

ABEGuardian

Full visibility of your ICS/OT Systems in one centralized location

OT Asset Management, Vulnerability Management, and a host of additional features. Developed by Control Systems Experts, our software is designed to meet the unique needs of Control Systems professionals.

The screenshot displays the ABE Guardian web interface. On the left is a navigation sidebar with categories like Home, Diagram, Assets, Dashboard, Track Changes, Conditions, Reports, Query Tool, Vulnerabilities, Advisories, Configuration, Syslog Events, and Update Status. The main content area is divided into several sections:

- Asset Tree:** A hierarchical view of monitored assets, including Computers (499), Servers (31), Thin Clients (3), Network (34), OT Devices (1349), Hardware, and Security.
- Asset Details Table:** A table listing assets with columns for Type, Device Name, Alias, OS Version, System Boot Time, Total Physical Memory, Criticality, Zone, Last Update, and Release End Date. Assets include PDC1, AW7004, REFPLC03, DEMO1, LAPTOP-PSHFK182, WJN-76ASP0P14EI, 60AW05, and another 60AW05.
- Asset Summary (AW7004):**
 - Domain: IASERIES.local
 - System Manufacturer: Microsoft Corporation
 - System Model: Virtual Machine
 - Serial Number: 9571-8232-7583-4288-5277-9060-52
 - BIOS Version: American Megatrends Inc. 090008, 12/7/2018
 - System Locale: en-us;English (United States)
 - Time Zone: (UTC-08:00) Pacific Time (US_Canada)
 - NTP Server: Local CMOS Clock
 - NTP Last Sync: 2021-03-20 20:32:25
 - NTP Offset (seconds): 0.0000000s
 - Logged Users: administrator (Active, Idle Time: 2021-03-20 20:32:00, Session Name: 31c5ce9425)
- Usage Metrics:**
 - CPU Usage: 24.8%
 - Memory Usage: 61.1%
 - Network Usage: 3.6%
 - Disk Usage table:

Type	Drive Name	Percentage Usage	Size	Total Read	Total Write	File
C:\		22%	47 GB	1271912 K	540736 K	NTF
D:\		0%	0 GB	0 K	0 K	
 - Conditions: 81 (11 High, 31 Medium, 39 Low)
 - Vulnerabilities: 805 (29 Critical, 575 High, 197 Medium, 4 Low)
- System Information (Microsoft Windows 10 Pro N):**
 - OS Version: 10.0.17763 N/A Build 17763 Release ID: 1809
 - Notification: Not Licensed
 - Installed: 2020-08-28 20:18:38
 - OS Product Key: 00331-90000-00001-AA681
 - OS Product ID: 1 Processor(s) Installed, [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~2112 Mhz
 - Processor Type: Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
 - OS Directory: 2020-11-10 00:00:00
 - Release End Date: 1
 - Installed Apps: 4
 - Hotfixes Installed: 0
 - Pending Updates: 0

ABEGuardian helps Control Systems Engineers identify, evaluate, respond and report on software insecurities and misconfigurations of endpoints.

Identify

Centralized management solution to help manage IT and OT resources from a single interface, using a simple interface that makes your job easier.

Evaluate

Find all valuable assets across the organization that could be harmed by threats in a way that can result in a monetary loss.

Detect

Analyze the entirety of your plant Ecosystem to identify any malicious activities that could compromise the network or the integrity of the System.

Respond

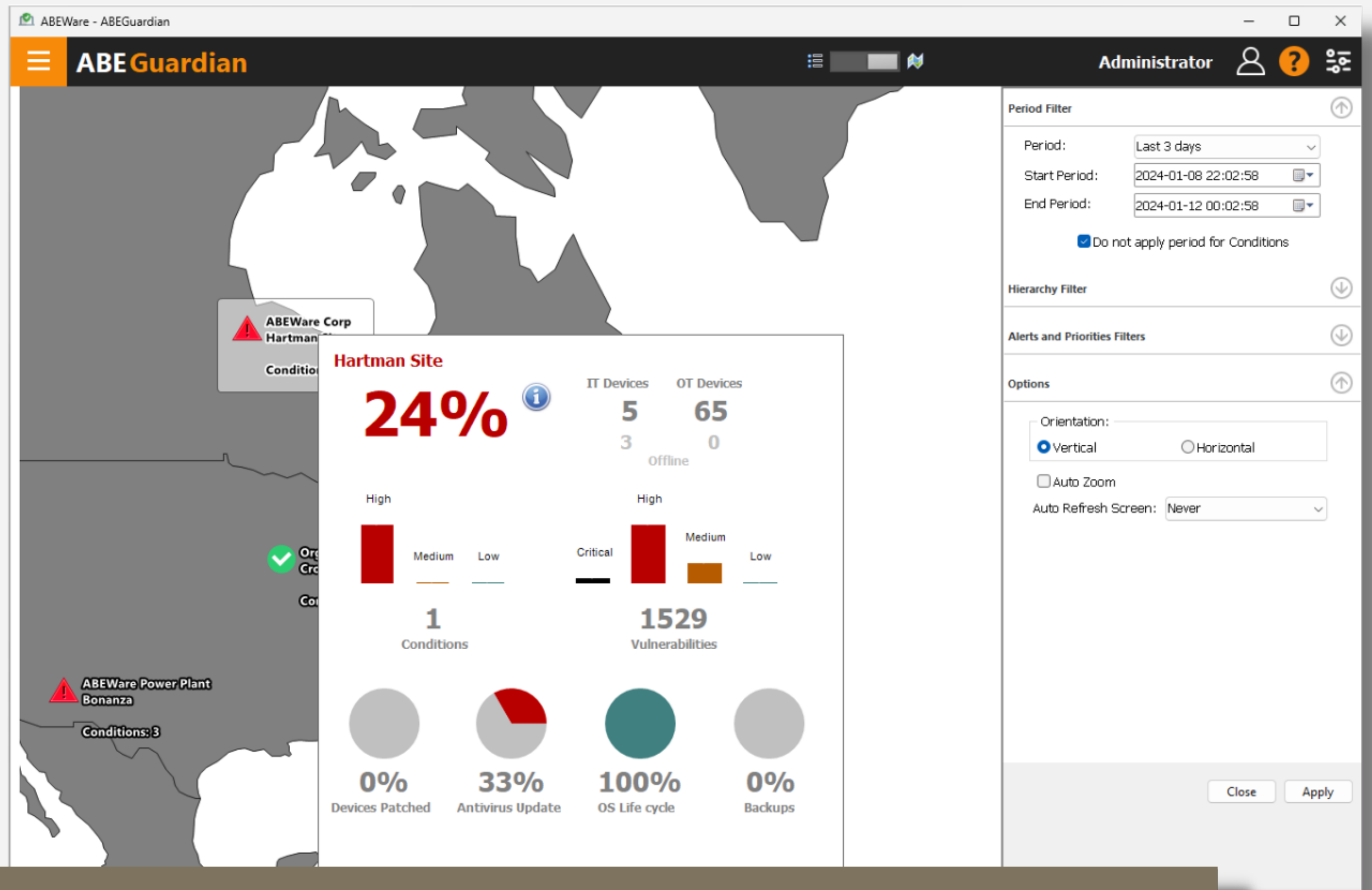
Quickly act against detected malicious threats with the help of the an advanced Alert System.

Report and Alert

Monitor all devices proactively to guarantee the best practices defined are being enforced throughout the plant. When an event is detected it will generate an Alert that can notify the user in the application or by email.

Multi Site Support

MANAGE ALL YOUR SITES FROM A SINGLE LOCATION, WITH A FULL VISUALIZATION OF YOUR ASSETS AND THREATS



Overview Diagram

- ABEware LLC
 - SoCal Site
 - Oak Hill Site
 - Refinery
 - Hartman Refinery
 - Wonderbiz Office
 - Honeywell DCS
 - Foxboro DCS

Active Conditions

Type	Device Name	Device	Condition Date	Condition	Prior	Details
Enterprise : ABEware LLC (Count = 2005)						
Site : Oak Hill Site (Count = 2005)						
Plant : Hartman Refinery (Count = 2005)						
Zone : Foxboro DCS (Count = 1843)						
▲	AW7004	Computers	2022-02-15 11:08:15 EST	Antivirus Definition not up to date	1	"Entity": "Windows Defender" "Version": "0.0.0.0" "Definition Date": "1970-04-02 00:00:00" "Definition Version": "0.0.0.0"
▲	AW7004	Computers	2022-02-15 11:08:15 EST	Users with Password set to never expire	1	"Entity": "Access1" "Source": "Local" "Password Expires": "1970-01-01 00:00:00" "Password Never Expires": null
▲	AW7004	Computers	2022-02-15 11:08:15 EST	Users with Password set to never expire	1	"Entity": "Administrator" "Source": "Local" "Password Expires": "1970-01-01 00:00:00" "Password Never Expires": null
▲	AW7004	Computers	2022-02-15 11:08:15 EST	Users with Password set to never expire	1	"Entity": "DefaultAccount" "Source": "Local" "Password Expires": "1970-01-01 00:00:00" "Password Never Expires": null
▲	AW7004	Computers	2022-02-15 11:08:15 EST	Users with Password set to never expire	1	"Entity": "fox" "Source": "Local" "Password Expires": "1970-01-01 00:00:00" "Password Never Expires": null

Add new Conditions

Conditions Available:

Enter text to search... Find Clear

- Category : Authentication (Count = 8)
 - Locked Users
 - New user accounts created
 - Too many failed user logon attempts
 - Umass Cond
 - User with older Passwords
 - Users logged for too long
 - Users with Password not Required
 - Users with Password set to never expire
- Category : Hardware Monitoring (Count = 10)
 - High CPU Usage
 - High Hard Disk Usage
 - High RAM Memory Usage
 - Switch Fan RPM
 - Switch Fan Status
 - Switch PSU Status
 - Switch Temperature Exceeded
 - Syslog Events
 - Unknown USB Device
 - Unsafe USB Device
- Category : Security (Count = 19)
 - All Removable Classes Enabled
 - Antivirus Definition not up to date

Manage Conditions and Alerts

MORE THAN 70 CONDITIONS AND ALERTS CAN BE MANAGED LIKE PROCESS ALARMS, WITH ACKNOWLEDGE, SHELVE AND IGNORE CAPABILITIES. STAY ON TOP OF ALL EVENTS AND MAKE SURE NOTHING IS LEFT BEHIND. USERS CAN ALSO CREATE THEIR OWN CUSTOM ALERTS AND CONDITIONS ADDING INFINITE CAPABILITIES TO THIS MODUL

Manage Vulnerability Exposure

DETECT AND MANAGE VULNERABILITIES APPLICABLE TO DEVICES IN THE PROCESS NETWORK BY CROSS REFERENCING NIST.GOV, MICROSOFT AND VENDOR DATABASE INFORMATION

The screenshot displays the ABE Guardian interface. On the left is a navigation menu with options like Home, Diagram, Assets, Dashboard, Track Changes, Conditions, Reports, Query Tool, Vulnerabilities, Advisories, Configuration, Syslog Events, and Update Status. The main area is divided into 'Asset Details' and a 'Vulnerabilities' table.

Severity	CVE	Product	Base	Impact	Exploitability	Remediation	Vendor Approved	Approved Date	Approve Vendor
High	CVE-2022-21874	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5009546	CONDITIONALLY APPROVED	2022-01-28 00:00:00	Schneider Electr
High	CVE-2022-21849	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5009546	CONDITIONALLY APPROVED	2022-01-28 00:00:00	Schneider Electr
High	CVE-2021-43217	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5008207	CONDITIONALLY APPROVED	2022-01-03 00:00:00	Schneider Electr
High	CVE-2021-43215	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5008207	CONDITIONALLY APPROVED	2022-01-03 00:00:00	Schneider Electr
High	CVE-2021-36965	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5005573	CONDITIONALLY APPROVED	2021-09-29 00:00:00	Schneider Electr
High	CVE-2021-36936	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5005043	CONDITIONALLY APPROVED	2021-08-25 00:00:00	Schneider Electr
High	CVE-2021-33757	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5004238	CONDITIONALLY APPROVED	2021-07-28 00:00:00	Schneider Electr
High	CVE-2021-31962	Windows 10 Version 1607 for x64-based Systems	9.8	5.9	3.9	KB5003638	CONDITIONALLY APPROVED	2021-06-23 00:00:00	Schneider Electr
High	CVE-2021-28476	Windows 10 Version 1607 for x64-based Systems	9.9	6.0	3.1	KB5003197	CONDITIONALLY APPROVED	2021-05-26 00:00:00	Schneider Electr

Vulnerability Dashboard

MULTIPLE DASHBOARDS AVAILABLE TO KEEP THE VULNERABILITIES UNDER CONTROL AND FOCUS ON THE HIGHER RISK AND LOWER COMPLEXITY THREATS

The screenshot shows the 'Vulnerabilities Dashboard' in ABE Guardian. It features several key metrics and charts:

- Total Vulnerabilities:** 12838
- Vulnerabilities per Score:**
 - Critical: 353
 - High: 8949
 - Medium: 3411
 - Low: 125
- Vulnerability per Criticality:** A stacked area chart showing the distribution of vulnerabilities across severity levels from 8/12/2022 to 8/25/2022.
- Attack Vector Criticality:** A table listing attack vectors and their counts:

Type	Attack Vector	Severity	Count
LOCAL	LOCAL	HIGH	5262
NETWORK	NETWORK	HIGH	3554
LOCAL	LOCAL	MEDIUM	1948
NETWORK	NETWORK	MEDIUM	1170
NETWORK	NETWORK	CRITICAL	343
PHYSICAL	PHYSICAL	MEDIUM	172
ADJACENT_NETWORK	ADJACENT_NETWORK	HIGH	130
ADJACENT_NETWORK	ADJACENT_NETWORK	MEDIUM	121
LOCAL	LOCAL	LOW	57
NETWORK	NETWORK	LOW	53
ADJACENT_NETWORK	ADJACENT_NETWORK	LOW	15
ADJACENT_NETWORK	ADJACENT_NETWORK	CRITICAL	10
PHYSICAL	PHYSICAL	HIGH	3
- Integrity Impact:** Pie chart showing 9,070 NONE (27.1%), 289 HIGH (70.6%), and 2 LOW (2.25%) vulnerabilities.
- Confidentiality Impact:** Pie chart showing 10,870 NONE (12.01%), 426 HIGH (84.67%), and 3 LOW (3.32%) vulnerabilities.
- Availability Impact:** Pie chart showing 9,669 NONE (23.89%), 102 HIGH (75.32%), and 3 LOW (0.79%) vulnerabilities.
- Attack Complexity:** Pie chart showing 10,289 NONE (18.88%) and 2,549 LOW (80.14%) vulnerabilities.

Condition Monitoring

MONITOR ALL ACTIVE CONDITIONS, EVENTS, PATCH MANAGEMENT, ANTIVIRUS DEFINITION, INSTALLED SOFTWARES AND MUCH MORE

The image displays three overlapping screenshots of the ABE Guardian software interface, illustrating its capabilities in condition monitoring and software management.

Active Conditions Dashboard: This dashboard provides a comprehensive overview of system conditions. It features a 'Total Conditions' card showing 2169 active conditions. A 'Conditions per Priority' section breaks down the total into Priority 1 (1686), Priority 2 (246), and Priority 3 (237). A 'Conditions per Type' pie chart shows the distribution: Security (68.61%), Windows Features (4.37%), Vulnerabilities (10.36%), Hardware Monitoring (13.73%), Watchdog (0.52%), and Authentication (2.4%). A 'Conditions per Priority per Day' area chart tracks the volume of conditions over time from August 12, 2022, to August 26, 2022.

Installed Software Dashboard: This dashboard tracks the software installed on the network. It shows a total of 4588 installed software instances and 2970 unique software titles. An 'Installed Software by Day' bar chart shows the daily count of software installations. Below this, a 'Most Common Publishers' pie chart identifies the top publishers: Microsoft Corporation (34.07%), Fedora Project (14.34%), and Other Vendors (21.62%). The dashboard also includes a table of 'Unique Versions' and a list of 'Least Common Softwares'.

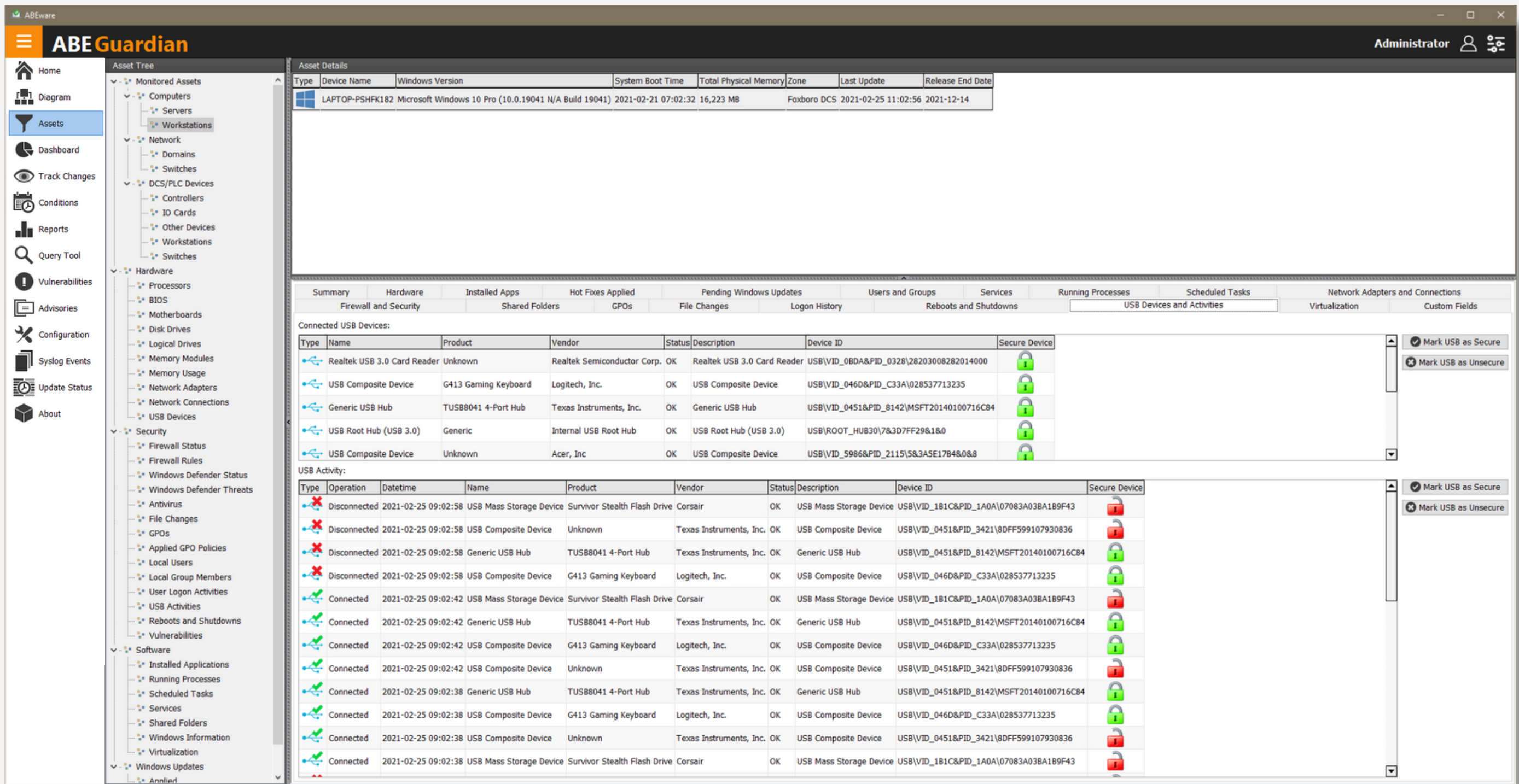
Overview Dashboard: This dashboard provides a high-level summary of system health. It shows that 63% of ABEware Corp devices are online, with 21 IT devices and 1629 OT devices. It also displays 536 conditions and 17507 vulnerabilities. Four progress indicators show the status of key tasks: 93% of devices are patched, 78% have antivirus updates, 87% are within their OS life cycle, and 86% have backups.

Compare Sites and Plants

COMPARE SITES AND PLANTS USING THE OVERVIEW CARDS. THIS INCLUDES A SUMMARY OF THE MOST IMPORTANT METRICS CALCULATED BY ABEGUARDIAN

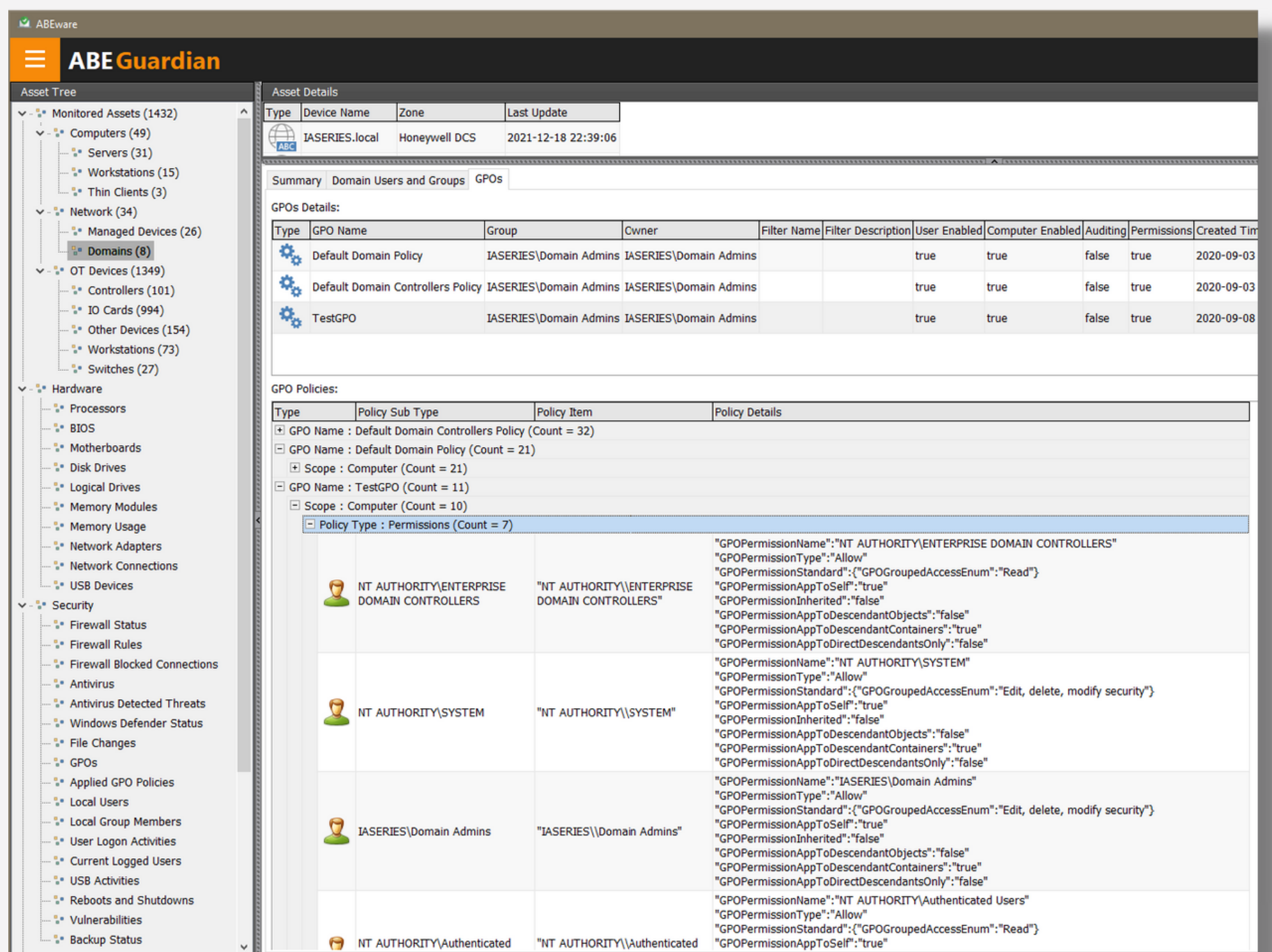
External Devices Management

TRACK USB EXTERNAL DEVICES AND STORAGE, FLAG DEVICE'S AS SAFE OR UNSAFE AND CREATE ALERTS WHEN UNKNOWN OR UNSAFE DEVICES ARE ACCESSING YOUR NETWORKS



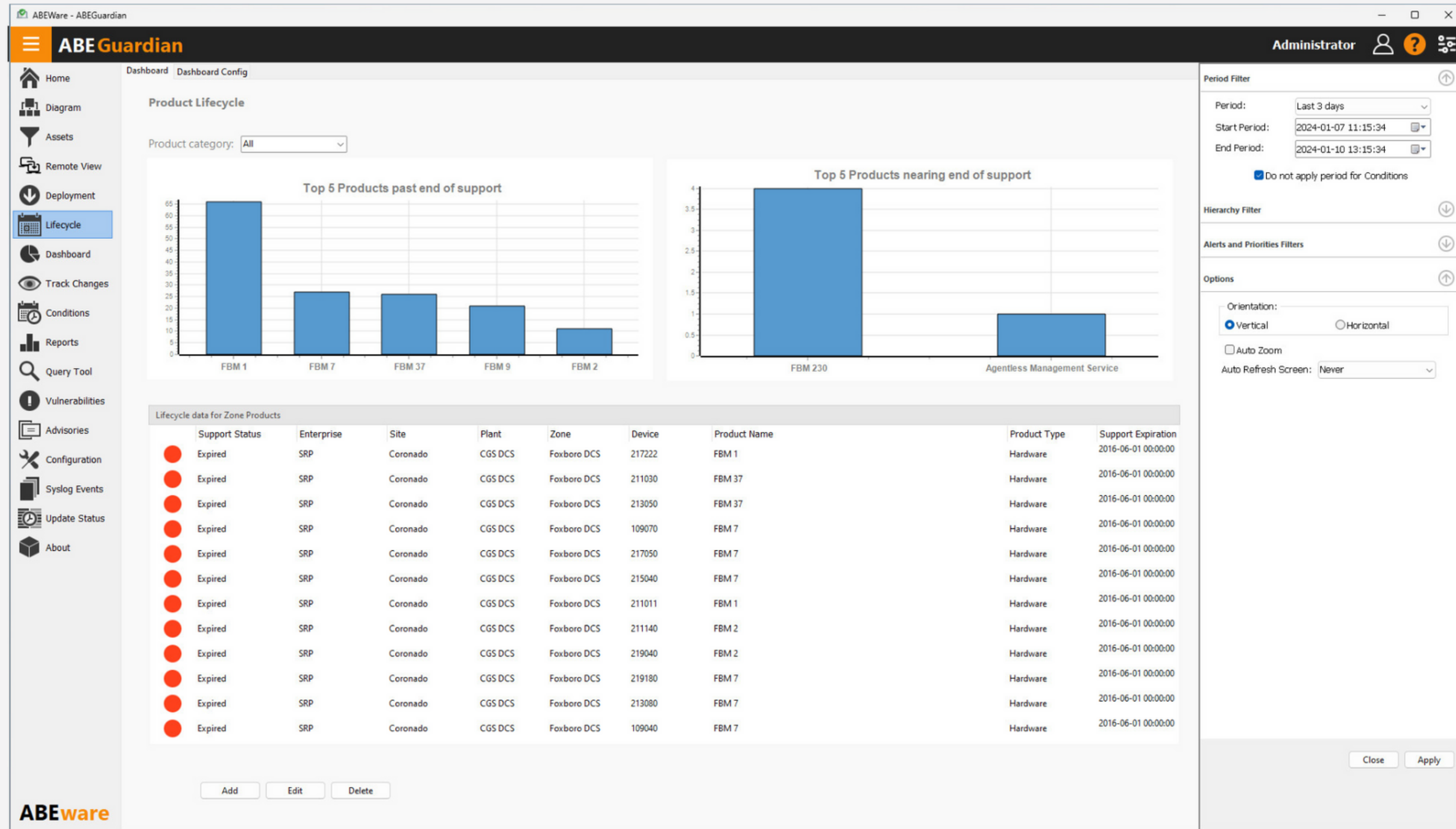
GPO Monitoring

BE SURE ALL SERVERS ARE UP TO DATE WITH GROUP POLICIES AND TRACK ANY CHANGES TO THE POLICIES AS THEY HAPPEN TO AVOID MALICIOUS ACTIONS GO UNNOTICED FOR TOO LONG



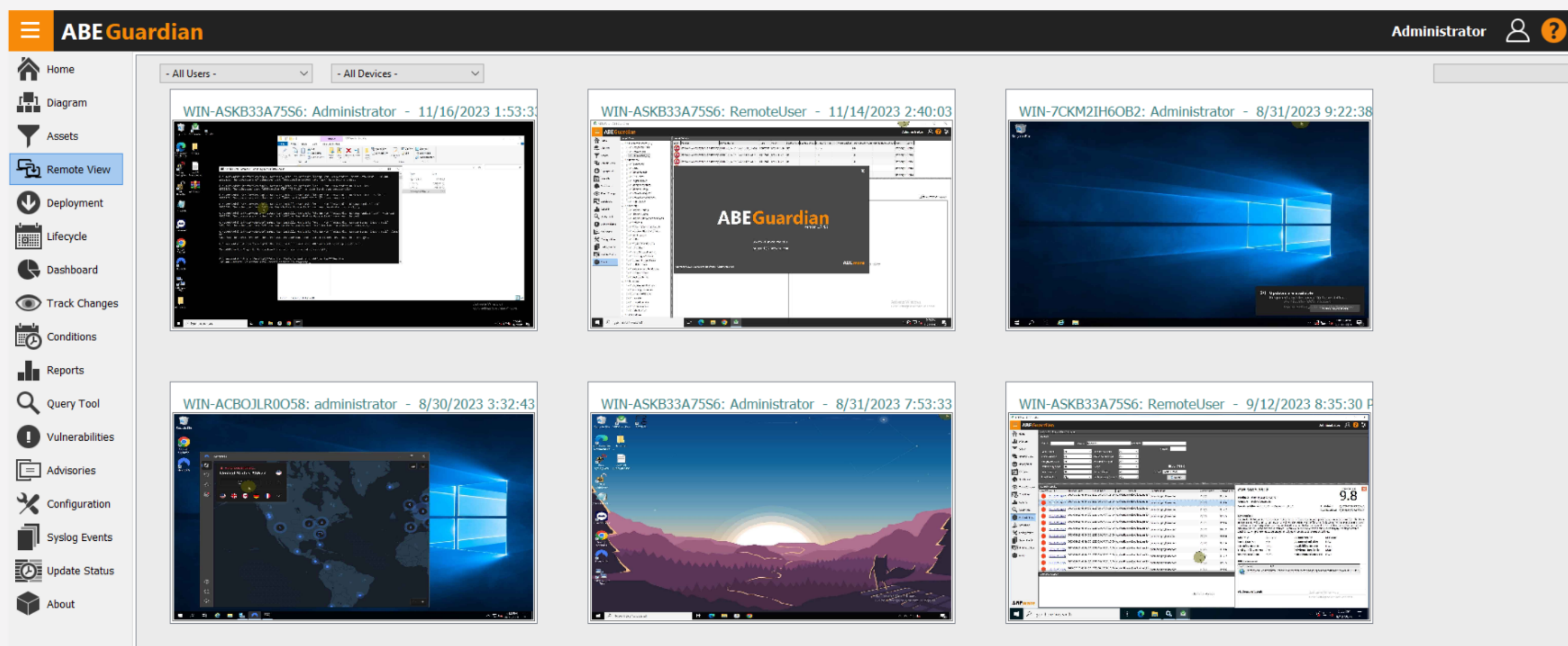
Lifecycle Management

LIFECYCLE MANAGEMENT HELPS SYSTEM ENGINEERS EFFECTIVELY MANAGE, OPTIMIZE, AND MAKE THE RIGHT DECISIONS ACROSS THE ENTIRE LIFESPAN OF PRODUCTS, AND SYSTEMS. THIS FEATURE HELPS WITH OVERALL EFFICIENCY, SUSTAINABILITY, AND SUCCESS.



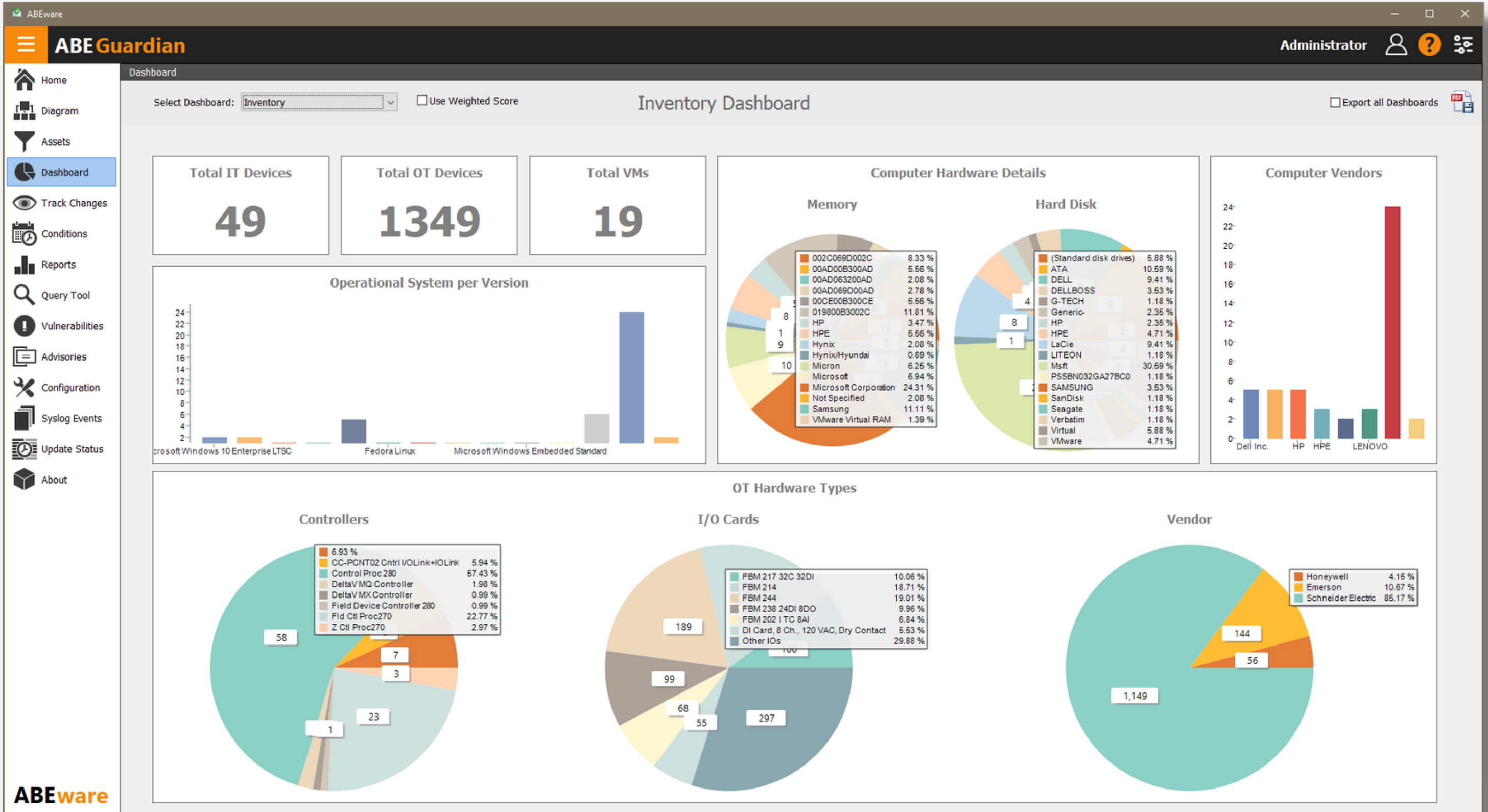
Remote View & Recording

THIS FEATURE ALLOWS THE SYSTEM ENGINEER TO EASILY MONITOR ANY SERVER WITHIN THE NETWORKS THAT REPORT BACK TO ABEGUARDIAN. THIS CAPABILITY HAS DEMONSTRATED ITS VALUE IN TRAINING AND INCIDENT SCENARIOS.



Inventory Management

DISCOVER AVAILABLE OT DEVICES, VENDOR, MODEL, FIRMWARE, REVISION AND STATUS. DETECT DEVICES NOT RUNNING PROPERLY AND WITH PENDING UPDATES



The screenshot shows the 'Asset Tree' and 'Asset Details' sections of the ABE Guardian interface. The Asset Tree on the left shows a hierarchy of assets, including Monitored Assets (1432), Computers (49), Network (34), and OT Devices (1349). The Asset Details table on the right provides a detailed view of the selected asset, including its vendor, device name, type, model, and status.

Logo	Vendor	Device Name	Type	Model	Status	Main	Sta
H	Honeywell	PM1EWS	Workstation	Console	On		
H	Honeywell	PM1OWS1	Workstation	Console	Off		
H	Honeywell	SPTROWS1	Workstation	Console	Off		
H	Honeywell	SPTROWS2	Workstation	Console	Off		
S	Schneider Electric	01CP01	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01CP02	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01CP03	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01CP04	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01GW01	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01GW02	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01GW03	Controller	Control Proc 280	Off		Off
S	Schneider Electric	01GW04	Controller	Control Proc 280	Off		Off

The 'Device Details' section for the selected asset (01CP01) shows the following parameters and values:

Parameter	Value
@HOST STATION	01CP01
@SYSMON NAME	01SM01
ALARMING STATE	Enabled
CABLE STATE	No Information
DIAG STATE	Not Active
DOWNLOAD STATE	Not Downloading
EE UPDATE STATE	Not Updating
FAIL ACK STATE	Not Acknowledged
FAIL DEV ACK	Acknowledged
FAIL DEV ATT	No
FAIL STATE	Failed
FT STATE	Non Operational
MT REPORT STATE	Sync_Not_Config
PRIM EEPROM REV	093002
PRIM HARD DATE	1430
PRIM HARD PART	RH924YA
PRIM HARD REV	cD

Multi Vendor Support

ABEGUARDIAN SUPPORTS SCHNEIDER FOXBORO, HONEYWELL EXPERION AND EMERSON DELTA-V SYSTEMS, BESIDES MANY MORE OT/ICS VENDORS.

Deployment Manager

SIMPLY DEPLOY WINDOWS PATCHES, WINDOW DEFENDER, MCAFEEUPDATES, AND ANY CUSTOM UPDATES SIMPLY FROM DEPLOYMENT MANAGER. DEPLOY TO INDIVIDUAL STATIONS OR THROUGH YOUR ENTIRE INVENTORY. SELECT FROM ABEGUARDIAN SERVER LIST, OR UPLOAD YOUR OWN FILES.

The image displays two overlapping screenshots of the ABE Guardian software interface. The top screenshot shows the 'Active Deployments' section with a table of deployment tasks. The bottom screenshot shows the 'Configuration' window for selecting update types and devices.

State	Type	Enterprise	Site	Plant	Zone	Device Name	Alias	Action Type	Item	Status	Filename	Auto Update	Update ASAP	Do not reboot	Deploy only (do not install)	Custom Command
🔄	🔄	ABEWare Corp	Hartman Site	Refinery 2	Office	DESKTOP-BRG45A1		wsus	KB5031445	KB not found		✖	✖	✔	✔	
🔄	🔄	ABEWare Corp	Hartman Site	Refinery 2	Office	WIN-UL1005NSGRB	DC0002 (Secondary Domain Controller)	wsus	KB5030213	Available to Deploy	windows10.0-kb5030213-x64_98599efc4c53e361d14e6f5cb4be332b8123f97c.msu	✖	✖	✔	✔	
🔄	🔄	ABEWare Corp	Hartman Site	Refinery 2	Office	WIN-UL1005NSGRB	DC0002 (Secondary Domain Controller)	wsus	KB5032789	Available to Deploy	windows10.0-kb5032789-x64_33ea3888c89d2388b845c02ebd2395041341d1f1f.msu	✖	✖	✔	✔	

Configuration Window:

- Select update type:** Windows patches (selected), Windows defender update, McAfee DAT update, Custom update.
- Browse update file:** Select from a list (KB5034134), Type manually.
- Custom command:** (empty)
- Select devices to apply updates:** OS Filter: %
- Available KB list:** KB5034588 - 2024-01 Servicing Stack Update for Windows Server 2012 - KB5034588, KB5034276 - January 9, 2024 - KB5034276 Cumulative Update for .NET Framework 3.5, 4.8, 4.8.1 for Windows 11, KB5034273 - January 9, 2024 - KB5034273 Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10, version 1809 and Windows Server, version 2019, KB5034272 - January 9, 2024 - KB5034272 Cumulative Update for .NET Framework 3.5, 4.8, 4.8.1 for Windows Server 2022, KB5034184 - January 9, 2024 - KB5034184 (Monthly Rollup), KB5034176 - January 9, 2024 - KB5034176 (Security-only update), KB5034173 - January 9, 2024 - KB5034173 (Monthly Rollup), KB5034171 - January 9, 2024 - KB5034171 (Monthly Rollup), KB5034169 - January 9, 2024 - KB5034169 (Monthly Rollup), KB5034167 - January 9, 2024 - KB5034167 (Security-only update), KB5034134 - January 9, 2024 - KB5034134 (OS Build 10240.20402), KB5034130 - January 9, 2024 - KB5034130 (OS Build 25398.643), KB5034129 - January 9, 2024 - KB5034129 (OS Build 20348.2227), KB5034127 - January 9, 2024 - KB5034127 (OS Build 17763.5329), KB5034123 - January 9, 2024 - KB5034123 (OS Builds 22621.3007 and 22631.3007), KB5034122 - January 9, 2024 - KB5034122 (OS Builds 19044.3930 and 19045.3930), KB5034121 - January 9, 2024 - KB5034121 (OS Build 22000.2713), KB5034119 - January 9, 2024 - KB5034119 (OS Build 14393.6614), KB5033910 - January 9, 2024 - KB5033910 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server, version 2016, KB5033466 - 2023-12 Servicing Stack Update for Windows Server 2008 - KB5033466, KB5033433 - December 12, 2023 - KB5033433 (Monthly Rollup), KB5033429 - December 12, 2023 - KB5033429 (Monthly Rollup), KB5033427 - December 12, 2023 - KB5033427 (Security-only update), KB5033424 - December 12, 2023 - KB5033424 (Security-only update), KB5033422 - December 12, 2023 - KB5033422 (Monthly Rollup), KB5033420 - December 12, 2023 - KB5033420 (Monthly Rollup), KB5033383 - December 12, 2023 - KB5033383 (OS Build 25398.584), KB5033379 - December 12, 2023 - KB5033379 (OS Build 10240.20345), KB5033375 - December 12, 2023 - KB5033375 (OS Builds 22621.2861 and 22631.2861), KB5033373 - December 12, 2023 - KB5033373 (OS Build 14393.6529), KB5033372 - December 12, 2023 - KB5033372 (OS Builds 19044.3803 and 19045.3803), KB5033371 - December 12, 2023 - KB5033371 (OS Build 17763.5206), KB5033369 - December 12, 2023 - KB5033369 (OS Build 22000.2652), KB5033118 - December 12, 2023 - KB5033118 (OS Build 20348.2159), KB5032391 - 2023-11 Servicing Stack Update for Windows 10 Version 1607/Server 2016 - KB5032391, KB5032390 - 2023-11 Servicing Stack Update for Windows 10 - KB5032390, KB5032383 - 2023-11 Servicing Stack Update for Windows 7/Server 2008 R2 - KB5032383, KB5032340 - November 14, 2023 - KB5032340 Cumulative Update for .NET Framework 3.5, 4.8, 4.8.1 for Windows 10, KB5032337 - November 14, 2023 - KB5032337 Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10, version 1809 and Windows Server, version 2019, KB5032336 - November 14, 2023 - KB5032336 Cumulative Update for .NET Framework 3.5, 4.8, 4.8.1 for Windows Server 2022, KB5032309 - 2023-11 Servicing Stack Update for Windows Server 2012 - KB5032309, KB5032288 - December 4, 2023 - KB5032288 (OS Builds 22621.2792 and 22631.2792) Preview, KB5032278 - November 30, 2023 - KB5032278 (OS Build 19045.3750) Preview, KB5032254 - November 14, 2023 - KB5032254 (Monthly Rollup), KB5032252 - November 14, 2023 - KB5032252 (Monthly Rollup), KB5032250 - November 14, 2023 - KB5032250 (Security-only update), KB5032249 - November 14, 2023 - KB5032249 (Monthly Rollup), KB5032248 - November 14, 2023 - KB5032248 (Security-only update), KB5032247 - November 14, 2023 - KB5032247 (Monthly Rollup), KB5032202 - November 14, 2023 - KB5032202 (OS Build 25398.531), KB5032199 - November 14, 2023 - KB5032199 (OS Build 10240.20308), KB5032198 - November 14, 2023 - KB5032198 (OS Build 20348.2113), KB5032197 - November 14, 2023 - KB5032197 (OS Build 14393.6452), KB5032196 - November 14, 2023 - KB5032196 (OS Build 17763.5122), KB5032192 - November 14, 2023 - KB5032192 (OS Build 22000.2600), KB5032190 - November 14, 2023 - KB5032190 (OS Builds 22621.2715 and 22631.2715), KB5032189 - November 14, 2023 - KB5032189 (OS Builds 19044.3693 and 19045.3693), KB5031989 - November 14, 2023 - KB5031989 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server, version 2016, KB5031659 - 2022-10 Servicing Stack Update for Windows Server 2008 - KB5031659, KB5031589 - 2023-10 Servicing Stack Update for Windows 7/Server 2008 R2 - KB5031589, KB5031588 - 2023-10 Servicing Stack Update for Windows 10 1809/Server 2019 - KB5031588, KB5031469 - 2023-10 Servicing Stack Update for Windows Server 2012 - KB5031469, KB5031466 - 2023-10 Servicing Stack Update for Windows 10 - KB5031466, KB5031466 - December 30, 2023 - KB5031466 (OS Build 23463.3606) Preview.

Device Selection: Exelon Corp, Hartman Site, Digital Realty, Warrington, ABEWare Corp, Everett, Mystic Turbine 1, Honeywell DCS, Computers, WIN-ASKB33A7556, Hartman Site, Refinery 2, Office, Computers, 10.10.81.5, 192.168.1.10, DESKTOP-BRG45A1, DESKTOP-PRJAGLD, DESKTOP-RVACV77, WIN-15MEEB367LQ, WIN-7CKM2IH6OB2, WIN-7GUKH-N8KJNR, WIN-88TOQR4MTRT, WIN-ABE008, WIN-ABE010, WIN-ABE201, WIN-ACB0ILR0058, WIN-ASKB33A7556, WIN-ESGV941UECT, WIN-HIKSAM6EMKK, WIN-UL1005NSGRB.

Deployment Options: Update ASAP, Deploy only (do not install), Do not reboot.

Additional features:

Credential Monitoring

Monitor all logins, log outs, failed login attempts, current users logged in, all credential properties, locked accounts and expired passwords.

File Tracking

Select folders and file types to track. Monitor changes, deleted and created files on chosen devices.

Services and Process Monitoring

Monitor and Track changes in Services and Processes to detect unwanted changes and unauthorized processes.

Hardware Management

Monitor CPUs, Motherboard, Memory, Hard disk of all Assets and detect unusual behaviors.

Query Tool

Create queries across the whole system in a centralized location. This allows users to expand the capabilities of ABEGuardian beyond existing features (secure RESTful API available for sharing data to other applications).

Security Monitoring

Track Firewall Settings and rules as well as Antivirus configuration (including Windows Defender), detected threats and much more.

CISA & NIST Alerts and Advisories

Automatically collect, detect and alert of specific CISA (Cybersecurity & Infrastructure Security Agency) alerts and advisories.

Backup Monitoring

Monitor backup status and last run time to allow a complete visualization of all backup tool status across the plants.

Syslog Server

Collect and historize Syslog messages from multiple devices. Monitor specific events and generate alerts and conditions.

Patch Approvals by Vendor

Import vendor specific patch approvals to monitor which patches are allowed to be installed.

Custom Dashboards

Create custom web dashboards with your data. Dashboards can be shares and also embedded into your own webpage or intraweb.

RESTful API for data exchange

Create secure views and share any data collected by ABEGuardian with 3rd party systems using our RESTApi interface in a secure and control way.

ABEGuardian

ICS/OT Asset Management Security made simple
ABEGuardian gives you Full visibility of your ICS/OT Systems in one
centralized location

CALL, TEXT OR EMAIL:

+1 508 446-3393

www.ABEware.com

[*sales@abeware.com*](mailto:sales@abeware.com)