TRIGGER it®

Introduction

Challenges

MONITOR / AUDIT

- Endpoints outside corporate network
- Applications behavior and network traffic correlation

MANAGE & CONTROL

- Multiple and complex tools with internal systems dependency
- Devices’ configuration for remote users

PROTECT

- Mitigate security threats on the spot (Zero Day Attack)
- Enforce information protection for remote users

VISIBILITY & TROUBLESHOOTING

- Deep visibility and network devices insights
- Troubleshooting by guessing

INVESTMENT

- Pay a Fortune or lose control

What is TRIGGERit

Converged Endpoints Controller

Visibility

Provides insights about performances, errors, issues and digital footprint

Correlation

Understand why certain events have happened and when changes have occurred

Actions

Take update/remediation or fix actions

Prevent

Create policies and settings to prevent threats/issues/events from happening

Works on

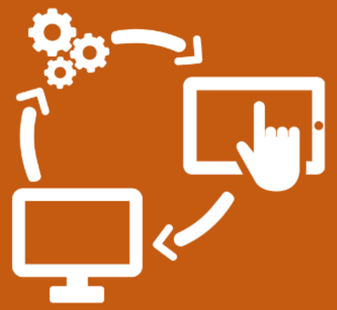




MDM in Trigger-it

- Mobiles are first class citizen in Trigger-it, Mobile agent supports Android 5+ and IOS(Beta).
- Supports BYOD, COPE and Kiosk modes.
- Supports Android for work profiles, Enterprise application store, QR/NFC provisioning and system application via OEM images.
- Supports remote sessions, compliance policy, location tracking, geo fencing and much more…
- Single console to manage all your devices.

Benefits of TRIGGERit



Control, monitor, & protect endpoints

Reduce attack surface & mitigate security threats on spot

Better operational insights for better service

Reduce cost by monitoring & controlling all printing activities

One console does it all with no need for multiple tools and vendors

Why TRIGGERit

1

WORKS EVERYWHERE

Works with any client like POS/ATM machines, remote branch offices, and roaming users like remote workers, regular travelers,…. And support workgroup machines

2

SINGLE APPLICATION DOES IT ALL

No need to purchase multiple applications and deploy multiple agents

3

MINIMAL PRE-REQUISITES

Simple server side installation and deployment time within 4 hours

4

DELIVERY & VENDOR SUPPORT

Local presence with local hotline, web based and email supports that enable rapid and responsive support.

5

FULL MONITORING & AUDIT

Monitor applications behavior, network devices, endpoints network traffic, print jobs, printers , and machine performance

6

INVESTMENT & ROI

Reduce integration and operational cost by replacing multiple applications with only one application doing it all, and giving the ability to monitor your licenses

3rd parties with TRIGGER it

splunk> Radar

ArcSight An HP Company

Microsoft System Center Service Manager

bmc servicenow

tenable

KASPERSKY lab

CROWDSTRIKE

Symantec

Integration

Integrate using Trigger-it syslog forwarder to forward events to any SIEM solution

Integrate using Trigger-it Workflows with more than 100+ adapters to send/receive data from any system

Collect events from application logs and display them centrally in Trigger-it console or forward them to any other system

TRIGGER it

Competitive Edge

Feature	Available Market Products			TRIGGERit
Control machines inside and outside the corporate network	Intune BIGFIX	Microsoft System Center Configuration Manager		
Monitor machines' inside and outside the corporate network	nexthink change your perspective McAfee	BIGFIX	with limitations	
Protect machines inside and outside the corporate network (web / network protection and application filtering)	eset McAfee	Symantec TREND MICRO	with limitations	
Monitoring network devices	solarwinds			

Supportability

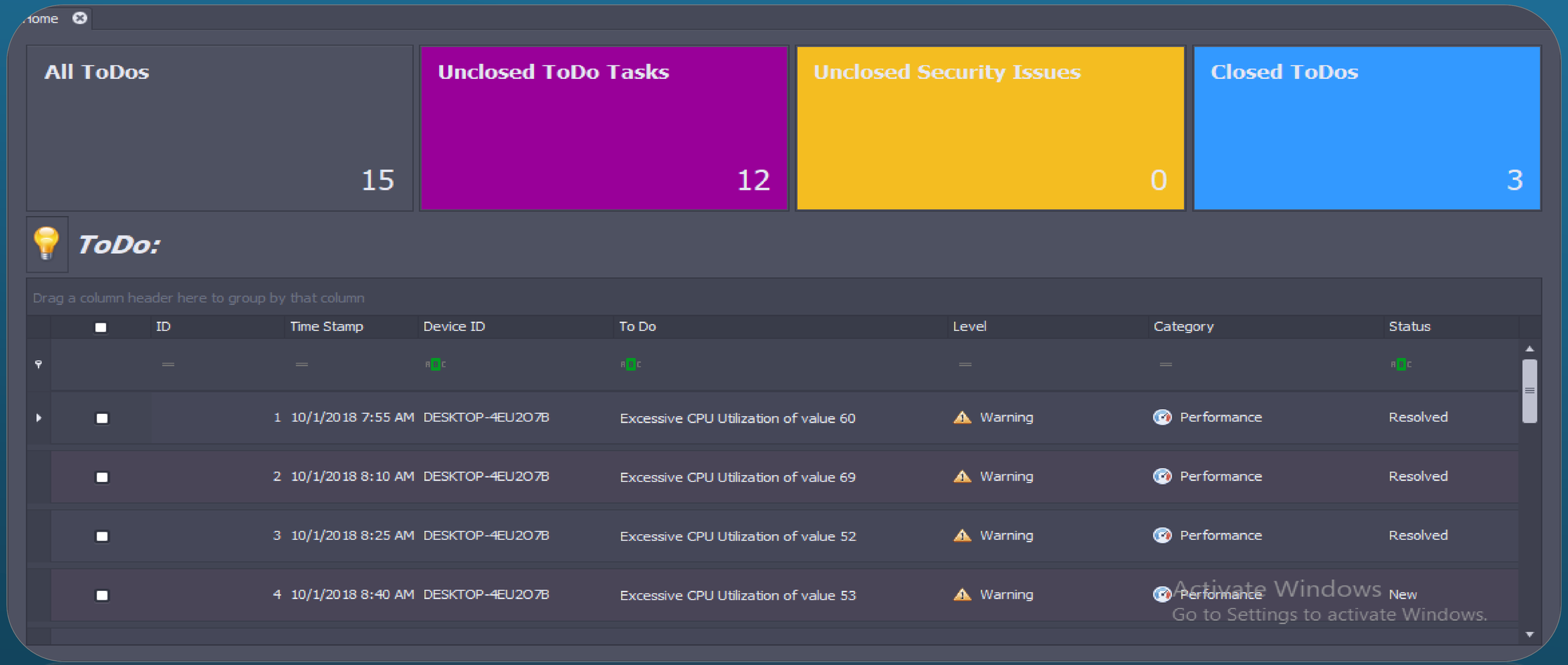
Machine Type	Supported Platform
Endpoints	Windows 7, Windows 8, Windows 8.1, Windows 10, Android
Servers	Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows Server 2019, redhat, Linux Mint (from freedom came elegance), SUSE, ubuntu
Network devices	f5, paloalto NETWORKS, CISCO, FORCEPOINT (POWERED BY Raytheon)

TRIGGERit®

Key Features

Proactive To-Do

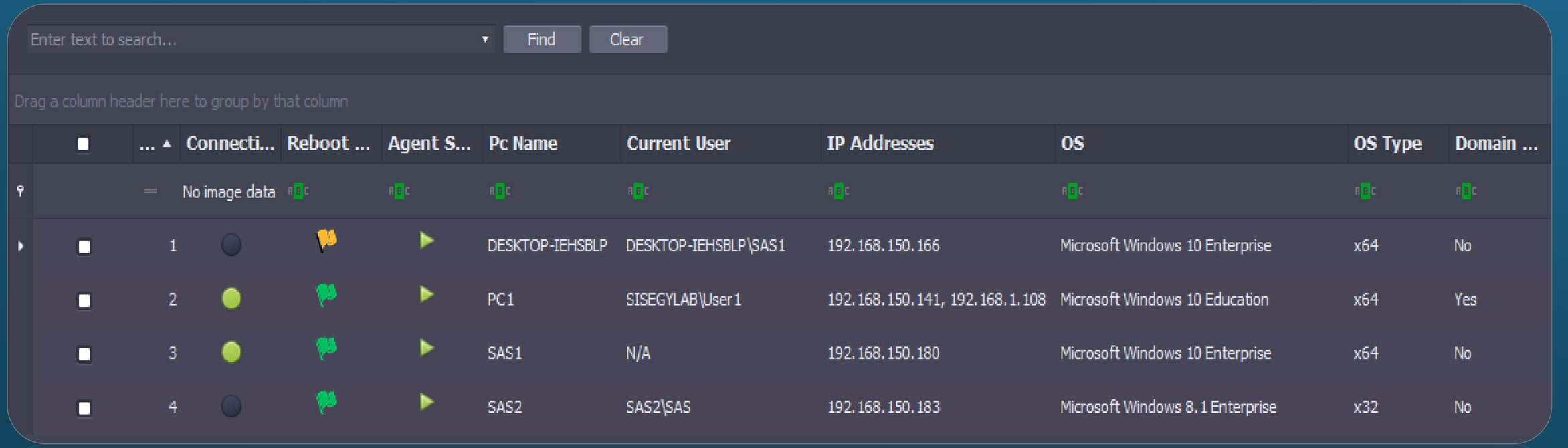
Interactive To-Do based on agents' insights



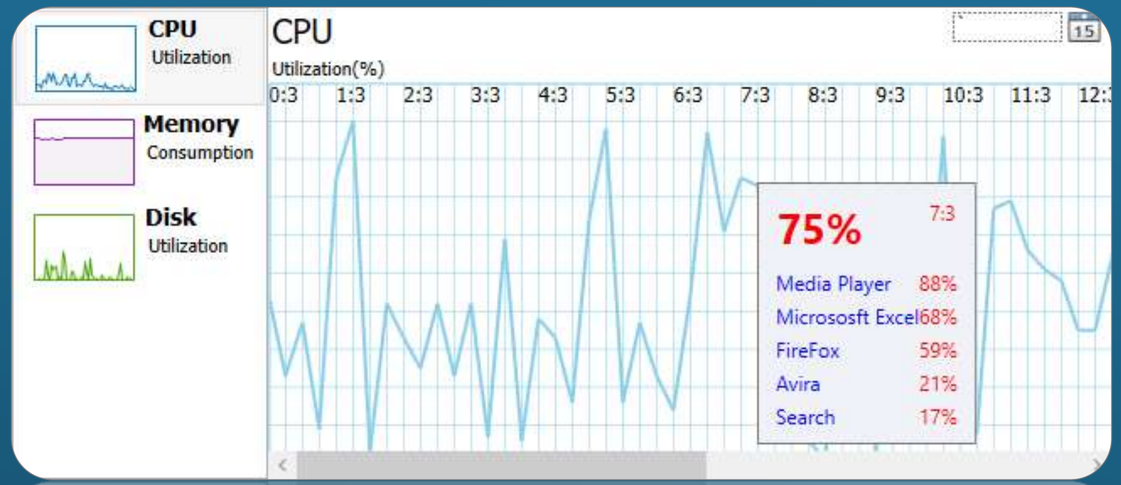
Machine Insights

Extract machine information like:

- Machine name
- Machine IP addresses
- Machine up time
- Current user
- Last logged-in user
- Reboot required status

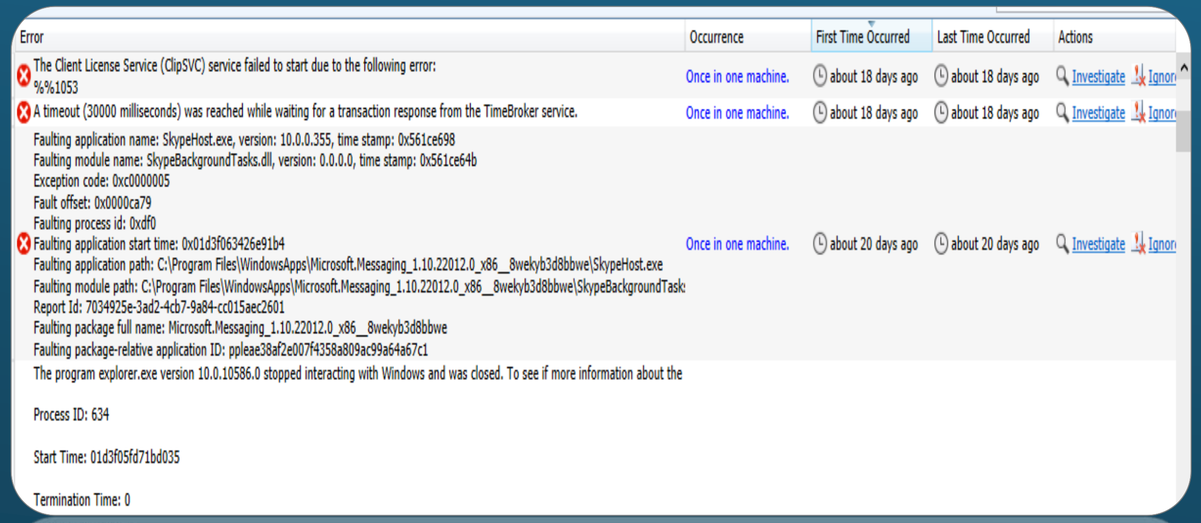


Machine Performance Analysis



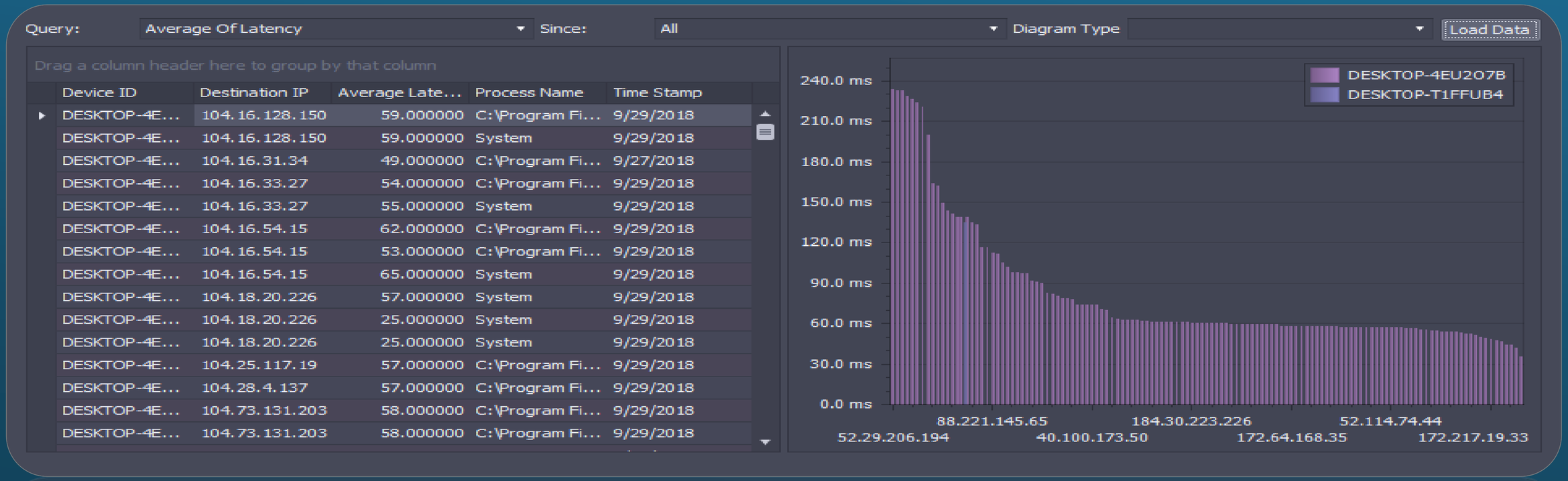
- Extract machine performance insights
- Identify overall performance
- Show top 5 applications utilizing CPU, memory, and disk

Track all application crash errors, and investigate changes that might have caused these crash errors across all affected machines



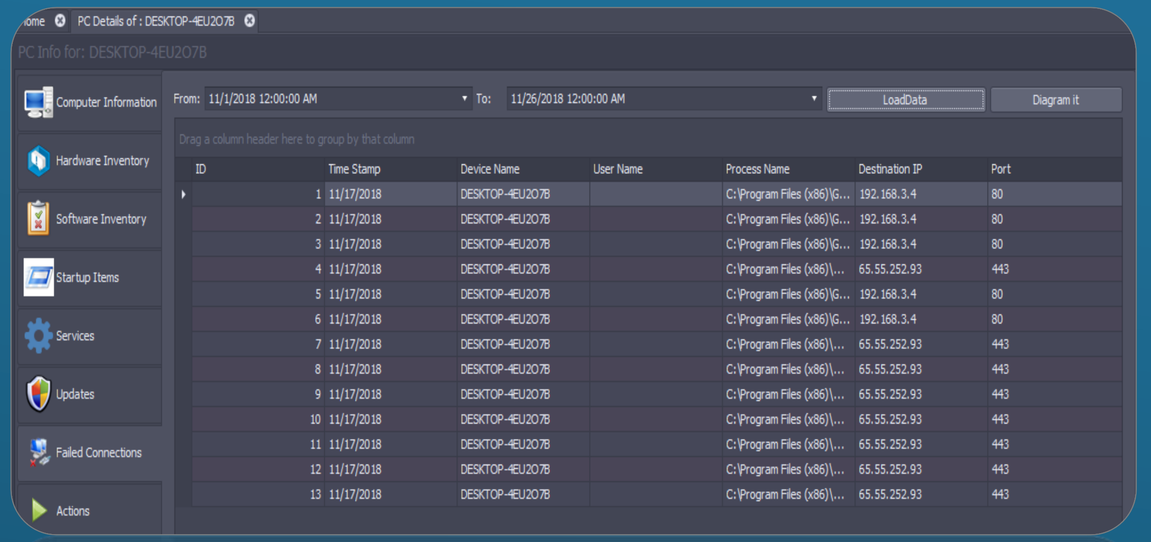
Network Traffic Insights

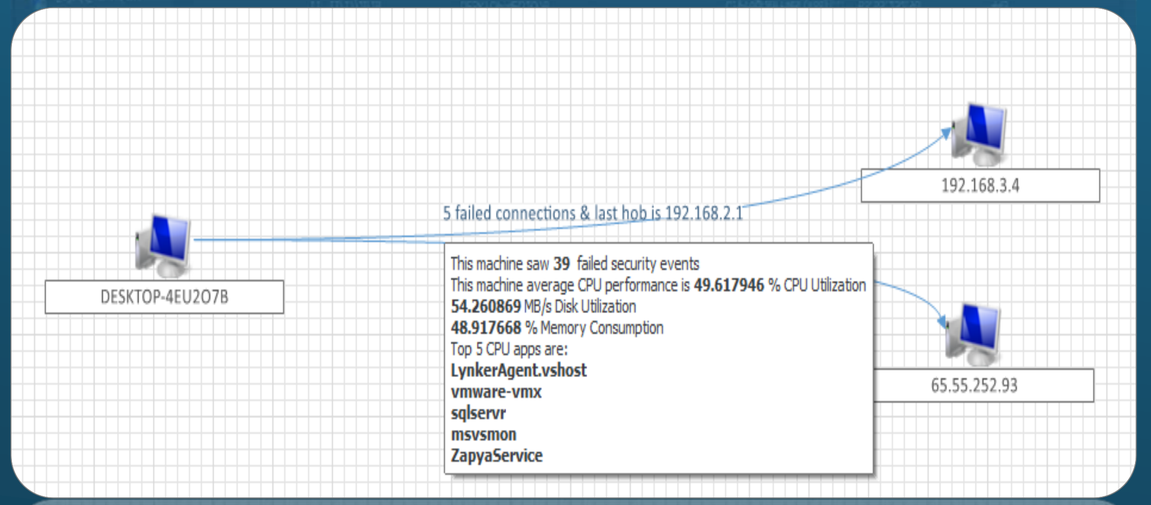
- Show network traffic in drill down way
- Sum of traffic and average of latency
- Applications' behavior over network



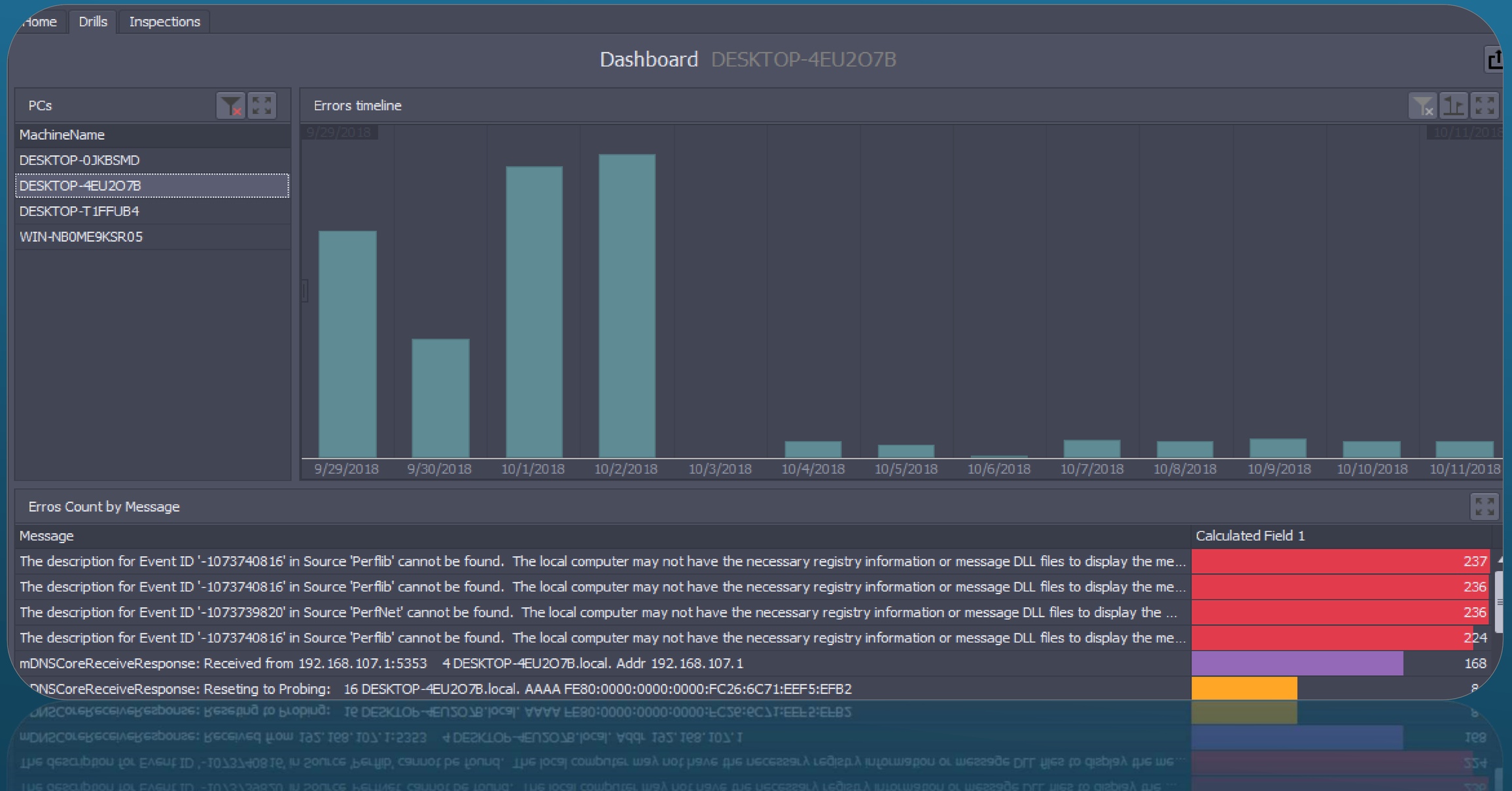
Failed Network Connections Tracking

- Find failed network connections
- Understand the failed connection reason with historical traceroute information
- Correlate failed connections with security events and performance data



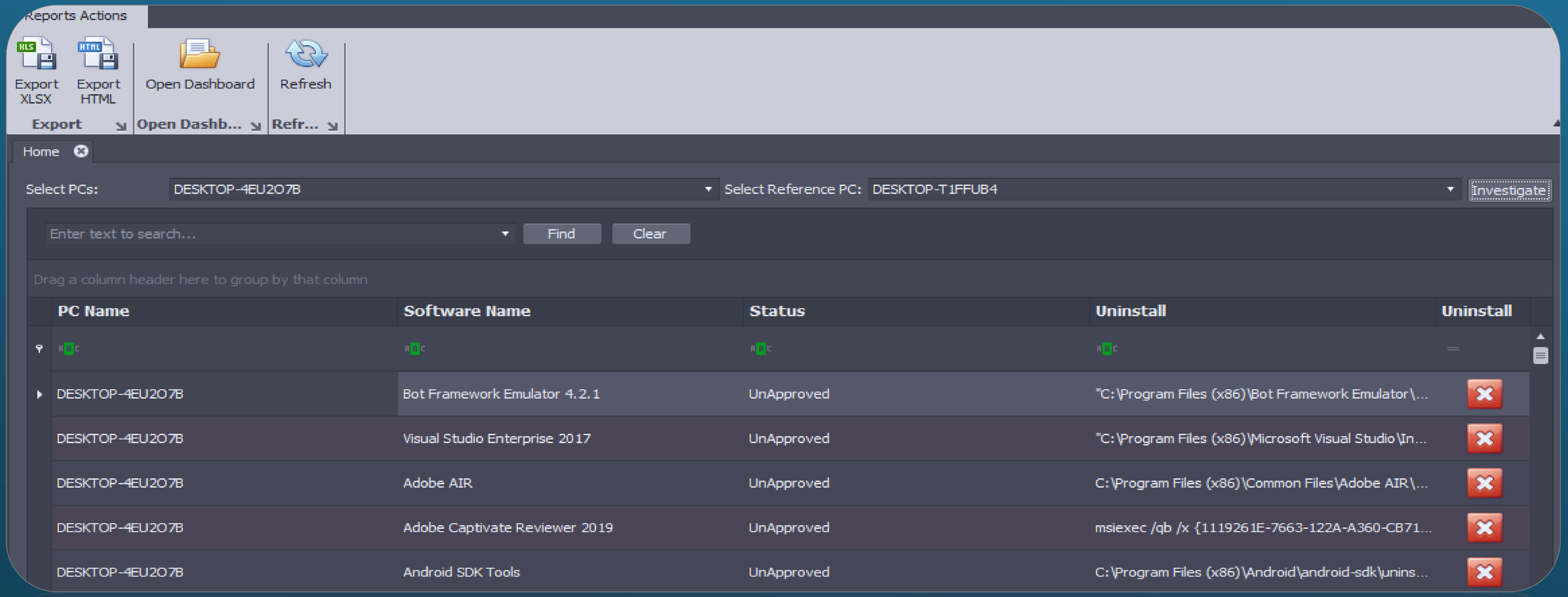


Endpoints Error Inspection



Software Compliance

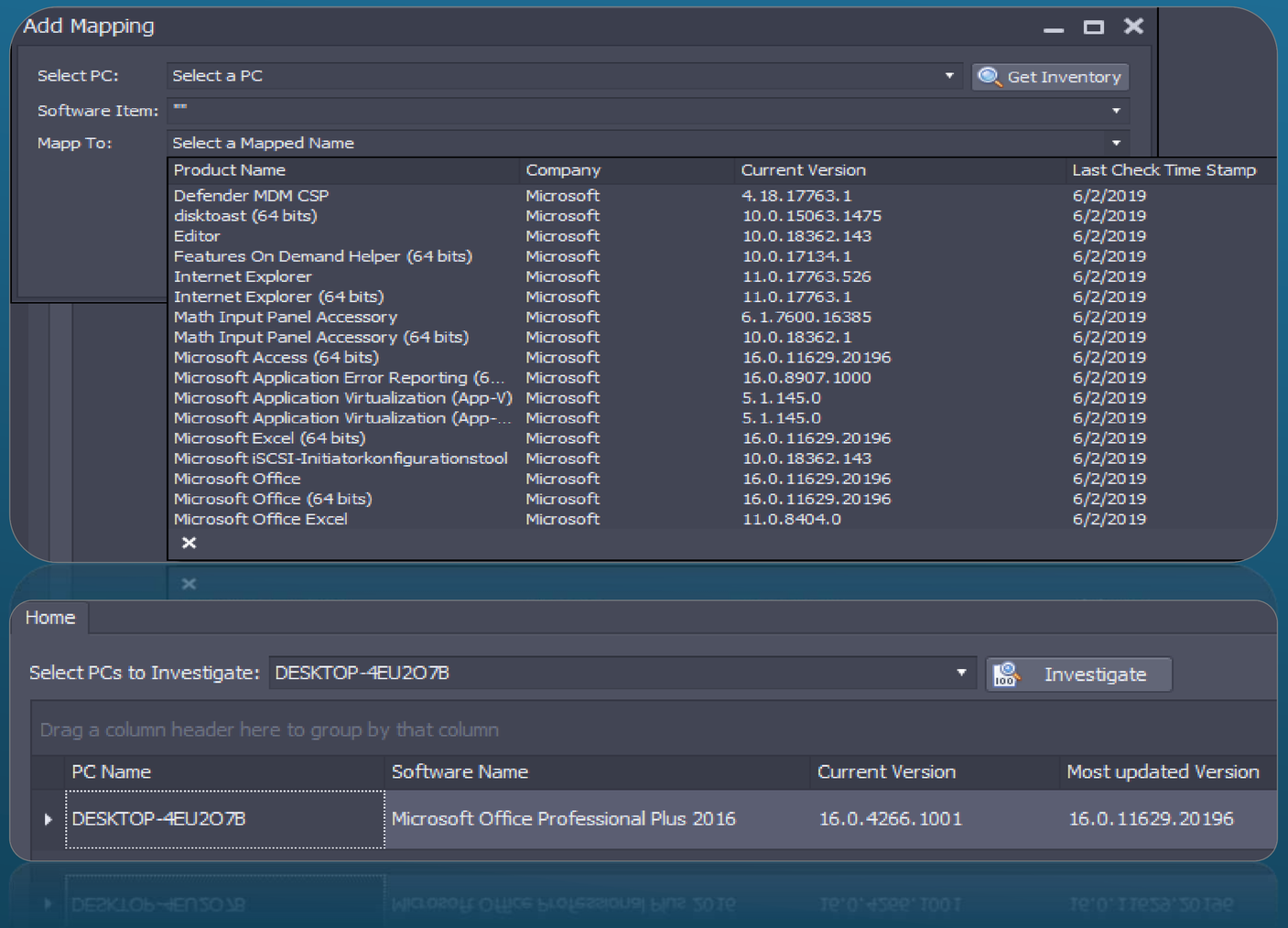
- Compare PCs for software compliance against a baseline PC
- Identify missing software and show any unapproved software



OS & 3rd Parties Patch Updates

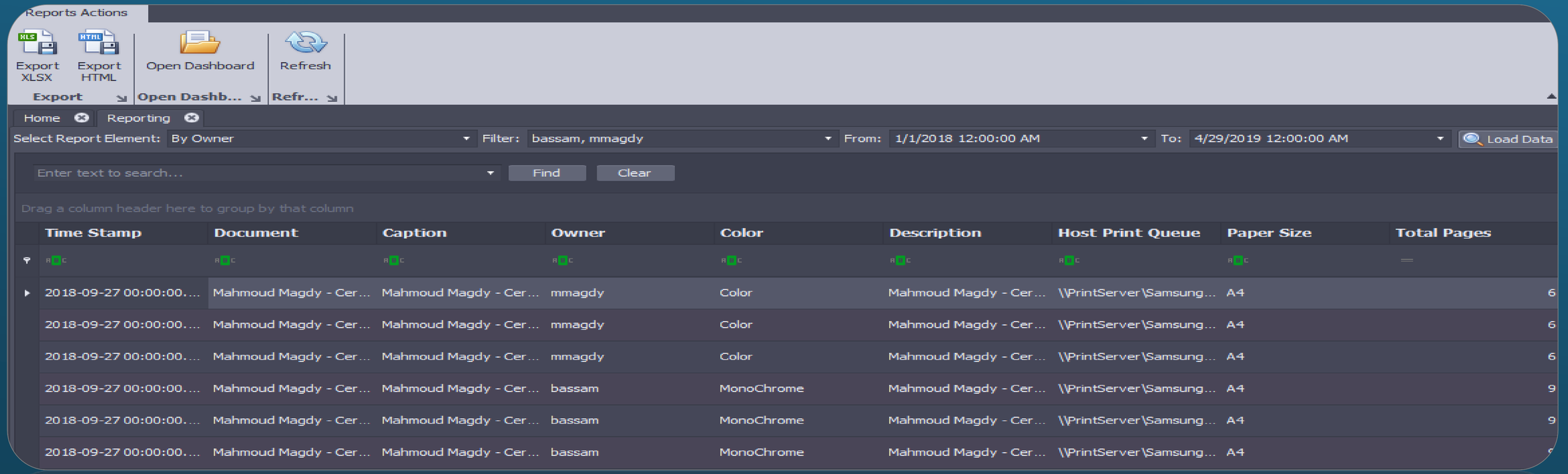
- Show OS updates
- Show 3rd parties patch compliance for the following vendors:

Adobe Systems
WinRAR
Apple Inc.
Ashampoo
Autodesk
AVAST Software
Cyberlink
Dell
ESET
Foxit Software
Google Inc.
Hewlett-Packard
7Zip
Intel
Kaspersky Lab
McAfee, Inc.
Microsoft
Mozilla Foundation
Oracle
SAP SE
TOSHIBA
Trend Micro Inc.
Winzip Computing



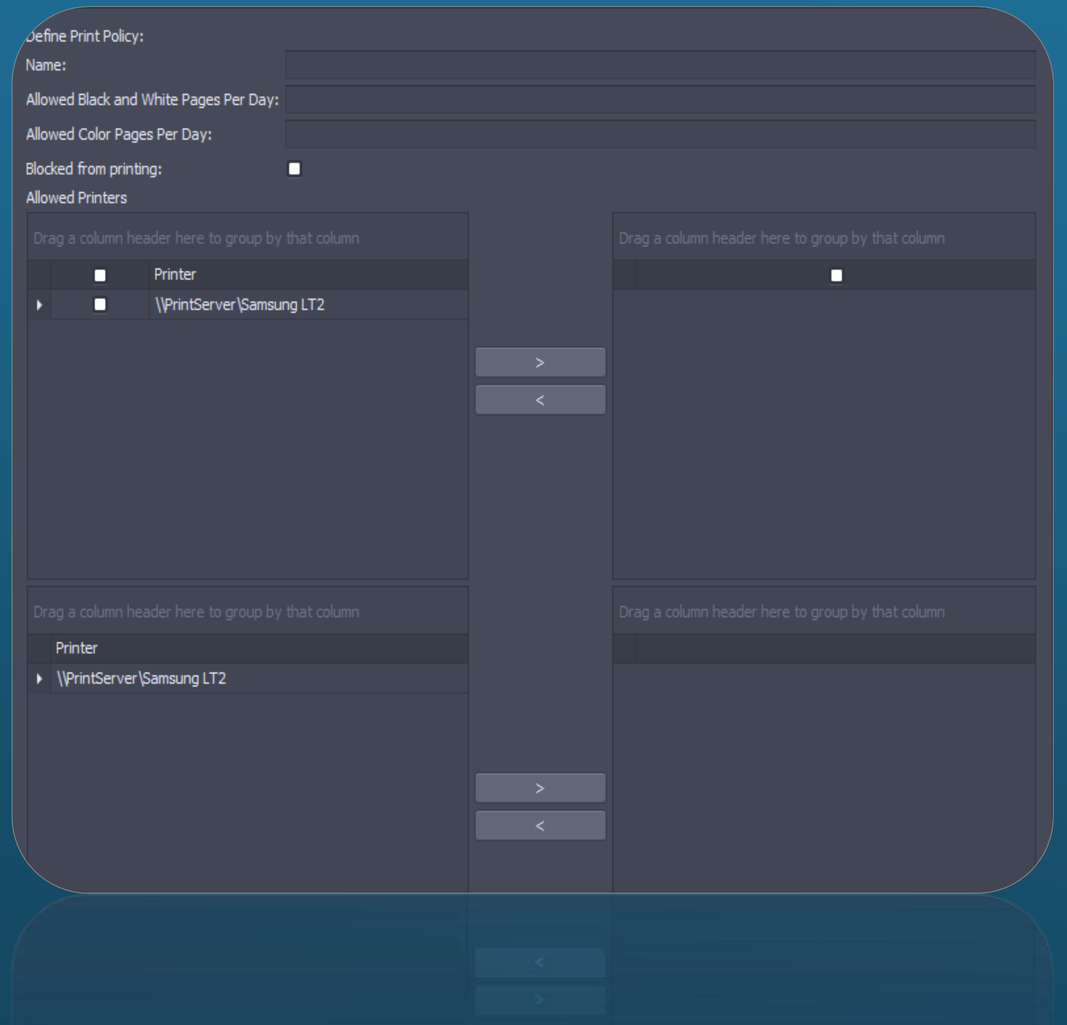
Print Monitor

- Track all print jobs for auditing and cost analysis
- Monitor network & non-network printers usage
- Full information on printed jobs like paper document name, owner, number of printed pages, black or colored, …..)



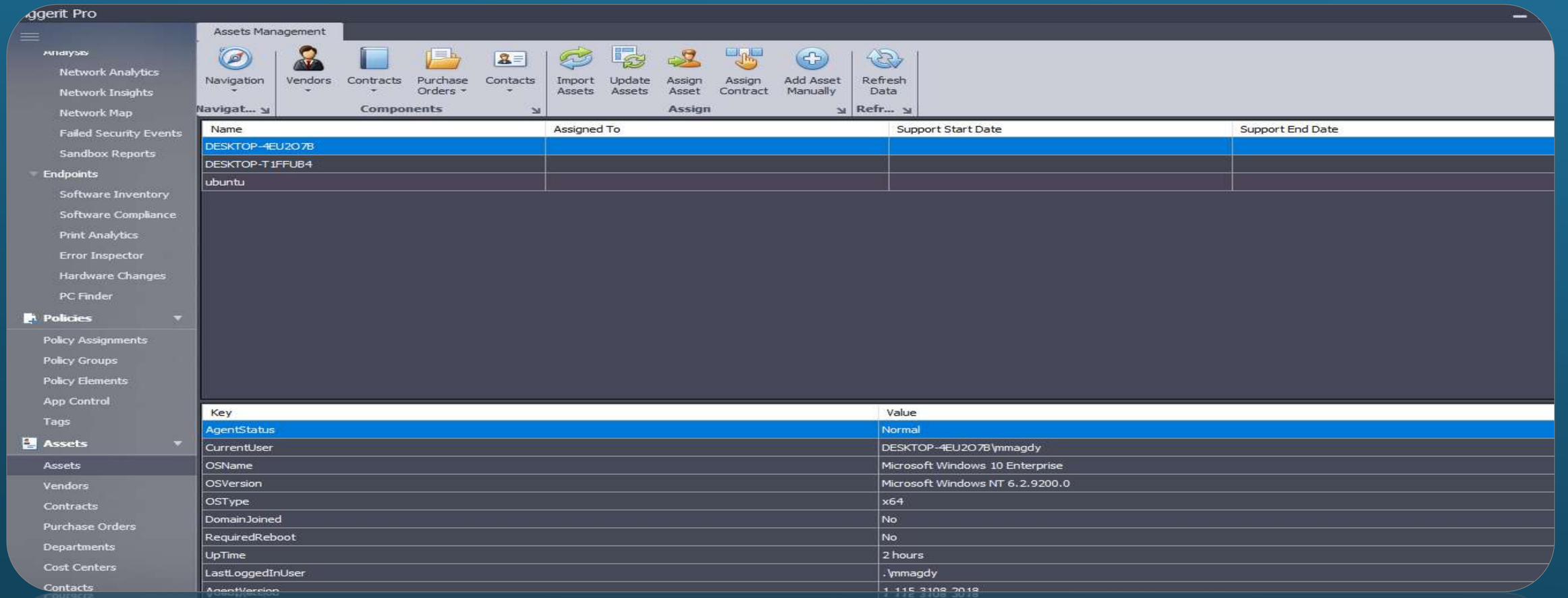
Print Control

- Limit No. of black and color pages printed per day
- Block users from printing entirely
- Define printers white and black lists



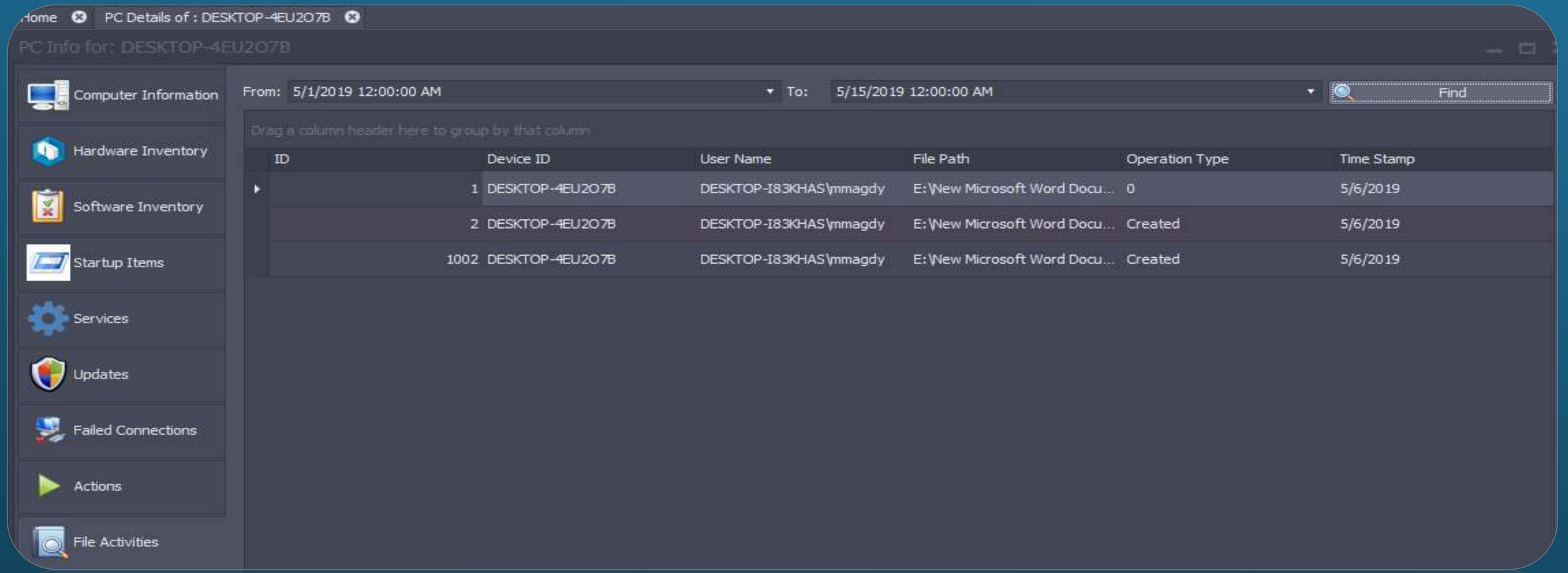
Digital Assets Management

- Tracking digital assets, contracts, vendors and SLA through a single interface
- Assigning digital assets to users, departments, or cost centers



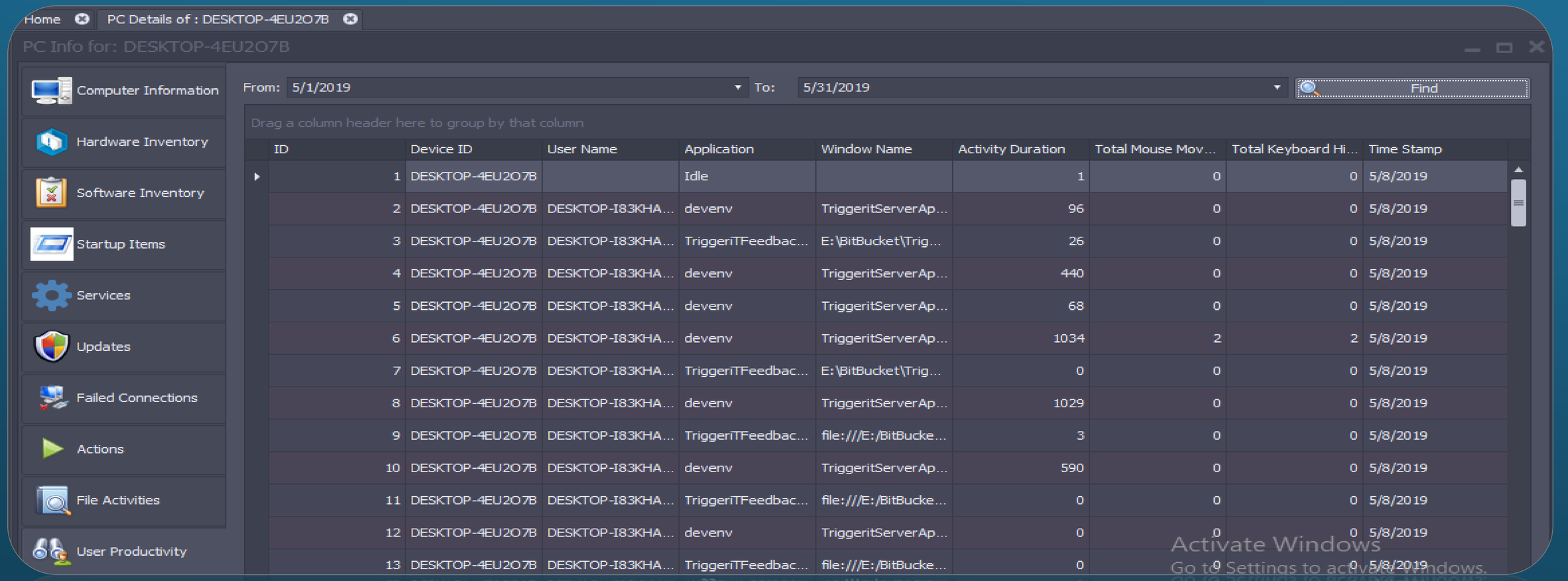
File Operations Tracking

- File operations (Creation, Rename, Change, Deletion)
- Useful for illegal file access, malicious activities and file changes



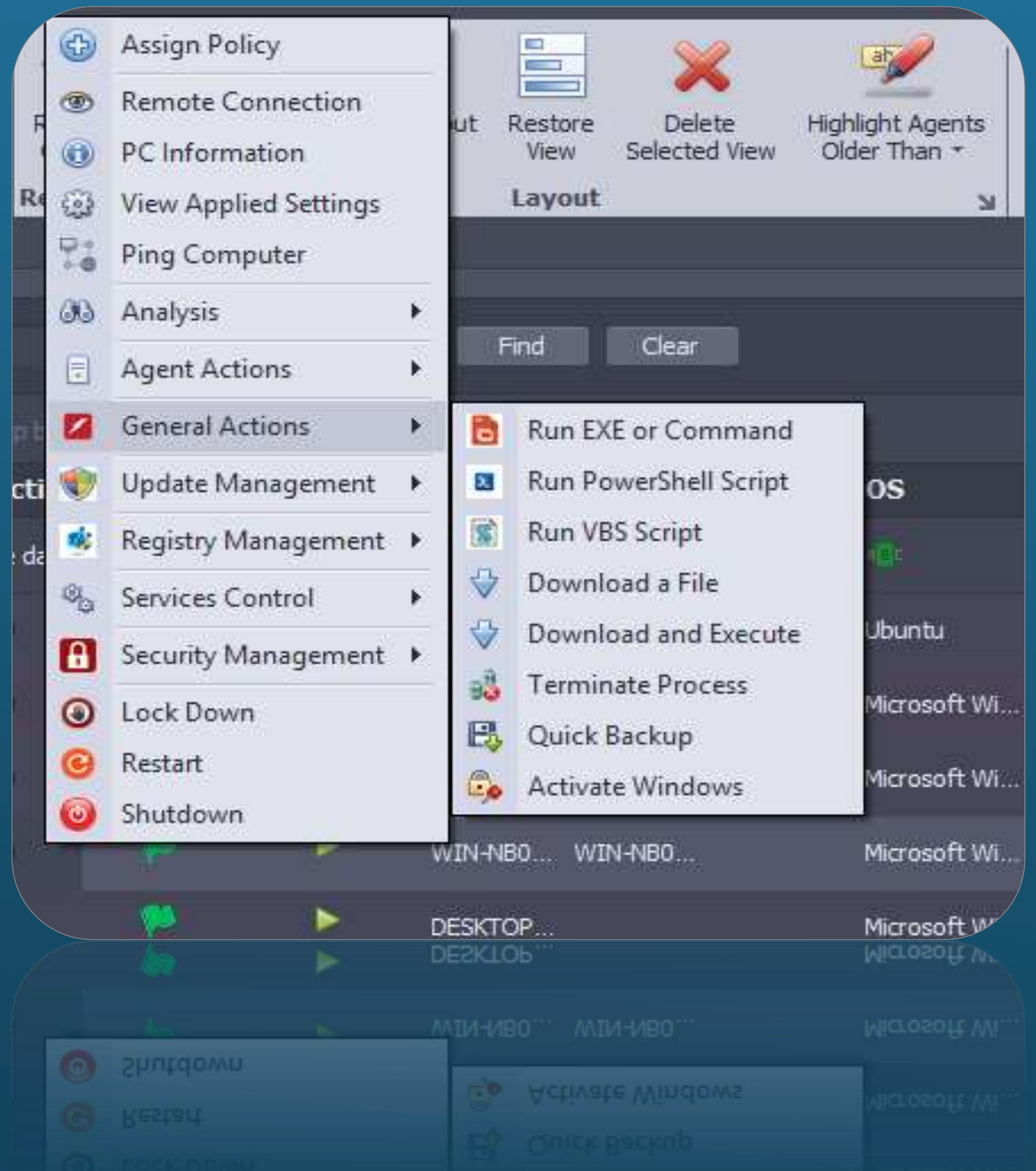
User Behavior Analysis

- Actual application usage time by user
- User behavior for a specific app including mouse moves and keyboard hits



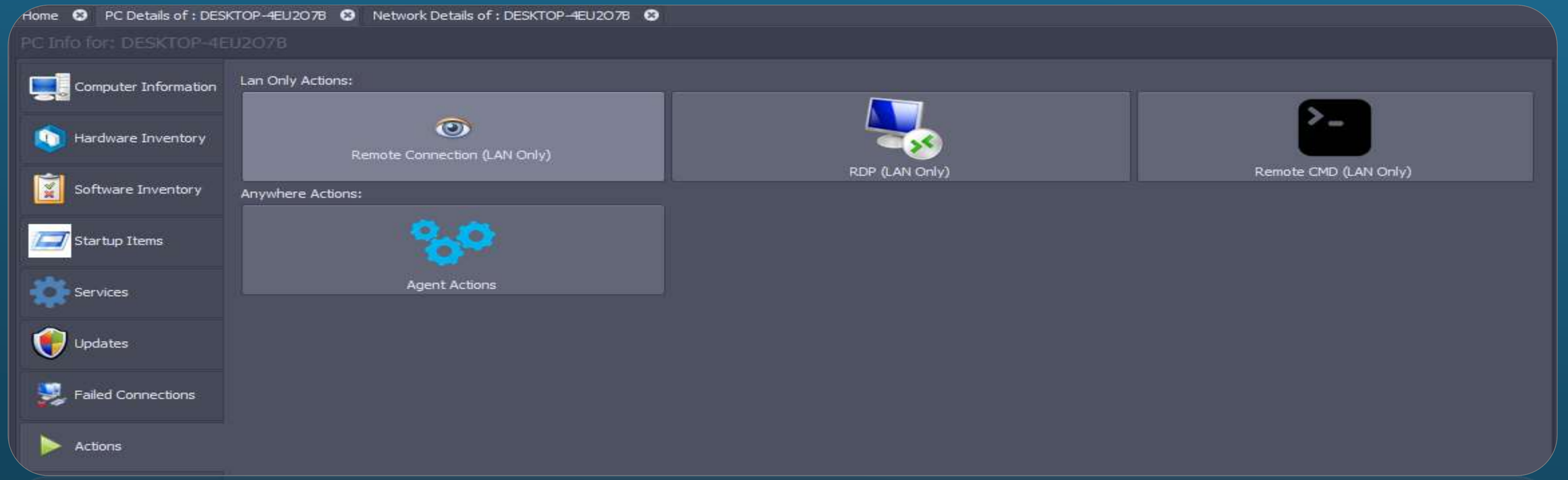
Taking Action

- Wide range of actions
- No scripting or 3rd party solutions required
- No service account needed
- All the execution features could be applied to LAN / WAN / Internet clients – No special configuration required



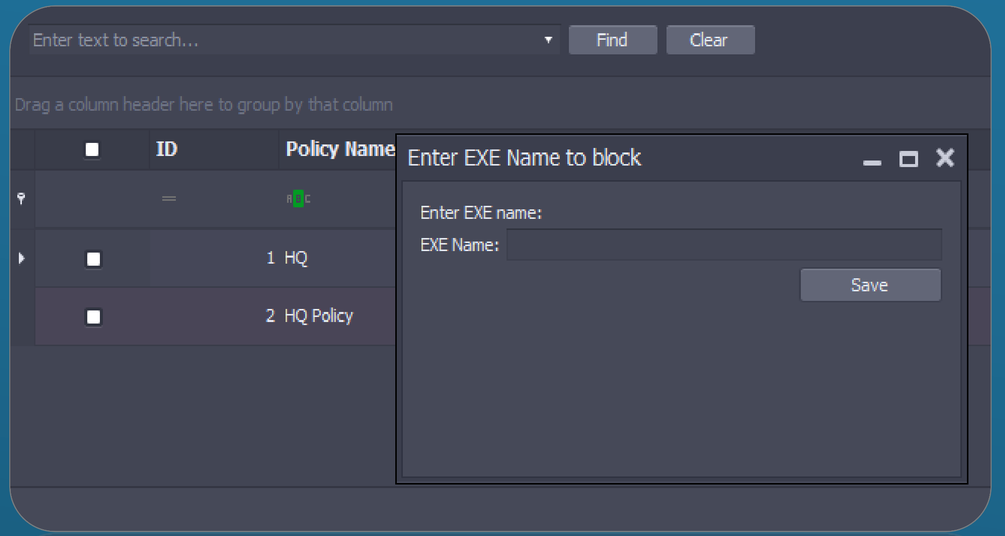
Built-in Remote Tools

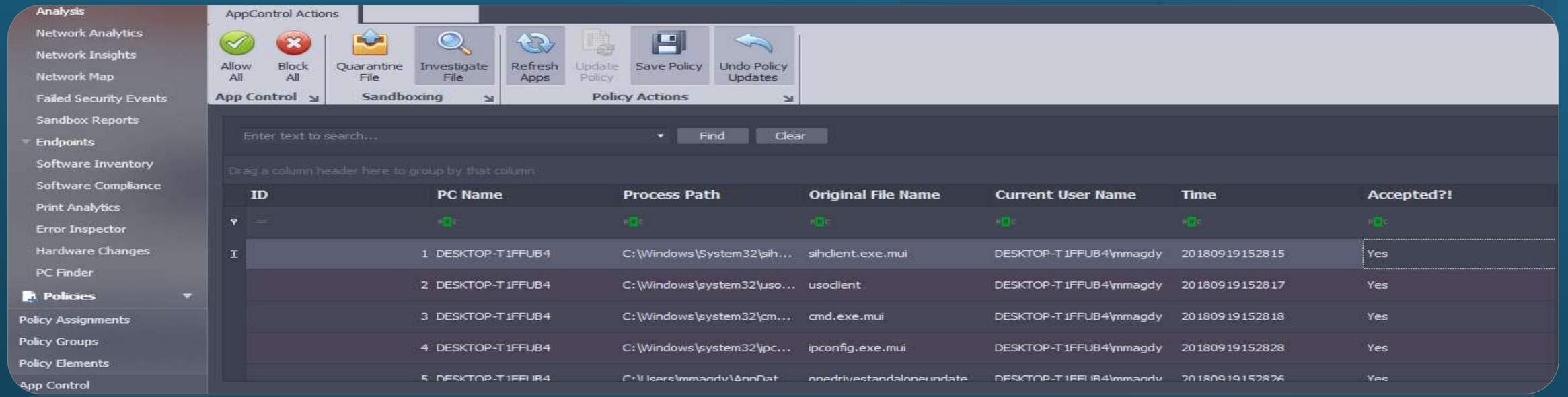
- Trigger-it has its own remote connection tool
- No need for DNS or internet connectivity for remote support within your corporate network
- Remote desktop, remote CMD, and built-in agent actions



Executables Blocking

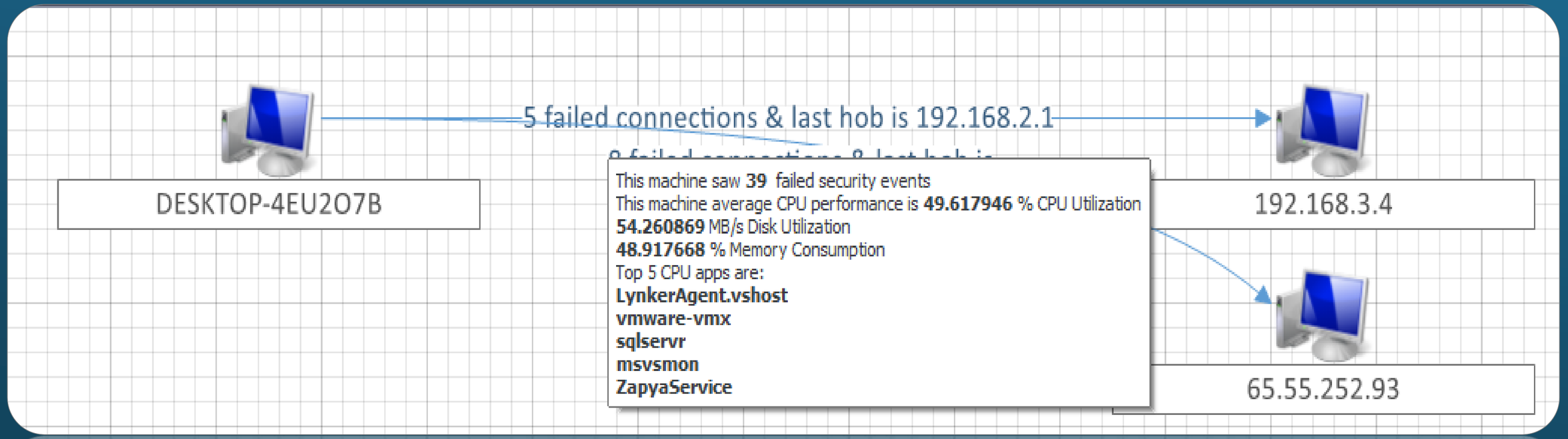
- Block unwanted and harmful executables even if they are renamed
- Process monitoring engine
- Black and white listing
- Integration with sandboxing technology to analyze unknown applications behavior when executed





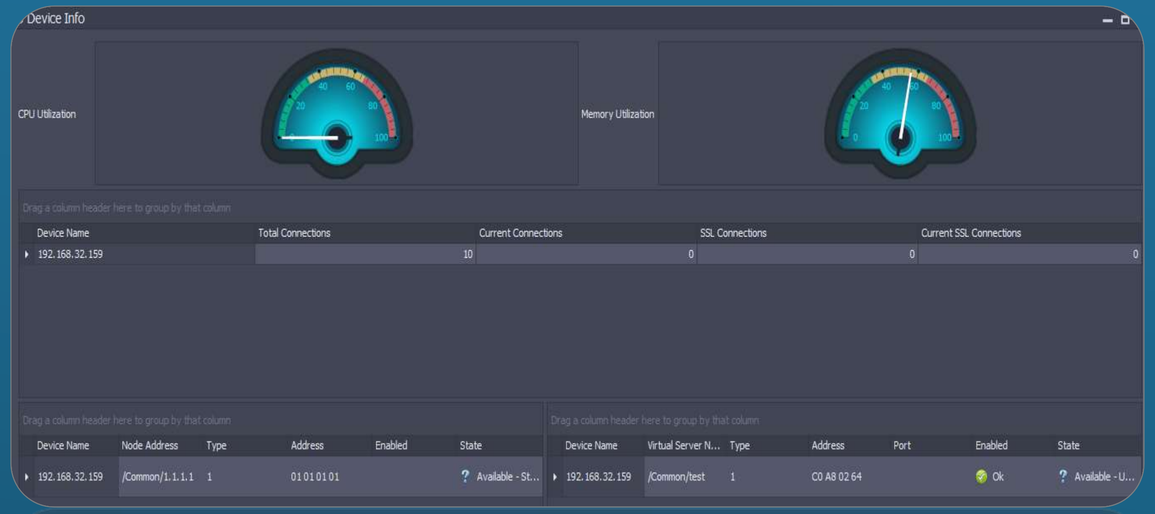
Network Traffic Control

- Drill down per site to show PCs and processes that generated the traffic
- Bandwidth reshaping per applications group
- Deep packet inspection for HTTP, HTTPs, SMTP and FTP



Network Devices Monitoring

- Real-time traffic and data analysis
- Neighbor and connected devices discovery
- SNMP traps lookups for events monitoring

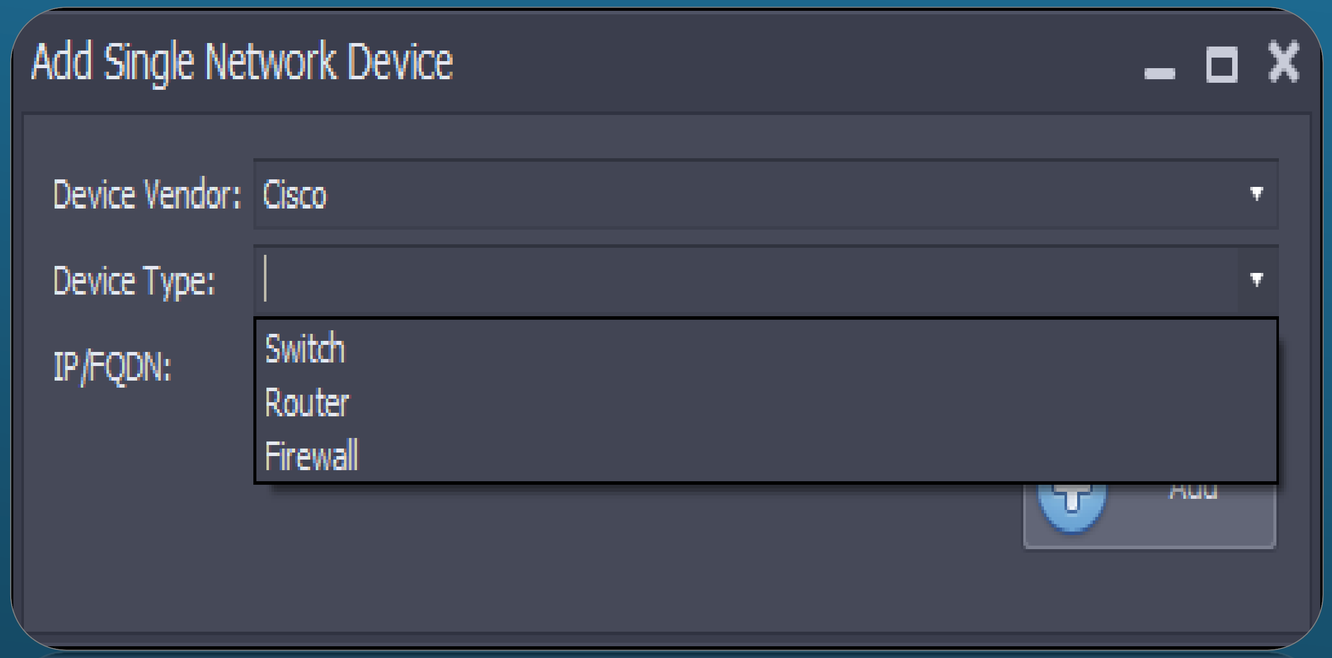


ID	Device IP	device Name	Device Vendor	Firmware Version	Device Type	Up Time	Last Update	Latitude	Longitude	Version
1	192.168.32.170		Cisco							
2	192.168.2.100		F5LTM							
3	192.168.32.159	f5.lab.com	F5	Linux f5.lab.com ...		0d 1h 1m 4s 100ms	3/4/2019		0	0	1

Network Devices Monitoring

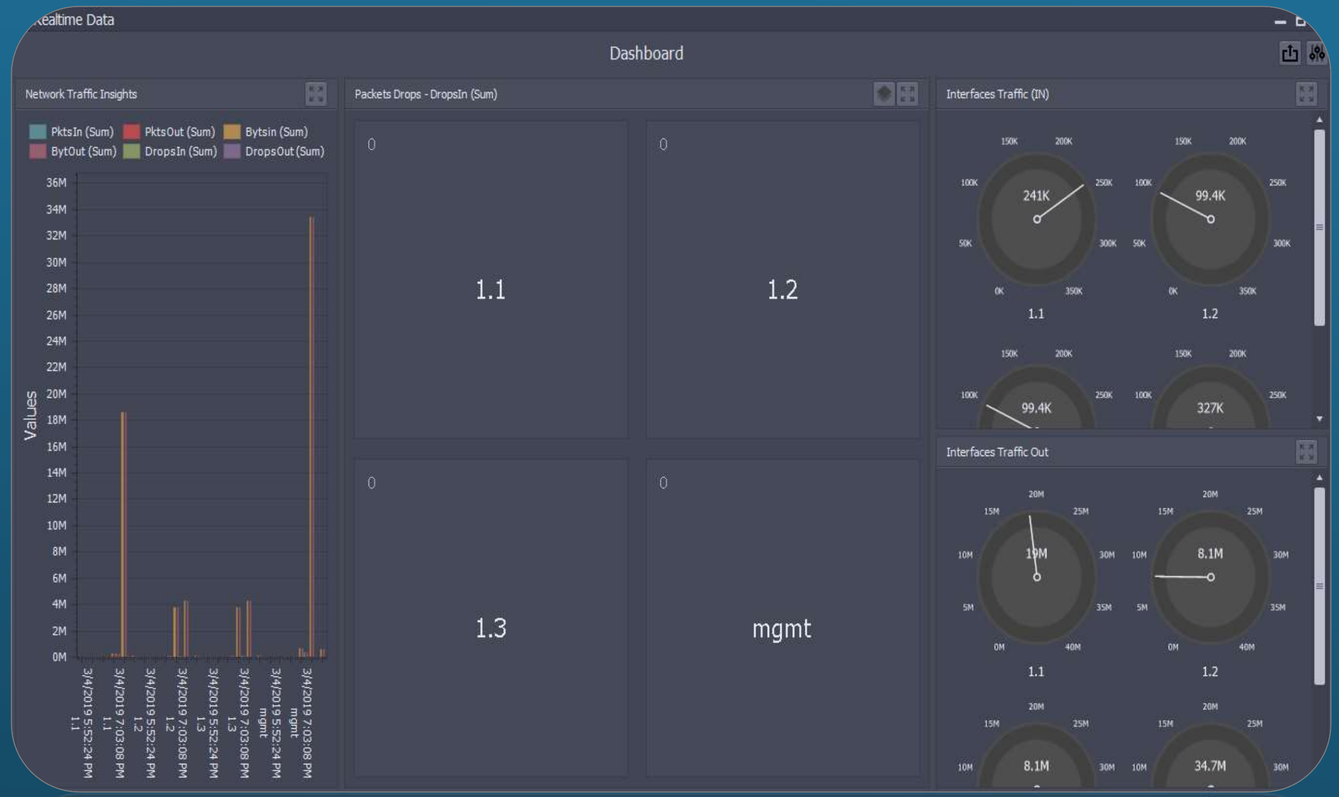
Supports wide range of network devices including:

- Cisco
- F5
- Force Point
- PaloAlto

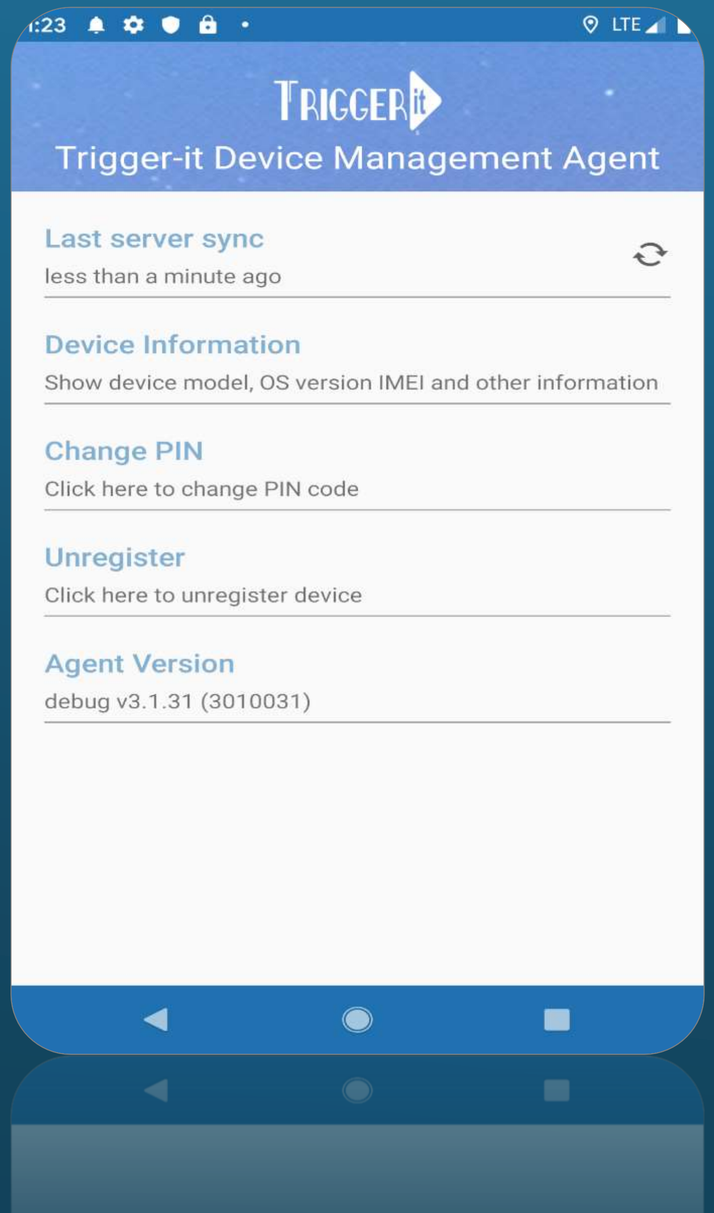


Network Devices Monitoring

High-performance SNMP traps receiver that allows administrators to receive alerts and notifications in real-time from network devices

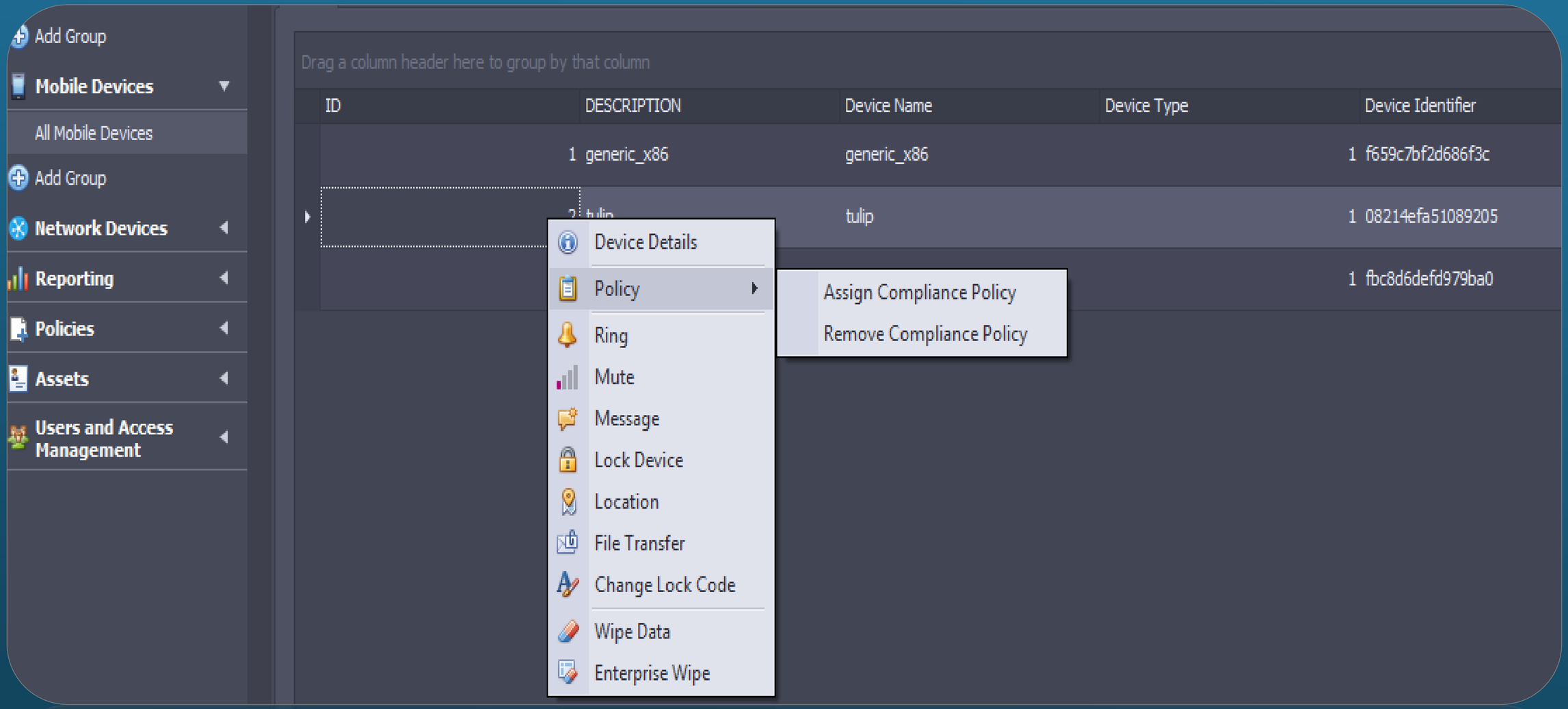


MDM Features

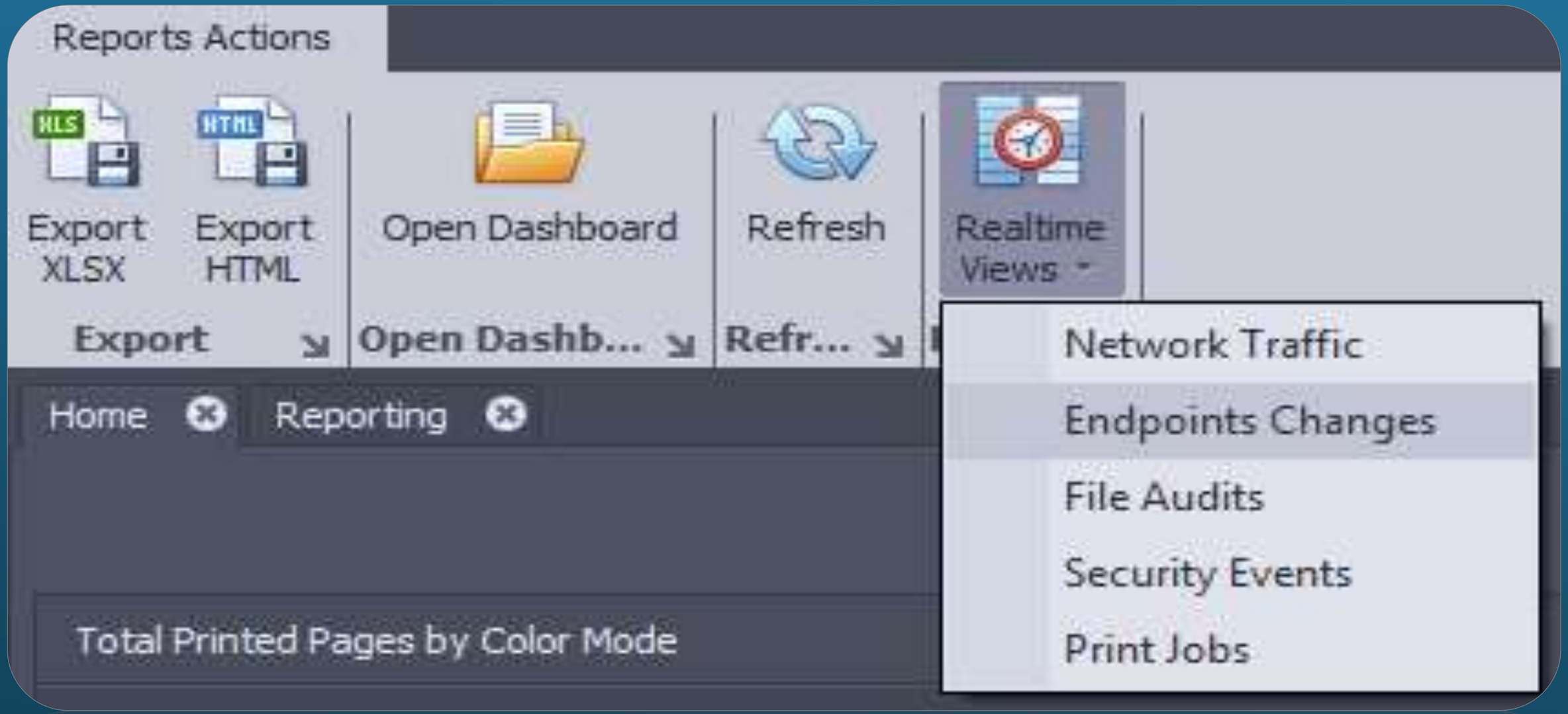


- Supports BYOD, COPE and system services through OEM installations.
- Supports ringing, messaging devices, locking devices, mute devices remotely.
- Location tracking with geo fencing capabilities.
- Remote wipe and enterprise wipe.
- Enterprise store for work profiles.
- Supports application Black/White listing,

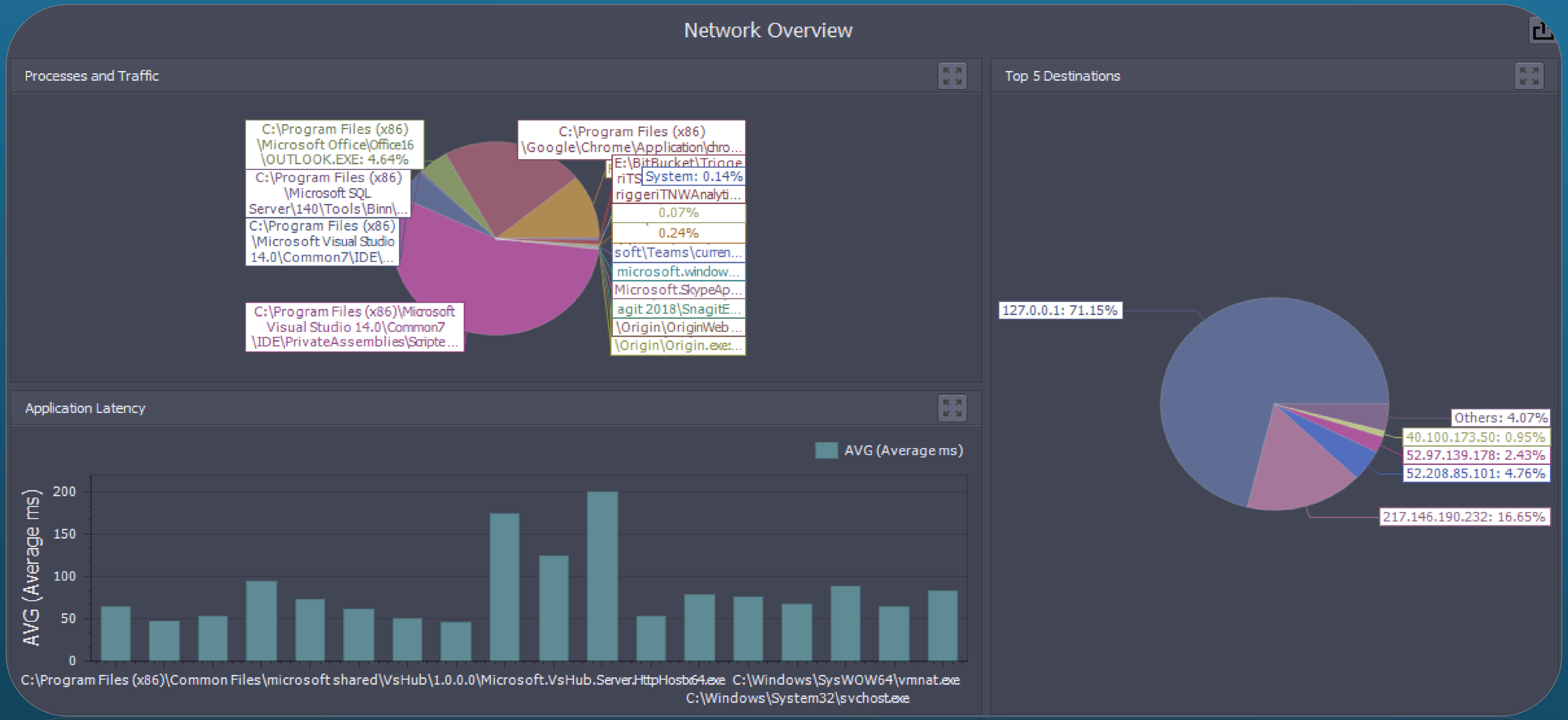
MDM Features



Real-Time Views



Dashboards Designer



Features List

#	FEATURES
1	Collect inventory (hardware and software)
2	Collect startup items and services
3	Collect machine info like (name, uptime, reboot required status, all assigned IPs, OS version/type, last seen, last login by, domain name if any, PC model, memory, CPU, HD, ...)
4	Collect launched executables compilation name/path per user
5	Collect OS and 3rd party updates
6	Collect software license count
7	Monitor network devices using SNMP traps receiver
8	Monitor network devices by pulling traffic statistics (Cisco , F5, Palo Alto, ForcePoint).
9	Build network topology including devices to network devices connectivity tracking
10	Monitor network traffic (total traffic and average of latency per process)
11	Monitor print jobs by user, file name, number of pages, page size, and color
12	Monitor machine performance (CPU, memory, and disk utilization per process)
13	Collect Errors on Managed PCs and inspect cause of error
14	Built-in general reports and real-time dashboards
15	Correlating machine performance insights with network traffic insights
16	PC categorization using tags
17	PC finder to find any PC with specific configuration (Hardware/software)
18	Tracking file operations
19	User behavior analytics
20	Interactive To-do list for administrators based on collected insights
21	Backup PCs to cloud storage
22	Create/Delete/Update registry keys

Features List - Continued

#	FEATURES
23	Run executables, commands, and scripts (PowerShell/VBS/Batch) remotely on managed PCs
24	Terminate process/executable on managed PCs
25	Download a file to managed PCs
26	Start OS update cycle on managed PCs
27	Stop/Start/Restart services on managed PCs
28	Reboot/Shutdown managed PCs
29	Activate windows remotely
30	Activate office remotely
31	Bandwidth reshaping per process
32	Digital asset management (Vendors, Contracts, POs) including support contracts renewals and asset transition tracking
33	Terminate Idle applications after certain period of time based on policies
34	Built-in remote tools
35	Control printing using policies like user quota, printers while/black lists, color printing prevention
36	Role based access for administrators
37	Software compliance by comparing managed endpoints by a reference image or configuration
38	Privilege access management on managed endpoints
39	Application white/black listing
40	Application behavior analytics and sandboxing integration
41	Block IP Address
42	Block TCP Port
43	Block UDP Port
44	Block Domain Name

Features List - Continued

#	FEATURES
45	Collected failed security events in real-time
46	MDM supports BYOD, COPE and system services through OEM installations
47	MDM supports ringing, messaging devices, locking devices, mute devices remotely
48	MDM supports location tracking with geo fencing capabilities
49	MDM supports remote and enterprise wipe
50	MDM supports enterprise store for work profiles
51	MDM supports application Black/White listing

SysGravity

sales@sysgravity.com

www.sysgravity.com