Absolute Insights for Endpoints

Deriving real-time asset and security insights across your endpoints

With a subscription to Absolute Visibility, Control, or Resilience, you can access a plethora of IT and security information to analyze the current state of your devices and security posture. With the new work from anywhere era, however, practitioners are having to manage and secure a largely remote endpoint fleet, resulting in the need for more dynamic historical endpoint trend analysis to understand device, user, and application behavior. In addition to analyzing trends, IT and security teams also require the ability to visualize device and security compliance patterns to hunt for anomalies. Common challenges in identifying potential device and security risks include:

Security and Compliance:

- Identifying the number of users and devices connecting to the corporate network and ones that are not
- Analyzing changes in data risk exposure over time due to accumulated sensitive personal, corporate, or customer data
- Pinpointing the presence of a specific file containing sensitive information across all your endpoints
- Monitoring changes in BIOS version over time to guard against potential threats below the OS
- Identifying suspicious devices with large number of IP address or location changes

User Experience:

- Monitoring CPU and memory usage of devices and running applications over time to identify and resolve issues impacting user experience proactively

Health:

- Tracking historical application health status across different device or user groups in the organization and identifying ones that require improvement
- Monitoring OS patch health and software updates over time to maintain device health

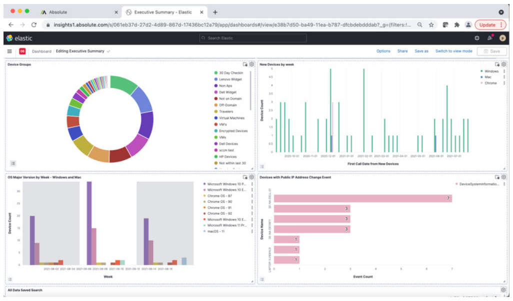
Asset Management:

- Tracking the rollout of new applications and patches across all endpoints
- Analyzing the usage of applications over time to optimize license spend
- Proactively assessing physical device characteristics over time to identify issues related to battery level and disk capacity

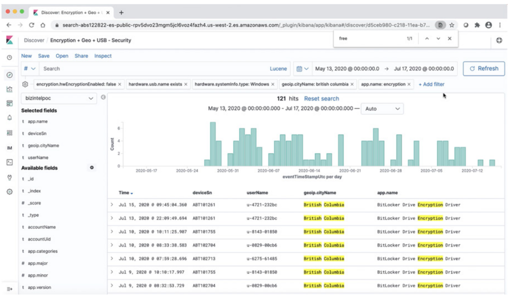
The need for dynamic asset and security insights

With the evolving business and work environment, there's a clear need for IT and security practitioners to be able to access fleet-wide device and security trends to effectively manage their endpoints, enforce policies to adhere with internal policies or regulatory frameworks, and respond to risks whenever they arise. Absolute Insights™ for Endpoints empowers administrators with trends into a variety of historical asset and security metrics across their device population, including OS patch health, software updates, application health and usage, geolocation, user behavior patterns, and sensitive data exposure to name a few. Absolute customers can access a set of pre-built dashboards or choose to create custom ones aligned with their organization's internal policies. Key capabilities include:

- Historical device and security trends across your entire device population
- Ability to leverage a growing library of pre-built dashboards or create custom ones based on your organization's policies
- Customize dashboard timelines (specify by month, week, day, or hour) to obtain drilled-down information
- Create data correlation from raw data points to identify abnormalities in device and security metrics
- Create custom visualizations through tables, pie, bar, and line charts among others
- Run queries across your device and security datapoints to search for and investigate anomalies



Absolute
Executive Summary - Elastic
insights1.absolute.com/s/061eb37d-27d2-4d89-867d-17436bc12a79/app/dashboards#/view/e38b7d50-ba49-11ea-b787-dfcbdebdddab?_g=(filters:!...
Update
elastic
Search Elastic
Dashboard / Editing Executive Summary
Options
Share
Save as
Switch to view mode
Save
Device Groups
30 Day Checkin
Lenovo Widget
Non Aps
Dell Widget
Not on Domain
Off-Domain
Travelers
Virtual Machines
VM's
Encrypted Devices
VMs
Dell Devices
sccm test
HP Devices
Not within last 30
New Devices by week
Windows
Mac
Chrome
Device Count
First Call Date from New Devices
OS Major Version by Week - Windows and Mac
Microsoft Windows 10 P...
Microsoft Windows 10 E...
Chrome OS - 87
Chrome OS - 90
Chrome OS - 91
Chrome OS - 92
Microsoft Windows 10 E...
Microsoft Windows 11 Pr...
macOS - 11
Device Count
Week
Devices with Public IP Address Change Event
DeviceSystemInformatio...
Device Name
Event Count
7
3
3
3
1
1
1
All Data Saved Search



Discover: Encryption + Geo + ...
search-abs122822-es-public-rpv5dvo23mgm5jcl6voz4fazh4.us-west-2.es.amazonaws.com/_plugin/kibana/app/kibana#/discover/d5ceb980-c218-11ea-b7...
Discover / Encryption + Geo + USB - Security
free 1/1
New
Save
Open
Share
Inspect
Search
Lucene
May 13, 2020 @ 00:00:00.0 → Jul 17, 2020 @ 00:00:00.0
Refresh
encryption.hwEncryptionEnabled: false
hardware.usb.name exists
hardware.systeminfo.type: Windows
geoip.cityName: british columbia
app.name: encryption
+ Add filter
bizintelpoc
Selected fields
app.name
deviceSn
geoip.cityName
userName
Available fields
_id
_index
_score
_type
accountName
accountUid
app.categories
app.major
app.minor
app.version
121 hits
Reset search
May 13, 2020 @ 00:00:00.000 - Jul 17, 2020 @ 00:00:00.000 —
Auto
Count
2020-05-17
2020-05-24
2020-05-31
2020-06-07
2020-06-14
2020-06-21
2020-06-28
2020-07-05
2020-07-12
eventTimeStampUtc per day

Time	deviceSn	userName	geoip.cityName	app.name
Jul 15, 2020 @ 09:45:04.360	ABT101261	u-4721-232bc	British Columbia	BitLocker Drive Encryption Driver
Jul 13, 2020 @ 22:09:49.694	ABT101261	u-4721-232bc	British Columbia	BitLocker Drive Encryption Driver
Jul 10, 2020 @ 10:11:25.907	ABT101755	u-8143-01850	British Columbia	BitLocker Drive Encryption Driver
Jul 10, 2020 @ 08:33:38.583	ABT102704	u-0829-00cb6	British Columbia	BitLocker Drive Encryption Driver
Jul 10, 2020 @ 07:59:28.696	ABT102713	u-6275-61485	British Columbia	BitLocker Drive Encryption Driver
Jul 9, 2020 @ 10:10:17.997	ABT101755	u-8143-01850	British Columbia	BitLocker Drive Encryption Driver
Jul 9, 2020 @ 08:32:53.729	ABT102704	u-0829-00cb6	British Columbia	BitLocker Drive Encryption Driver

Catering to a variety of IT and security challenges

Absolute Insights for Endpoints leverages Absolute's undeletable tether at the firmware of devices, allowing for unparalleled visibility into granular asset and security datapoints, helping you to tackle a variety of IT and security related challenges.

Category	Problems Solved	Historical Trends	Historical Data Investigations
Security and Compliance	• Maintain security posture by ensuring the efficacy of critical security apps • Proactively manage data leakage risk by assessing the accumulation of sensitive data across devices • Ensure devices have the latest BIOS or OS versions installed to guard against vulnerabilities or threats	• Monitoring the health of critical security applications over time and identifying core failure reasons • Anti-malware and encryption status trends over a certain time period • Average data risk exposure across endpoints over time	• Number of devices with a specific file containing sensitive data • Devices having old Windows OS patches or BIOS versions deployed
User Behavior	• Identify suspicious device or user behavior based on device movement and user logins • Track consumption of online content to identify risks from risky or uncertified usage	• Changes in number of off-network devices connecting from a home or a public network. • Weekly web usage trends to understand the consumption of online content	• Devices with the greatest number of IP address or location changes • Users with the greatest number of logins from unique devices
Applications	• Monitor the rollout of a new application version and identify devices that have yet to be upgraded • Ensure return on software investment by monitoring app adoption • Optimize software licenses and assess yearly subscriptions • Identify applications that are not performing as expected across devices	• Weekly application installations to monitor the roll out of new applications • Weekly or monthly change in usage or adoption of an application that was recently rolled out	• Number of devices with a specific uncertified or vulnerable version of an application • Applications with the highest and lowest memory and CPU usage
Device Inventory	• Proactively identify devices with hardware issues related to battery or memory • Monitor the rollout of the latest BIOS and OS versions and identify devices that have yet to be upgraded • Identify devices being used by multiple user accounts and assess any resulting security risk • Identify devices that are not logging through valid Active Directory domains	• Changes in device battery level across endpoints over time • Weekly roll out of new BIOS or OS build versions	• Identify devices that have had high memory usage or disk utilization issues over a certain time period • Devices with external monitors or USB drives • Devices having multiple user accounts logging in to them • Number of devices in different Active Directory domains

Gain Insights Today

Absolute Insights for Endpoints is available for purchase as an add-on module and requires an existing Absolute Visibility, Control, or Resilience subscription. Contact your **Absolute Sales Account Executive** to learn more about Absolute Insights for Endpoints and get started.