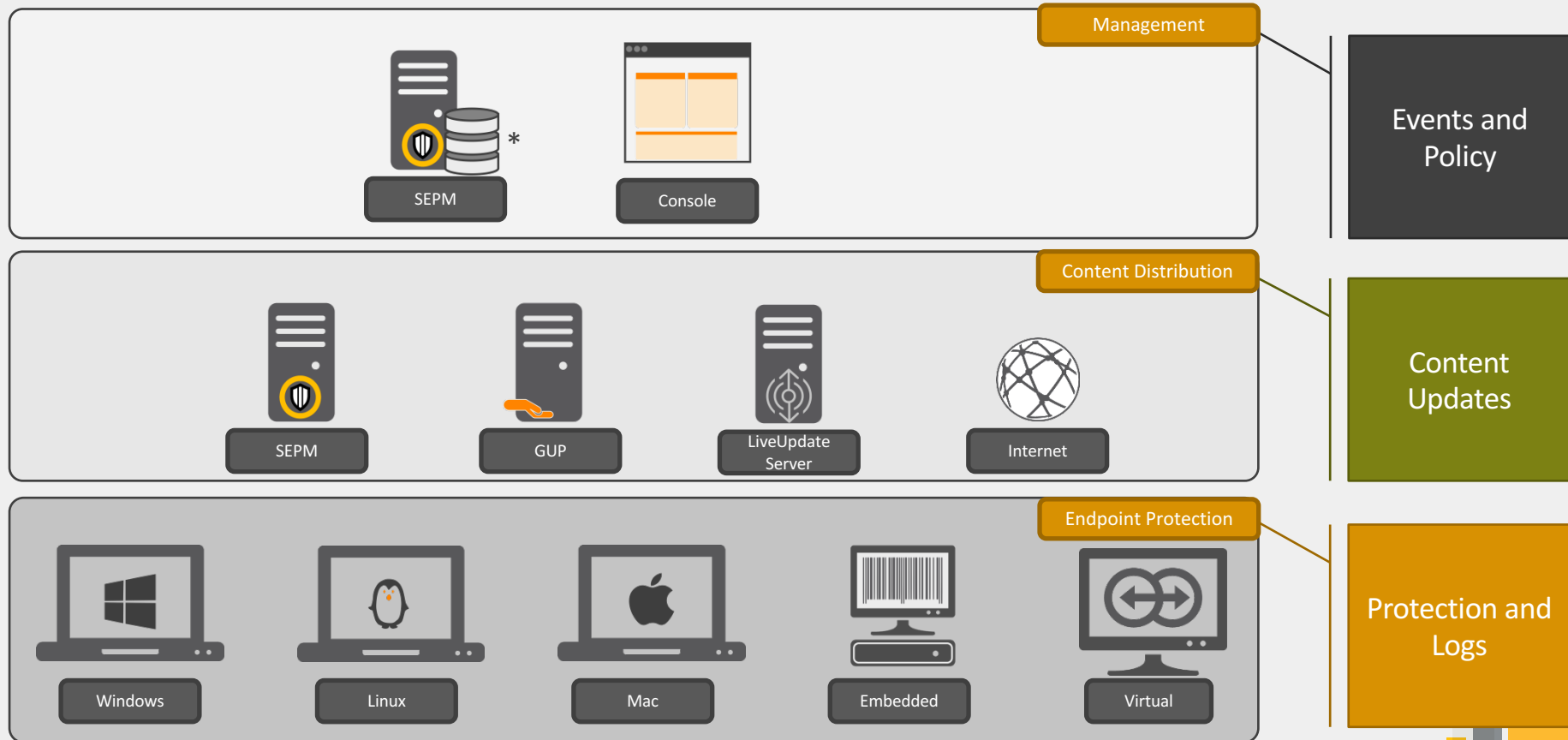
RESTful API to built in to SEPM to enable Programmatic integration with SEP

Customer Benefit:

- ✓ Orchestrate/automate SEPM functionality from other applications and scripts
- ✓ Connect SEP to 3rd party platforms for control or network plane integration with the endpoint

Architecture Overview

Symantec Endpoint Protection 14.x Architecture Components



* SEPM can use an embedded database of MS-SQL. MS-SQL is recommended for larger organization 1000+ Endpoints

Server architectures



SINGLE SITE

- ✓ Small environments
- ✓ Simple to implement
- ✓ No failover

<1000 Endpoints



MULTIPLE SITES

- ✓ Very large environment
- ✓ Provides failover
- ✓ Provides site disaster redundancy
- ✓ Provides geographical administration delegation
- ✓ Requires two servers per site
- ✓ MSSQL backend mandatory
- ✓ Introduces delay in log visibility due to the replication schedule

>50 000 Endpoints

Content Distribution methods



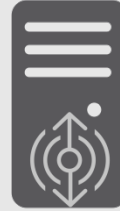
SEPM

- ✓ Direct distribution to endpoints
- ✓ Central control of content update



GUP

- ✓ Reduces WAN usage
- ✓ Acts as a content proxy
- ✓ Recommended for scattered environments
- ✓ Any client can be a GUP



LiveUpdate Server

- ✓ Provides content validation scheduling
- ✓ Distribute content to non Windows endpoints



Internet

- ✓ Rapid delivery
- ✓ Recommended for nomad users
- ✓ No central control of content used



Additional resources

Symantec Connect Forum

- Forums annotated by customers, staff, and partners
- Videos and tutorials
- Earn rewards

The screenshot shows the Symantec Connect Forum homepage. At the top, there is a search bar with the text "Enter keywords to search..." and a "Search" button. Below the search bar is a navigation bar with a home icon, "COMMUNITY: All Communities", and "Overview". To the right of the navigation bar are links for "Login or Register to participate", "English", "Help", and "Store".

The main content area features a large banner with the text "Welcome to Symantec Connect" and "Solve problems, Share knowledge, Earn rewards." Below this banner are three columns of information:

- FIND Your Community:** Content is grouped by products and topics:
 - Communities
 - Product Forums A-Z
 - Trending Topics:
 - Internet of Things
 - Security Response
 - Quick Tour
 - Help Center
- EARN Rewards:** Earn rewards points whenever you participate on Connect.
 - Earn Points
 - See Rewards
- MEET New People:** Network with people near and far.
 - User Groups
 - Upcoming Events
 - Blogs

Below the banner, there are two sections:

- Explore: Archiving and eDiscovery Community:** Features a post titled "Cloud Archiving Services for Microsoft Lync®" by Caren Havelock, a Symantec Employee. The post discusses Microsoft Lync® and its use in corporate communication. It is dated 09 Jun 2015 and has 14 comments.
- Explore: Backup and Recovery Community:** Features a post titled "Feature Pack 1 for Backup Exec 15 delivers improved performance, intelligent backups and enhanced platform support".

On the right side, there is a "Connect Activity" section with two discussion comments:

- discussion comment 07 Aug 2015: Marianne commented on: NetBackup for vmware for a linux client with NFS mount points. VMware snapshot backups will not work. What exactly is the source? Have you tried backing up from the source?
- discussion comment 07 Aug 2015: Marianne commented on: Missing drive path. See page 109 of the online manual (link in above post as well): http://filedownloads.qlogic.com/files/driver/44431/User_Guid

At the bottom right, there is a "new discussion" from Arsalan_2k posted: Netbackup appliance 5220 Fan failure error. The post includes the text: "Hi All, Can someone please guide on the below alert i have".

Symantec Education Services Offers Effective Product Training



Education Services

A broad range of training solutions to help you get the most out of Symantec products.

- Achieve expected value for your products.
- Learn how Symantec products can solve your business problems today and tomorrow.
- Gain best practice insight to keep your investments running smoothly long-term.
- For more information visit training.symantec.com

