



FALCON DISCOVER TRIAL GUIDE

150 MATHILDA PL SUITE 650, SUNNYVALE, CALIFORNIA 94086
TEL: (888)512-8906 FAX:(949) 417-1289
WWW.CROWDSTRIKE.COM

TABLE OF CONTENTS

- 3** INTRODUCTION
- 4** GETTING STARTED
- 5** NAVIGATING FALCON DISCOVER
- 6** APPLICATION USAGE
- 7** ASSET INVENTORY
- 10** DRIVE ENCRYPTION
- 12** ACCOUNT MONITORING
- 16** SUMMARY
- 17** ABOUT CROWDSTRIKE

INTRODUCTION

Falcon Discover™ is CrowdStrike's dynamic IT hygiene solution. CrowdStrike® Falcon Discover allows you to identify unauthorized systems and applications in real time across your environment and remediate issues quickly to improve your overall security posture. It gives you unprecedented visibility into your assets, accounts and applications. Since Falcon Discover uses the same agent as the CrowdStrike Falcon® platform, there is no additional agent to install. This means that you have always-on visibility to monitor your systems and see who has access to them.

This user guide highlights how you can use Falcon Discover to monitor all of your systems, with the added value of being able to quickly pivot to other modules directly within the Falcon platform. In this guide, we'll explore a few use cases on how Falcon Discover provides complete visibility in your entire environment.

Application Inventory: Monitor and maintain an up-to-date inventory of all applications. In this guide we will show you how to see the applications and hosts in your environment.

Asset Inventory: Identify all assets in your network and gain access to detailed information on all assets. Learn how to view lists of managed, unmanaged and unsupported assets.

Drive Encryption: Learn how to quickly identify which Windows hosts are using BitLocker disk encryption to better protect your Windows hosts.

Account Monitoring: Find all users on Windows hosts to see who is logged on. Track admin privileges, monitor password resets and see at a glance other user/logon behavior.

“

Falcon Discover allows organizations to proactively improve security posture by providing unprecedented visibility over assets, applications and accounts.

GETTING STARTED

Falcon Discover provides reporting on your entire environment. For best results, we recommend that you have the CrowdStrike agent installed on multiple systems using different operating systems and applications.

- For existing customers with 20+ agents installed, your existing agents should provide you with good reporting details, especially if you have different operating systems, servers and domain controllers under management.
- For trial customers, we recommend that you install the Falcon agent on more than one or two machines. Having servers, workstations and domain controllers as well as different operating systems covered will help give you the most complete reporting experience.

NAVIGATING FALCON DISCOVER

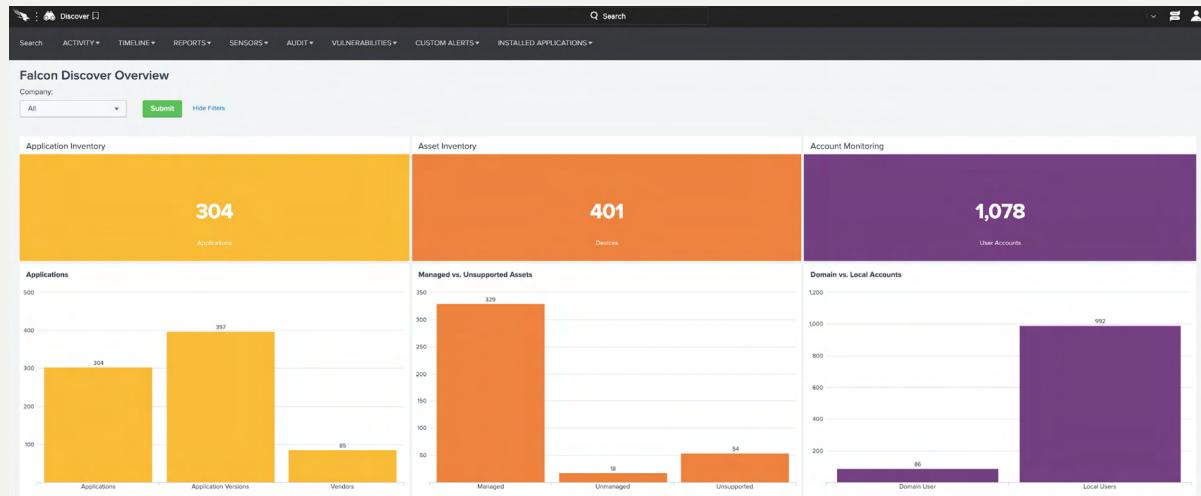
After logging in to the CrowdStrike user interface (UI), you can access Falcon Discover from the menu under the Discover icon. While you have access to explore all of the menu options, the next section will walk you through four different potential use cases.

After logging in to the CrowdStrike UI, you can access Falcon Discover by clicking on the Overview link under the Discover icon in the menu page. You will have access to explore all menu options within the Falcon Discover module.

Please note that once you install Falcon Discover, it may take up to 24 hours for the data to populate.

VIEWING YOUR ENVIRONMENT IN THE OVERVIEW DASHBOARD

The main dashboard in Falcon Discover is the Overview page. From here you can quickly see the inventory of your applications, assets and accounts. You can click each of the charts to dive into more detail.



APPLICATION USAGE

Let's look at a few ways you can view and manage the applications in your environment. To view a list of all of the applications in your environment, select the Application Inventory chart in the Overview dashboard. From here you will be taken to the Application Usage page.

138 Application Versions Used Last 7 Days							
Company #	Vendor #	Application #	Application Version #	File Name #	File Version #	Hosts (Used App) #	Hosts (Did Not Use App) #
1	_Talon 1	#Vendor	#Application	TrustedInstaller.exe	0.0	View Hosts	View Hosts
				cvtres.exe			
				spovce.exe			
2	_Talon 1	#Vendor	#Application	dnsExFiltrator.exe	0.0	View Hosts	View Hosts
3	_Talon 1	#Vendor	LocalBridge	LocalBridge.exe	18.2005.1191.0	View Hosts	View Hosts
4	_Talon 1	#Vendor	MSISummer	adisummer.exe	1.2	View Hosts	View Hosts
5	_Talon 1	#Vendor	Maps	Maps.exe	18.2006.11.0	View Hosts	View Hosts
6	_Talon 1	#Vendor	Microsoft Visual Studio	VISXAutoupdate.exe	16.5	View Hosts	View Hosts
7	_Talon 1	#Vendor	TheHunting	soundrecorder.exe	1.0	View Hosts	View Hosts
8	_Talon 1	#Vendor	UpdateServiceNameCheck	GoogleUpdate.exe	1.0	View Hosts	View Hosts
9	_Talon 1	#Vendor	nfusetcng	nfusetcng.exe	1.76	View Hosts	View Hosts
10	_Talon 1	Adobe Inc.	#Application	AdobeARMHelper.exe	1.824	View Hosts	View Hosts
				armsvc.exe	1.824	View Hosts	View Hosts
11	_Talon 1	Adobe Inc.	Adobe Acrobat Update Service	1.824	1.824	View Hosts	View Hosts
12	_Talon 1	Adobe Inc.	Adobe Reader and Acrobat Manager	AdobeARM.exe	1.824	View Hosts	View Hosts
13	_Talon 1	Adobe Systems Incorporated	Adobe Acrobat	ReaderCEF.exe	20.12	View Hosts	View Hosts
14	_Talon 1	Adobe Systems Incorporated	Adobe Acrobat	reader_11.exe	15.6	View Hosts	View Hosts
15	_Talon 1	Adobe Systems Incorporated	Adobe Acrobat	reader_11.exe	29.9	View Hosts	View Hosts
16	_Talon 1	Adobe Systems Incorporated	Adobe Acrobat Reader DC	AcroD32.exe	20.13	View Hosts	View Hosts
17	_Talon 1	Adobe Systems Incorporated	Adobe Acrobat Reader DC	AcroD32.exe	20.9	View Hosts	View Hosts
18	_Talon 1	Adobe Systems Incorporated	Adobe Flash Player Update Service	FlashplayerupdateService.exe	18.0	View Hosts	View Hosts
19	_Talon 1	Adobe Systems, Incorporated	Adobe Genuine Software Integrity Service	AGDService.exe	7.1	View Hosts	View Hosts
20	_Talon 1	Adobe Systems, Incorporated	Adobe Genuine Software Service	AGDService.exe	7.1	View Hosts	View Hosts

On this page you will see a number of charts across the top providing detailed information about the applications in your environment. Within this page you are able to filter search results using the search fields at the top, or by selecting one of the entries listed below the charts. Each one of these charts is clickable to dive into to see data around:

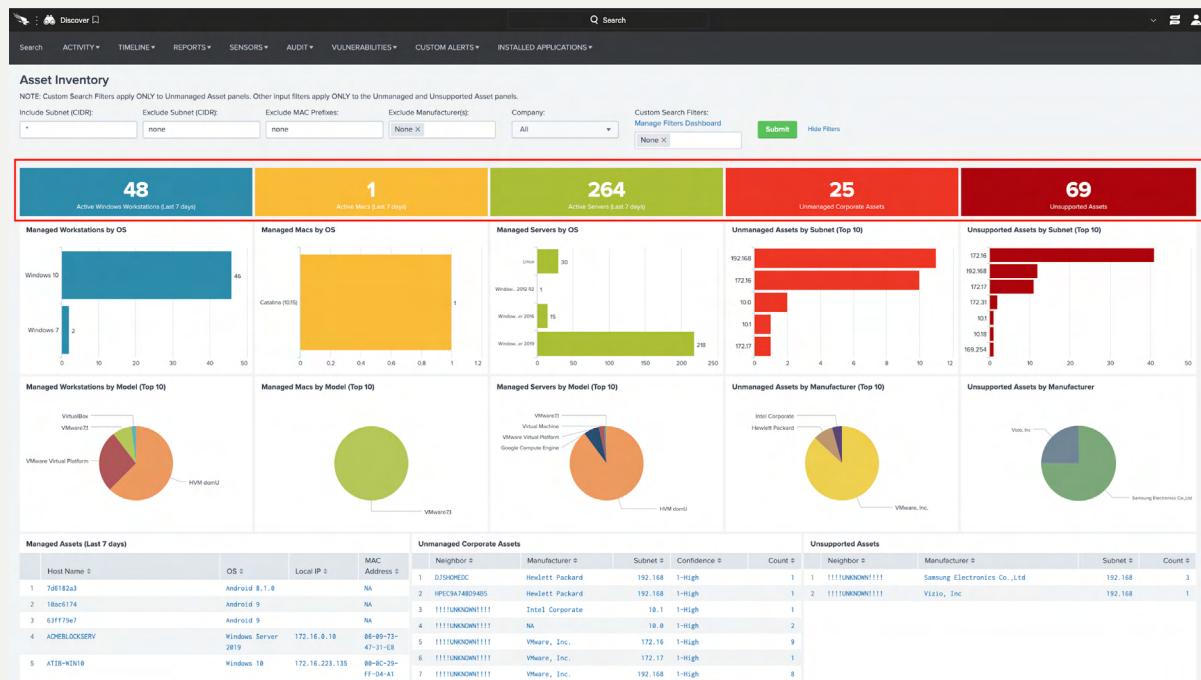
- Applications in your environment
- Application versions
- Application vendors
- Application files
- Any suspicious applications

ASSET INVENTORY

To learn details about the assets in your environment, select the Asset Inventory chart from the Overview page, or navigate to it by clicking on the Asset Inventory link under the Discover icon in the Falcon menu.

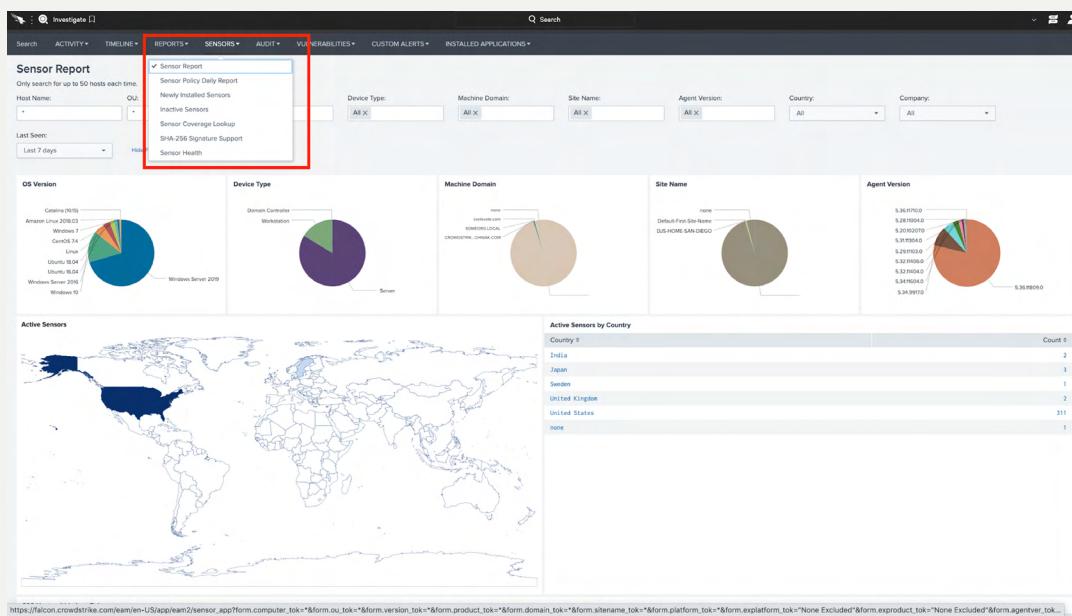
On this dashboard you are able to view managed, unmanaged and unsupported assets. Again, across the top of the dashboard are several clickable charts that allow you to filter your inventory search by:

- Active Windows workstations
- Active Mac workstations
- Active servers
- Unmanaged assets
- Unsupported assets



You can filter your search results by using the search fields above the charts.

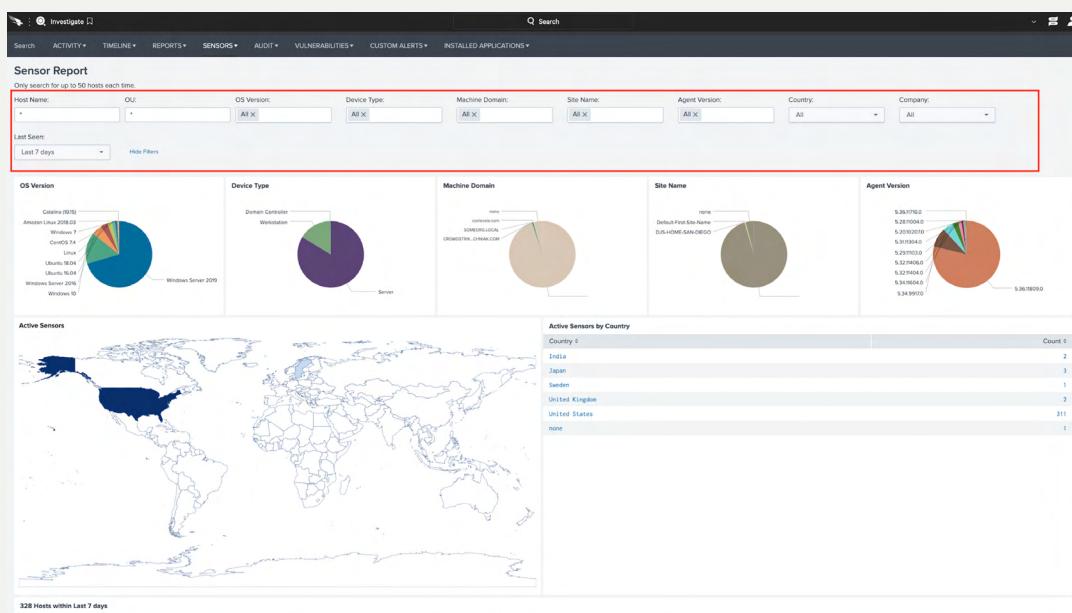
Please note that using the search filters within this chart will only apply to the Unmanaged Asset panels. To get a complete view of all assets covered by Falcon sensors, select the Sensors tab on the top menu and click on Sensor Report. This will take you to a visual chart of which sensors are installed globally in your environment. You will have the ability to further your search using the filters at the top of the page.



The screenshot shows the Falcon Discover interface with the 'Sensor Report' selected in the top navigation bar. A red box highlights the 'REPORTS' dropdown menu, which is open to show the 'Sensor Report' option. Below the menu, there are search filters for Host Name, Last Seen, and various agent settings. The main content area contains five charts: OS Version (a pie chart showing a large majority of Windows Server 2019), Device Type (a pie chart showing a large majority of Workstation), Machine Domain (a pie chart showing a large majority of CLOUDFRONT.CHINAK.COM), Site Name (a pie chart showing a large majority of Default-Fail-Site-Name/DUS-HOME-SAN-DIEGO), and Agent Version (a pie chart showing a large majority of 5.36.9910). Below these charts is a world map showing active sensors. A table titled 'Active Sensors by Country' lists the following data:

Country	Count
India	2
Japan	3
Sweden	1
United Kingdom	2
United States	311
none	1

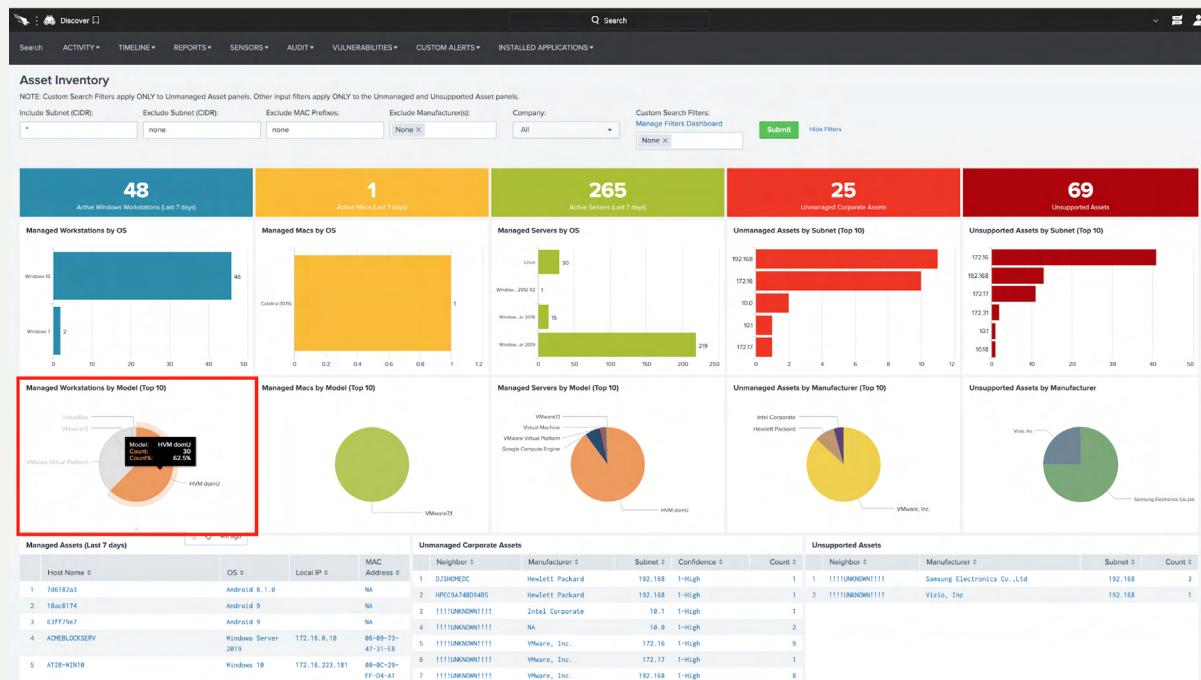
At the bottom of the page, the URL is visible: https://falcon.crowdstrike.com/eam/en-US/app/eam2/sensor_appForm/computer_tok=&form.ou_ou_tok=&form.version_tok=&form.product_tok=&form.domain_tok=&form.sitename_tok=&form.platform_tok=&form.explatform_tok=&None Excluded&form.exproduct_tok=&None Excluded&form.agentver_tok...



This screenshot shows the same Falcon Discover interface as the previous one, but with a red box highlighting the search filters at the top of the page. The filters include Host Name, Last Seen, and various agent settings. The main content area contains the same five charts and world map as the first screenshot. The 'Active Sensors by Country' table is identical to the one in the first screenshot.

At the bottom of the page, the URL is visible: https://falcon.crowdstrike.com/eam/en-US/app/eam2/sensor_appForm/computer_tok=&form.ou_ou_tok=&form.version_tok=&form.product_tok=&form.domain_tok=&form.sitename_tok=&form.platform_tok=&form.explatform_tok=&None Excluded&form.exproduct_tok=&None Excluded&form.agentver_tok...

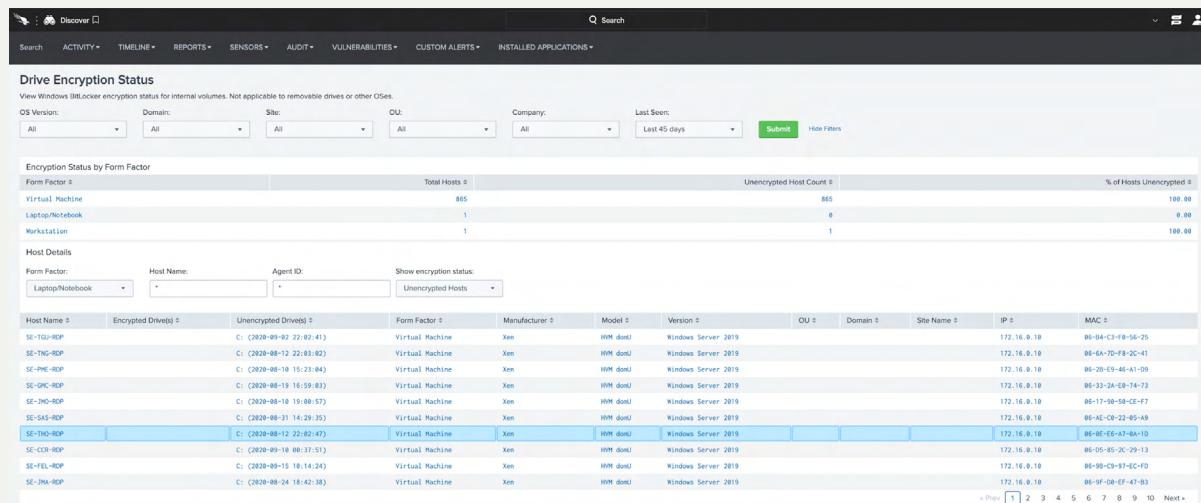
By hovering over the pie charts within the Asset Inventory dashboard, you can get additional quick stats about the model or manufacturer of an asset including count and count percentage. Export and Refresh buttons below each chart allow you to share and refresh the data respectively.



The Asset Inventory page gives you visibility on all managed, unmanaged and unsupported assets within your environment. From this page you can look into specific hosts indicating suspicious activity, or get detailed data around unmanaged corporate assets.

DRIVE ENCRYPTION

To find out which Windows hosts are using BitLocker encryption, navigate to the Drive Encryption dashboard by clicking on the link under the Discover icon in the menu.



Drive Encryption Status

View Windows BitLocker encryption status for internal volumes. Not applicable to removable drives or other OSes.

OS Version:	Domain:	Site:	OU:	Company:	Last Seen:	Submit	Hide Filters				
All	All	All	All	All	Last 45 days						
Encryption Status by Form Factor											
Form Factor #	Total Hosts #	Unencrypted Host Count #	% of Hosts Unencrypted #								
Virtual Machine	865	865	100.00								
Laptop/Notebook	1	0	0.00								
Workstation	1	1	100.00								
Host Details											
Form Factor:	Host Name:	Agent ID:	Show encryption status:	Unencrypted Hosts							
Laptop/Notebook	*	*	Unencrypted Hosts								
Host Name #	Encrypted Drive(s) #	Unencrypted Drive(s) #	Form Factor #	Manufacturer #	Model #	Version #	OU #	Domain #	Site Name #	IP #	MAC #
SE-TGU-ROP	C: (2020-09-02 22:02:41)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-04-C3-FB-56-25
SE-TNG-ROP	C: (2020-09-12 22:03:42)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-6A-7D-F8-2C-41
SE-PME-ROP	C: (2020-09-18 15:23:04)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-20-E9-46-A1-09
SE-GPC-ROP	C: (2020-09-19 16:59:03)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-33-2A-E8-74-73
SE-ZHD-ROP	C: (2020-09-19 19:00:57)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-17-90-59-01-F7
SE-SAS-ROP	C: (2020-09-31 14:29:35)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-AE-C9-22-01-69
SE-THO-ROP	C: (2020-09-12 22:02:47)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-0E-E8-A7-04-10
SE-CCR-ROP	C: (2020-09-18 09:37:51)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-05-85-2C-29-13
SE-FEL-ROP	C: (2020-09-19 10:14:24)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-90-C9-F7-41-F0
SE-JMA-ROP	C: (2020-09-24 18:42:38)		Virtual Machine	Xen	HW domU	Windows Server 2019				172.16.0.10	06-9F-0B-F7-41-B3

From here you can filter and search by Windows operating version, domain, site, organizational unit and company. Please note that this is only available for Windows operating systems.

Selecting any of the entries below Encryption Status by Form Factor will toggle down additional data around hosts.

Drive Encryption Status

View Windows BitLocker encryption status for internal volumes. Not applicable to removable drives or other OSes.

OS Version: Domain: Site: OU: Company: Last Seen:

Encryption Status by Form Factor

Form Factor	Total Hosts	Unencrypted Host Count	% of Hosts Unencrypted
Virtual Machine	836	836	100.00
Workstation	4	4	100.00

Host Details

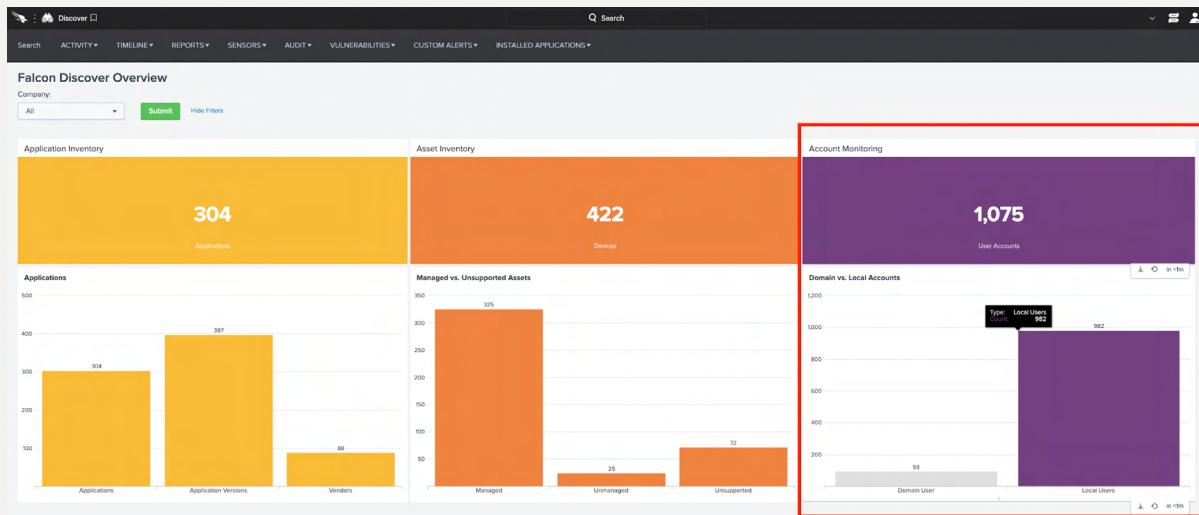
Form Factor: Host Name: Agent ID: Show encryption status:

Host Name	Encrypted Drive(s)	Unencrypted Drive(s)	Form Factor	Manufacturer	Model	Version	OU	Domain	Site Name	IP	MAC
SE-TNG-RDP	C: (2020-08-12 22:03:02)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-6A-7D-F8-2C-41
SE-PHE-RDP	C: (2020-08-18 15:33:04)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-2B-09-40-A1-09
SE-GHC-RDP	C: (2020-08-19 16:59:03)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-33-2A-00-74-73
SE-AST-RDP	C: (2020-07-14 22:07:18)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-45-0B-1D-05-28
SE-TMD-RDP	C: (2020-08-10 19:00:57)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-17-00-59-CE-17
SE-CAH-RDP	C: (2020-07-29 12:19:18)		Virtual Machine	Xen	VM domU	Windows Server 2019	none	none	none	172.16.8.18	06-FD-50-0C-0F-44
SE-DEE-RDP	C: (2020-07-27 17:51:34)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-58-10-E3-5A-2A
SE-PHE-RDP	C: (2020-07-22 19:34:01)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-4E-CE-12-8D-08
SE-NDE-RDP	C: (2020-07-25 12:44:34)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-21-0D-39-24-CC
SE-THO-RDP	C: (2020-08-12 22:02:47)		Virtual Machine	Xen	VM domU	Windows Server 2019				172.16.8.18	06-9E-65-A7-0A-10

x prior

ACCOUNT MONITORING

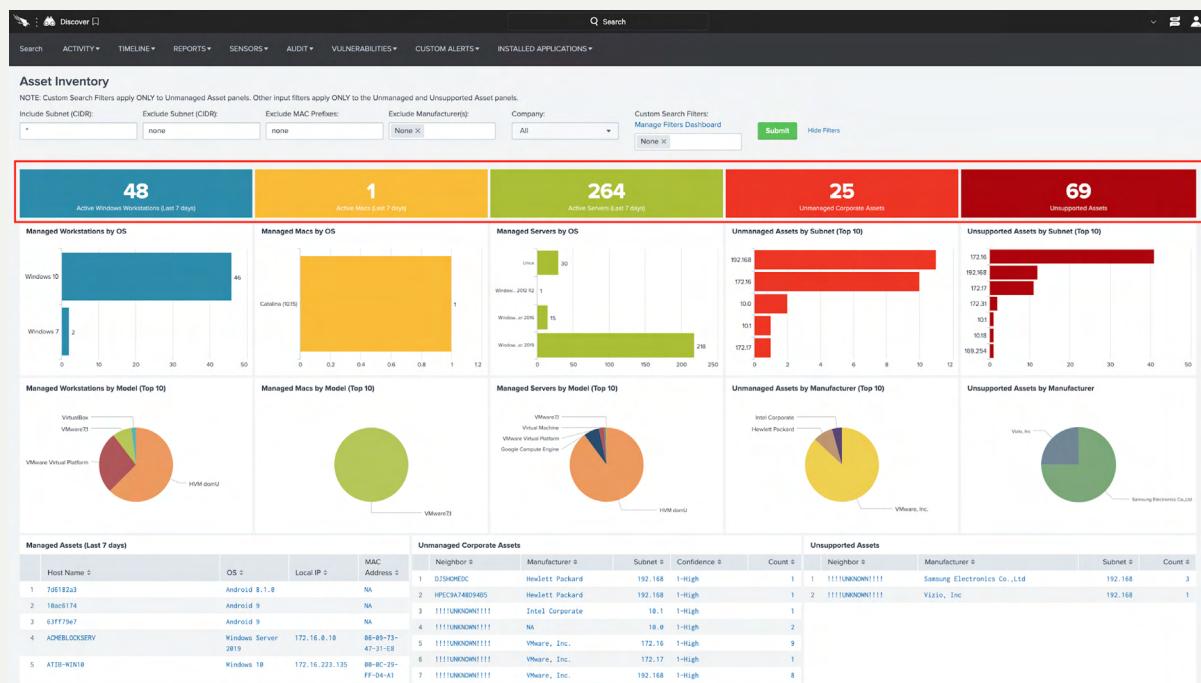
Last but not least, Falcon Discover provides you the ability to view detailed information around user accounts on Windows hosts. You are able to view the Account Monitoring dashboard either by clicking on the Account Monitoring chart in the Overview dashboard or by clicking the Account Monitoring link under the Discover icon in the menu.



In this dashboard you can see quick data:

- The number of domain accounts
- Average number of months since a password change across domain accounts
- The number of local accounts
- Average number of months since a password change across local accounts

The search fields below the charts allow you to filter by user name, security identifier (SID), account type, admin privilege and logon type.



Account Monitoring

Domain Accounts by Password Last Set

Local Accounts by Password Last Set

User Name: UserSID: Account Type: Admin Privileges: Logon Type: Last Logged On: Last 7 Days:

93 User Accounts

Company #	User #	User Name #	UserSID #	Account Type #	Local Admin Privileges #	Logon Type #	Last Logged On Host #	Last Logged On #	Password Last Set #	Months since Password Last Set #	
1	Talon 1	CROWNSTRIKEBERTMAR_GILFOYLE	BERTRAM_GILFOYLE	S-1-5-21-1785701866-175991678-242629327-1111	Domain User	Yes	Interactive	CS-SE-025-W10P	2020-08-28 07:11:59	2019-01-11 05:19:31	28
2	Talon 1	CROWNSTRIKEVINESH_CHOTAI	DINESH_CHOTAI	S-1-5-21-1785701866-175991678-242629327-1112	Domain User	Yes	Interactive	CS-SE-025-W10P	2020-08-28 07:11:59	2019-01-11 05:19:31	28
3	Talon 1	CROWNSTRIKELEIFUR_HENDRICKS	ERLICH_HENDRICKS	S-1-5-21-1785701866-175991678-242629327-1113	Domain User	Yes	Interactive	CS-SE-025-W10P	2020-08-28 07:11:59	2019-01-11 05:19:31	28
4	Talon 1	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	S-1-5-21-1785701866-175991678-242629327-1114	Domain User	Yes	Interactive	CS-SE-025-W10P	2020-08-28 07:11:59	2019-01-11 05:21:22	28
5	Talon 1	SE-BDO-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-1785701866-175991678-242629327-1115	Local User	Yes	Terminal Server	FC-051-40P	2020-08-11 23:12:06	2020-08-13 23:18:42	0
6	Talon 1	SE-BDO-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-1787877737-2378896273-27413271-509	Local User	Yes	Terminal Server	SE-BDO-RDP	2020-08-19 10:33:42	2020-08-19 15:24:18	0
7	Talon 1	SE-APR-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-33514415-488979379-12289516-508	Local User	Yes	Terminal Server	SE-APR-RDP	2020-08-17 04:51:13	2020-08-17 02:28:45	0
8	Talon 1	SE-ASR-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-3052746873-34263525-13980278-508	Local User	Yes	Terminal Server	SE-ASR-RDP	2020-08-14 17:33:37	2020-08-27 21:47:15	1
9	Talon 1	SE-BDO-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-147928891-297778881-18521249-508	Local User	Yes	Terminal Server	SE-BDO-RDP	2020-08-14 18:08:42	2020-08-14 18:08:18	0
10	Talon 1	SE-BDO-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-28291859-122713259-205527887-508	Local User	Yes	Terminal Server	SE-BDO-RDP	2020-08-17 13:57:36	2020-08-17 13:41:52	0
11	Talon 1	SE-BDO-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-31822897-23788432-288472863-508	Local User	Yes	Terminal Server	SE-BDO-RDP	2020-08-17 14:36:39	2020-08-17 14:32:58	0
12	Talon 1	SE-BTA-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-339779461-23313782-1111717-508	Local User	Yes	Terminal Server	SE-BTA-RDP	2020-08-18 16:08:14	2020-08-18 17:44:19	0
13	Talon 1	SE-BTA-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-12222447-395308782-388451339-508	Local User	Yes	Terminal Server	SE-BTA-RDP	2020-08-19 10:31:16	2020-08-19 15:31:31	0
14	Talon 1	SE-BTA-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-42375808-246481912-238062733-508	Local User	Yes	Terminal Server	SE-BTA-RDP	2020-08-19 16:21:08	2020-08-06 17:36:04	0
15	Talon 1	SE-CAH-REPLACEMENTADMINISTRATOR	ADMINISTRATOR	S-1-5-21-1588497881-2582098417-46298239-508	Local User	Yes	Terminal Server	SE-CAH-RDP	2020-08-14 09:00:48	2020-08-13 23:14:28	0

Clicking on any one of the user accounts below the search fields will lead you to an Account Details page. On this page you will see added details for the user you have selected. Specifically, the charts across the top offer information about the number of hosts currently logged on as well as the number of logon activities.

Account Details

User Name: Logon Domain: Company: Time range: Last 30 days: Submit Hide Filters

Logon Activities by Logon Type

Logon Activities

Account Details

User #	User Name #	User Name #	Account Type #	Local Admin Privileges #	Last Logged On Host #	Last Logged On #	Password Last Set #	Months since Password Last Set #
1	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Domain User	Yes	CS-SE-025-W10P	2020-08-28 05:32:59	2019-01-11 05:21:22	28
2	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-19 05:32:59	2020-08-19 05:33:24	00:00:24.825
3	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-17 05:32:57	2020-08-17 05:33:22	00:00:24.939
4	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-16 05:32:57	2020-08-16 05:33:21	00:00:21.548
5	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-15 05:32:57	2020-08-15 05:33:20	00:00:21.772
6	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-14 05:32:55	2020-08-14 05:33:21	00:00:25.769
7	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-13 05:32:54	2020-08-13 05:33:28	00:00:26.111
8	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-12 05:32:54	2020-08-12 05:33:20	00:00:25.666
9	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-11 05:32:54	2020-08-11 05:33:21	00:00:27.495
10	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-10 05:32:52	2020-08-10 05:33:18	00:00:28.897
11	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-09 05:32:52	2020-08-09 05:33:16	00:00:24.385
12	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-08 05:32:50	2020-08-08 05:33:12	00:00:24.975
13	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-07 05:32:50	2020-08-07 05:33:15	00:00:24.692
14	CROWNSTRIKELEIFUR_HENDRICKS	RICHARD_HENDRICKS	Interactive	CROWNSTRIKE	CS-SE-025-W10P	2020-08-06 05:32:49	2020-08-06 05:33:14	00:00:24.945

You can get to the User Search page by clicking on an entry in the Logon History section. The User Search page will allow you to investigate the user in question. The first chart shows Detection History in the last 7 days for the user you've searched for. It offers details on where the detection was sourced, a description of the detection, its severity, detection counts and other information displayed on the right of the chart. (Please note that the User Search page is a function of Falcon Insight.)

Scroll down in this page to see additional sections on:

- Unresolved detections in the last 7 days
- User logon activities (for Windows users only)
- Process executions
- Admin tool usage

The account monitoring functionality of Falcon Discover provides you with detailed account user information for research and analysis at your fingertips. Use it to home in on suspicious activities.

SUMMARY

Falcon Discover enables you to quickly view the assets, applications and accounts within your environment by providing comprehensive data and interactive dashboards. Quickly home in on suspicious activity or use it to uncover unprotected systems. Learn which applications are being leveraged and where privileged accounts are being used. Real-time and historical visibility provides a comprehensive picture of your assets and applications.

To learn how to add Falcon Discover to your console, please reach out to your account representative or email support@crowdstrike.com.

ADDITIONAL RESOURCES

[Falcon Discover User Guide](#)

[Falcon Discover Demo Video](#)

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

There's only one thing to remember about CrowdStrike: **We stop breaches.**