Time Critical Management Feature

Presenter
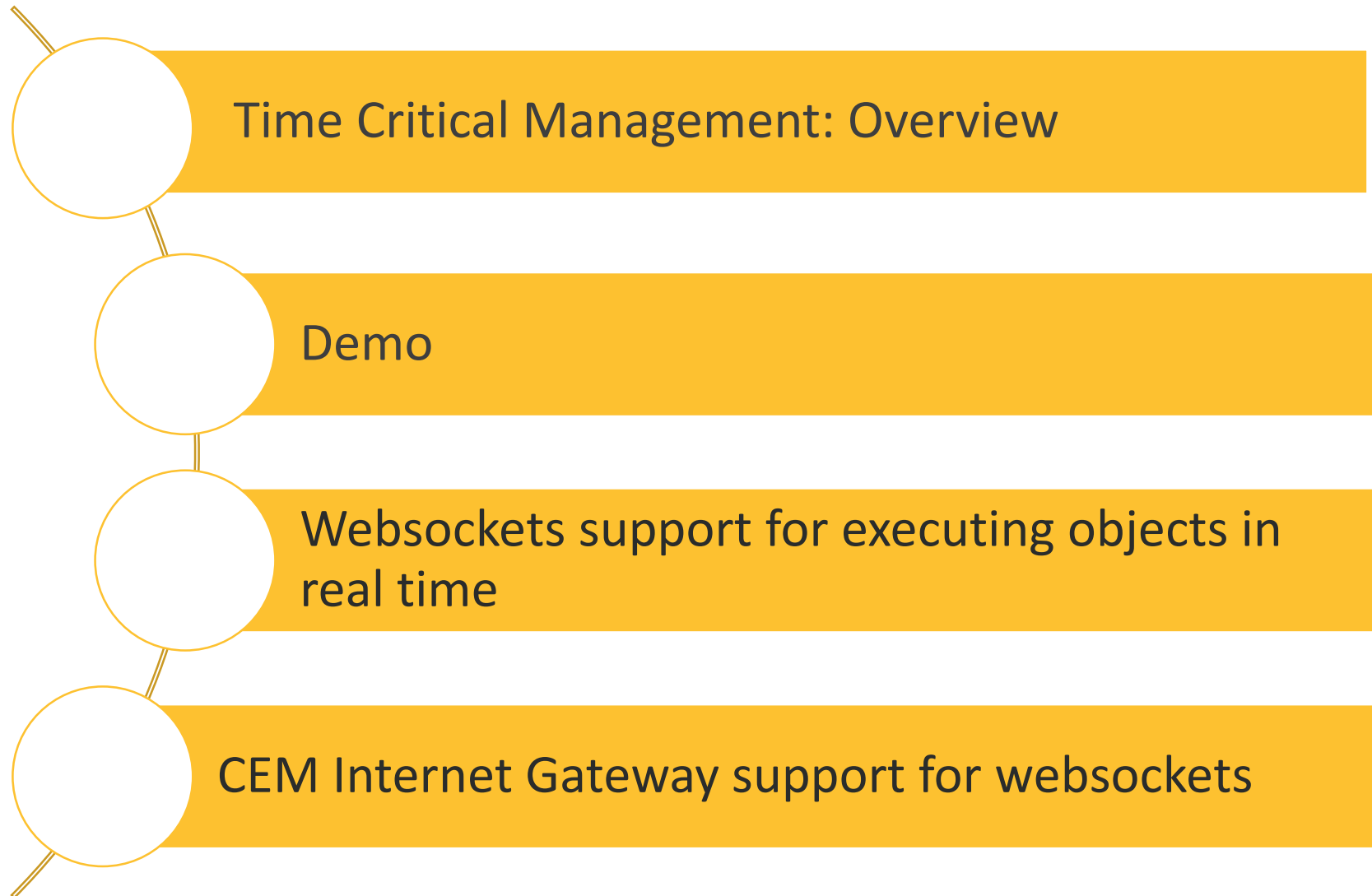
Rob Barker
Product Management

Date

October - 2018

✔ Symantec.

Agenda

Time Critical Management: Overview

Demo

Websockets support for executing objects in real time

CEM Internet Gateway support for websockets
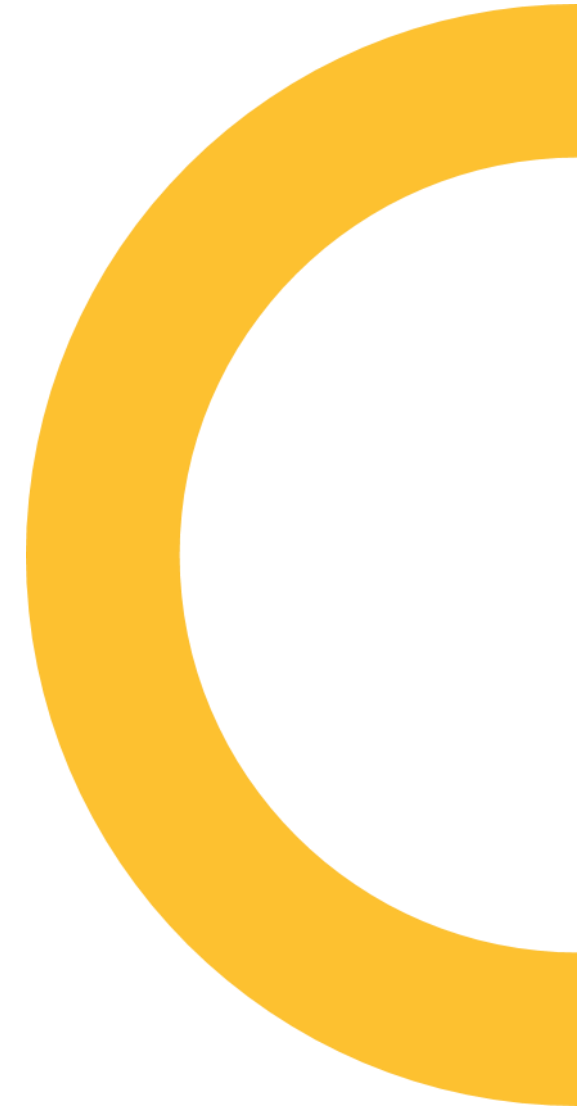
On Demand Management

NEED

"As an administrator, I need the ability to collect information on my endpoints in real time so that I can respond to situations using up to date information."

CHALLENGES

- Moderate latency with current architecture
- Endpoints must check in to receive updates
- Task Server is not CEM "aware"
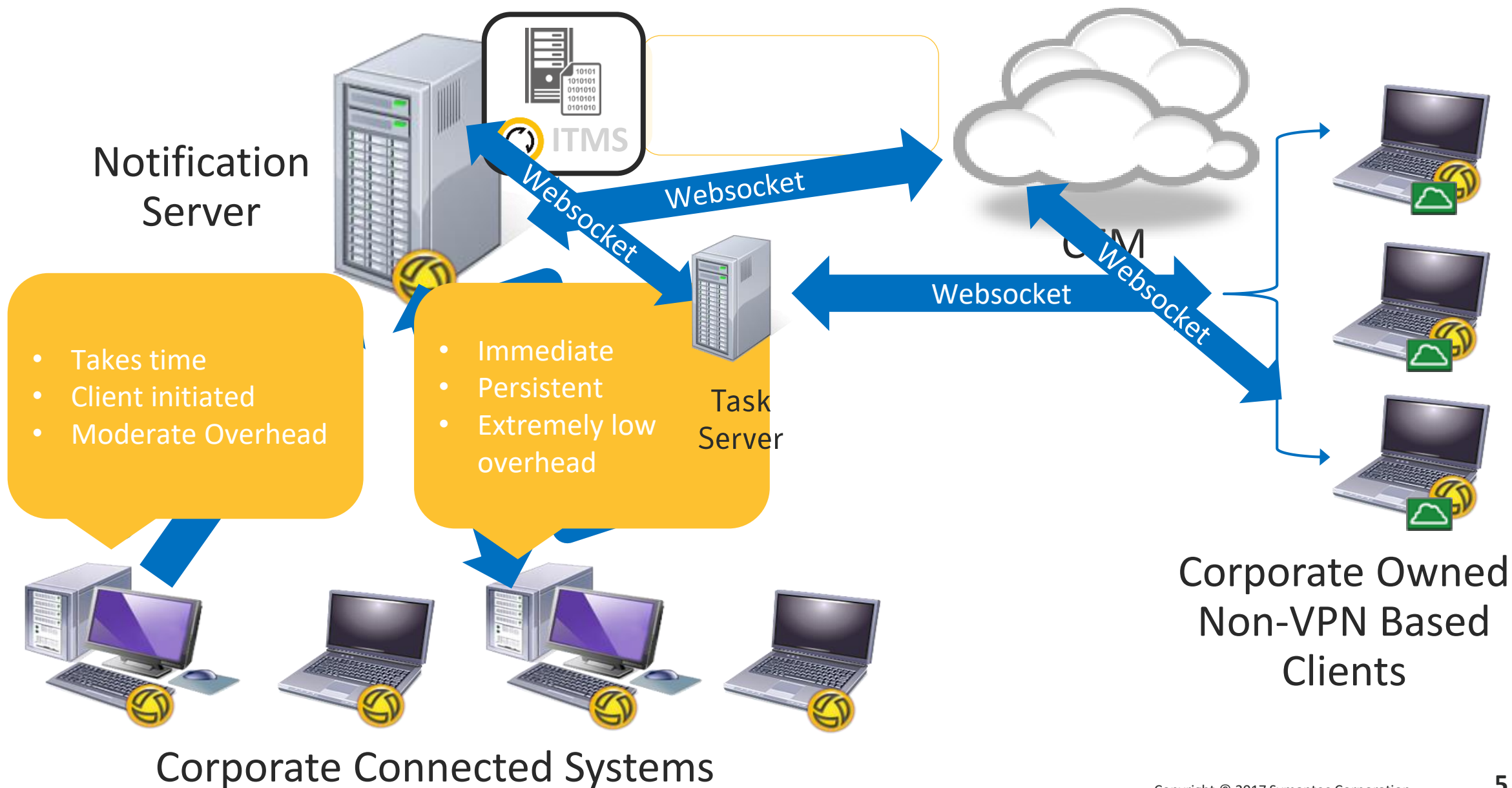- Task Services are not persistent connections

FEATURE

Time Critical Management – On Demand Inventory

CAPABILITIES

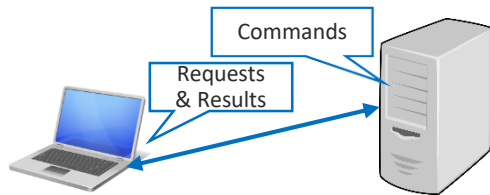Provide administrators with the ability to execute actions on demand

ITMS Architecture

Demo

Existing Challenges in communication layer

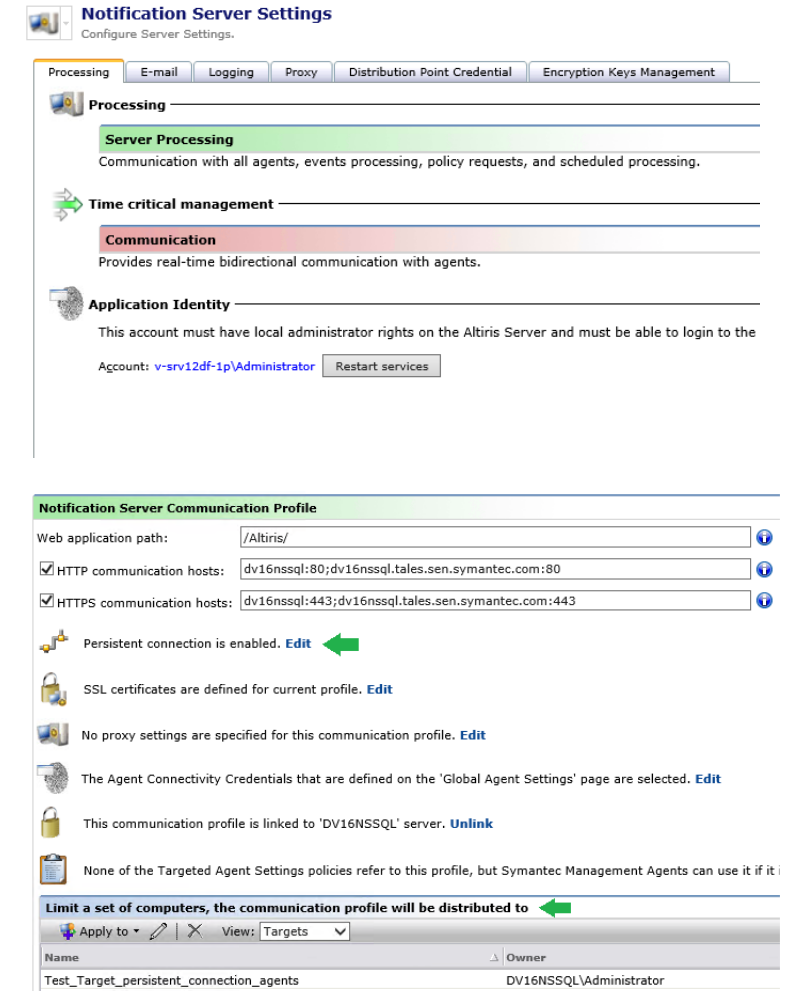|	
Chatty Client	ICMP pings to ensure connectivity
	Multiple HTTP(S) request/response for management traffic*
	Overhead on Network and Management Server
Limitations to Infrastructure from Task Management	Requires customer ports to notify (tickle) endpoint about urgent task
	Push management actions are NOT supported for CEM (only pull)
Latency of Management Actions	Due to scheduled check to request for policies from Management server
	Task Management when servicing CEM endpoints or tickle ports are closed

*   For example, request and receive policy, send inventory, send patch assessment scan output, send task execution results, etc., but DOESN'T include content and package delivery.

Websockets support for executing objects in real time

Server side changes

- New Websocket server:
    - manages persistent connections from clients
    - embedded into AexSvc and independent from IIS
    - running on same HTTPS port and uses existing SSL certificate
    - supported on Windows Server 2012 R2 and Windows Server 2016
    - supports new actions like PushPolicy, PushTask, to speedup task and policy delivery
    - actions execution and processing is available from all Altiris services
- Setting to enable TCM communication (disabled by default)
- Added targeting mechanism for connection profiles
- Added ability to create agent installation package from connection profile

Websockets support for executing objects in real time

Agent side changes

- New Websocket client transport:
  - Used for persistent connections from client
  - Embedded into AeXNetComms.dll and exposed via COM API
  - Supported on Windows 7 and above
- Software Portal proxy is modified
  - Still used for routing Software Portal traffic through CEM gateway
  - Used to route WebSocket connections to servers requiring SSL
  - Used to route WebSocket SSL connections through CEM gateway
  - Will be used to route WebSocket connections through proxy servers
- Core Agent:
  - Establishes and maintain persistent connection to SMP Server
  - Routes all core agent HTTP requests through SMP persistent connection
  - Able to receive data or actions from SMP server
  - Provides fallback mechanism to pure HTTP connectivity

Network Status	
Notification Server:	Available via internet gateway Cryptographic protocol: TLS 1.0 Cipher suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 View Notification Server certificate
CEM Mode:	Cloud-enabled Management mode is active Cryptographic protocol: TLS 1.0 Cipher suite: TLS_RSA_WITH_AES_128_CBC_SHA View internet gateway certificate
Server Connection:	Persistent Sent: 28.90 KB Received: 0.78 KB Terminate persistent connection	**NEW**
Peer Downloading:	Disabled
Network Usage:	Unrestricted

- Client Task Agent changes:
  - Establishes and maintain persistent connection to Task Server
  - Routes all CTA HTTP requests through the SMP persistent connection and TS persistent connection.
  - Able to receive data or actions from SMP or TS servers
  - Provides fallback mechanism to pure HTTP connectivity

CEM Internet Gateway support for websockets

New Internet Gateway introduced

- o Replaces existing IG
  - o Hence removes dependency on Apache HTTP Server and OpenSSL – less maintenance efforts on security updates for IG
  - o In-place upgrade with complete settings migration
- o OS support
  - o Windows Server 2008R2, 2012R2 and 2016 (including Core Edition)
  - o Further support is possible for Linux (i.e. CentOS) via cross platform .net framework
- o Implemented based on open source cross-platform .NET Core 2.0 stack
- o Supports websockets
- o Improved Management UI
- o Extended functionality
  - o Reporting to several notification servers
  - o Performance counters
- o Scalability increase in few times
  - o Exact numbers are TBD pending full scalability testing. Target is to support not less then 15-20K per IG. Existing IG supports only 3K