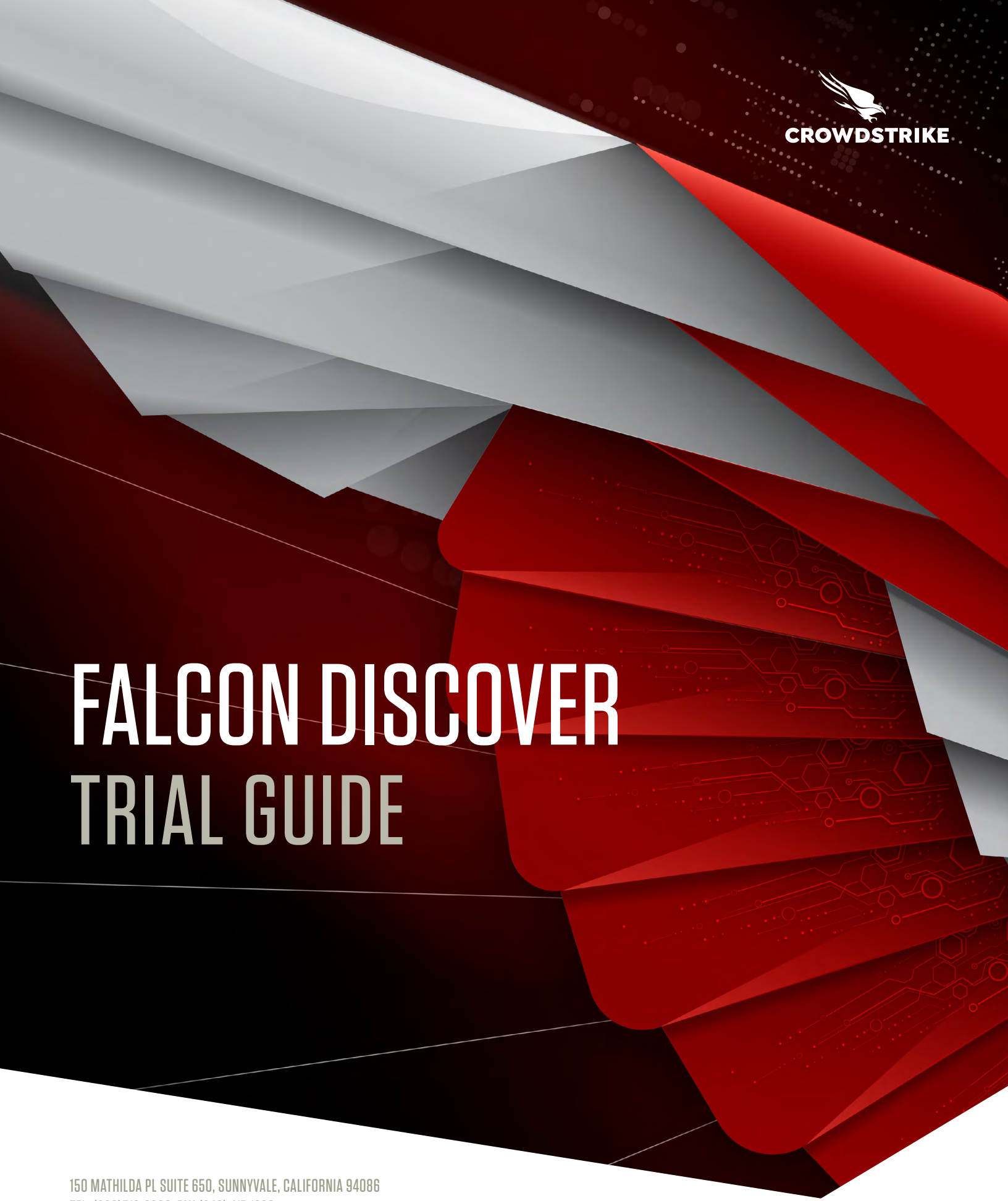


FALCON DISCOVER
TRIAL GUIDE

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

TABLE OF CONTENTS

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

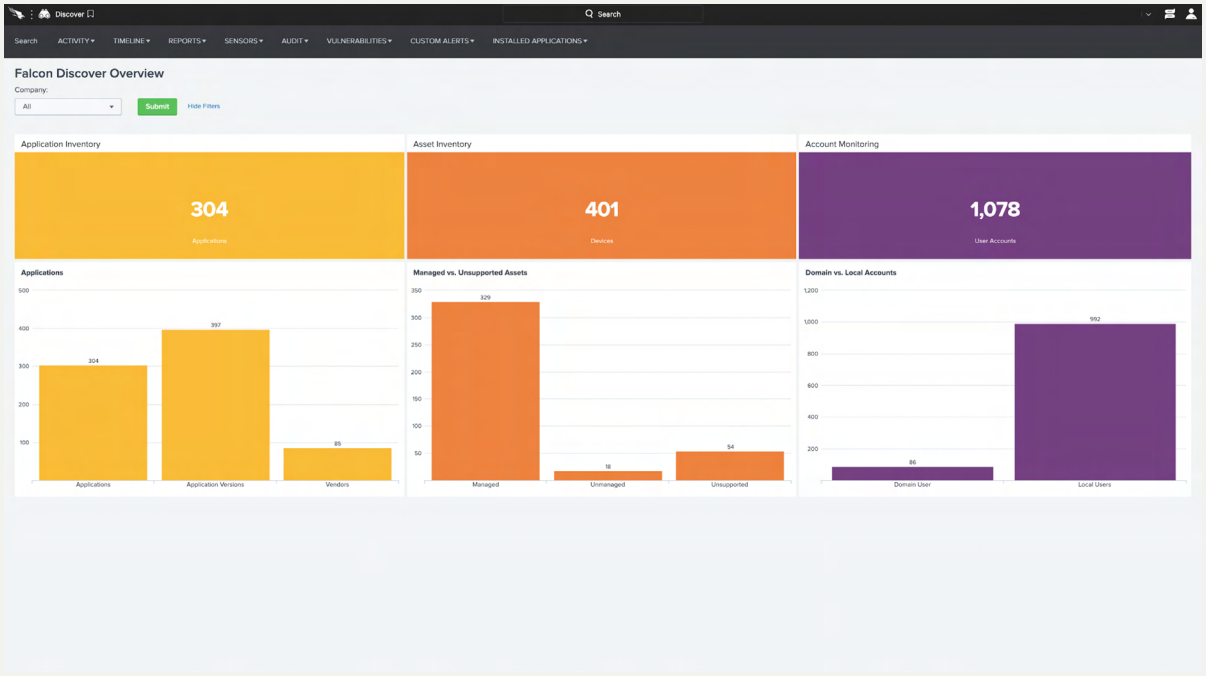
After logging in to the CrowdStrike user interface (UI), you can access Falcon Discover from the menu under the Discover icon. While you have access to explore all of the menu options, the next section will walk you through four different potential use cases.

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.

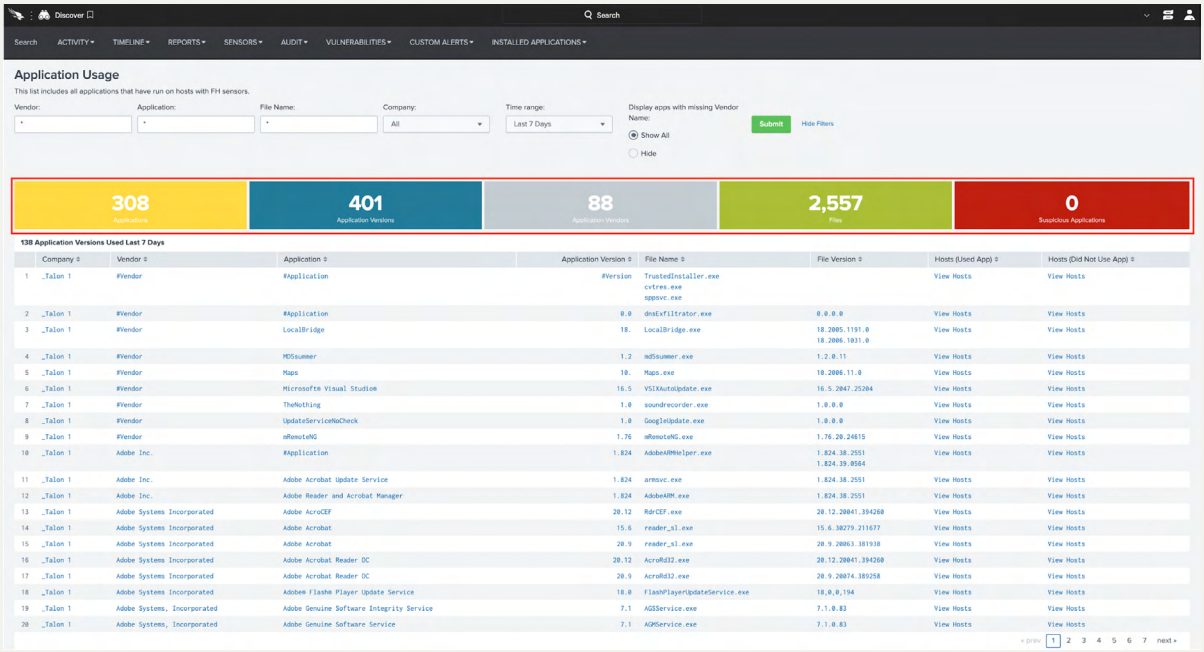
VIEWING YOUR ENVIRONMENT IN THE OVERVIEW DASHBOARD

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.



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:

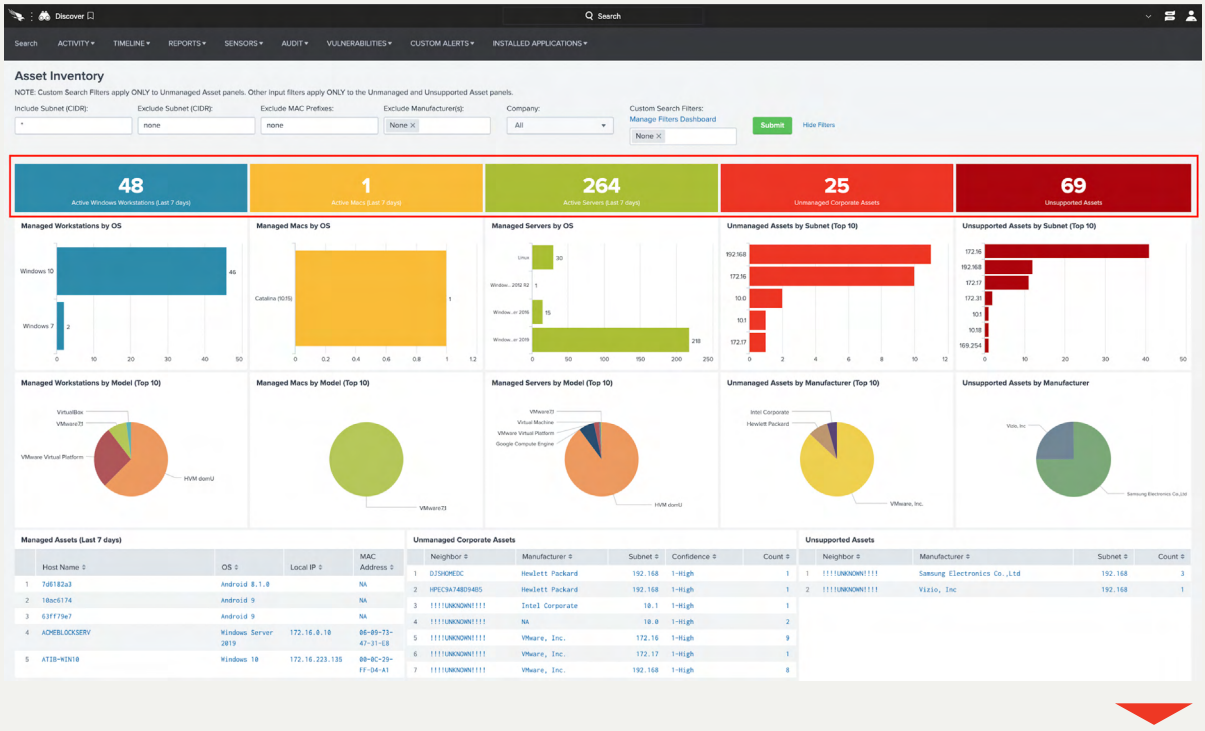
- Applications in your environment
- Application versions
- Application vendors
- Application files
- Any suspicious applications

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.

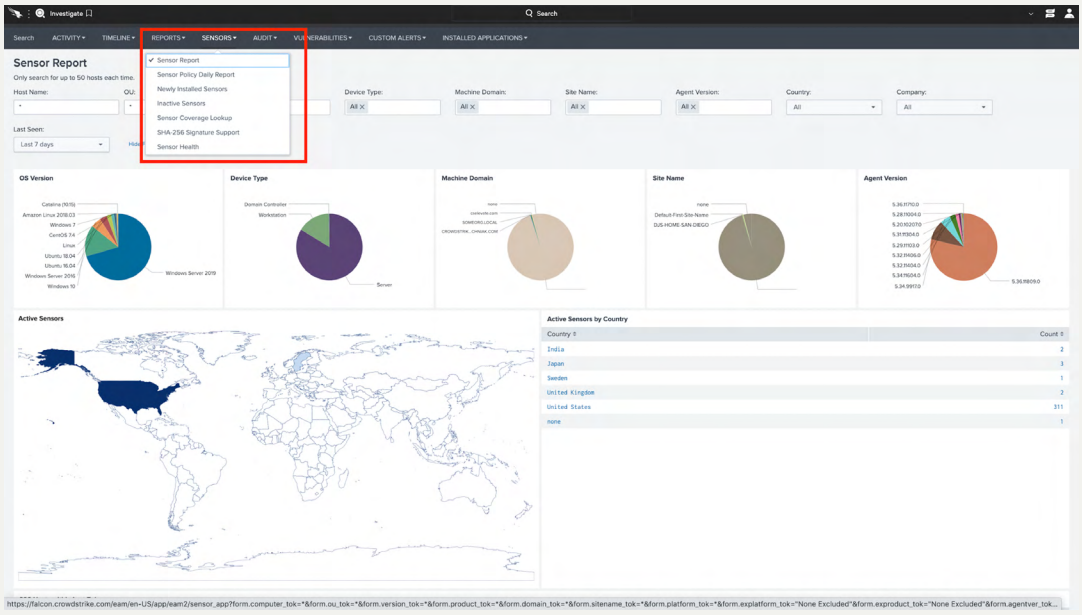
On this dashboard you are able to view managed, unmanaged and unsupported assets. Again, across the top of the dashboard are several clickable charts that allow you to filter your inventory search by:

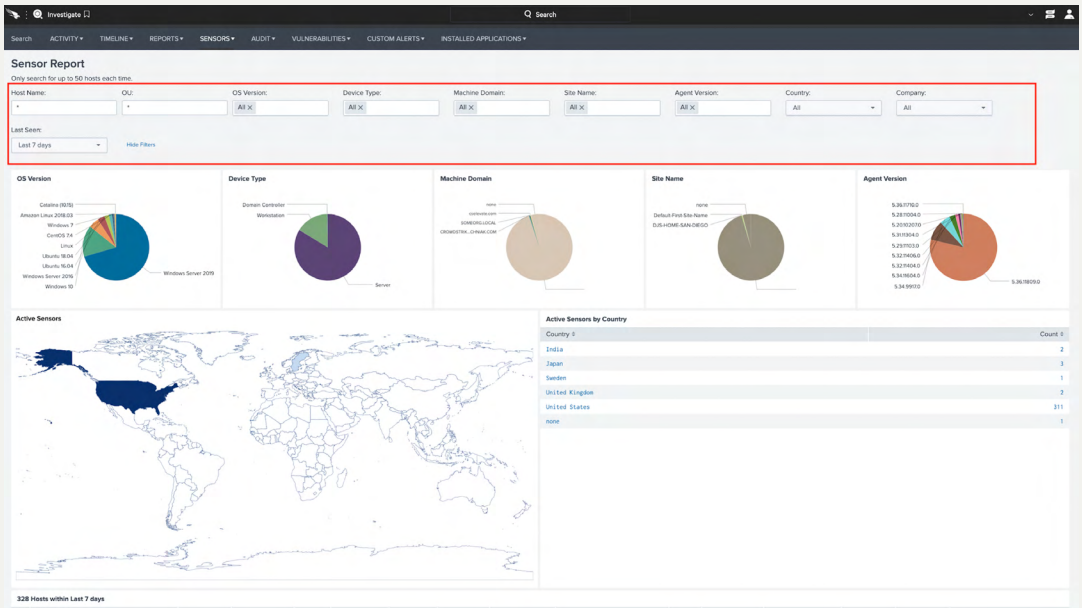
- Active Windows workstations
- Active Mac workstations
- Active servers
- Unmanaged assets
- Unsupported assets



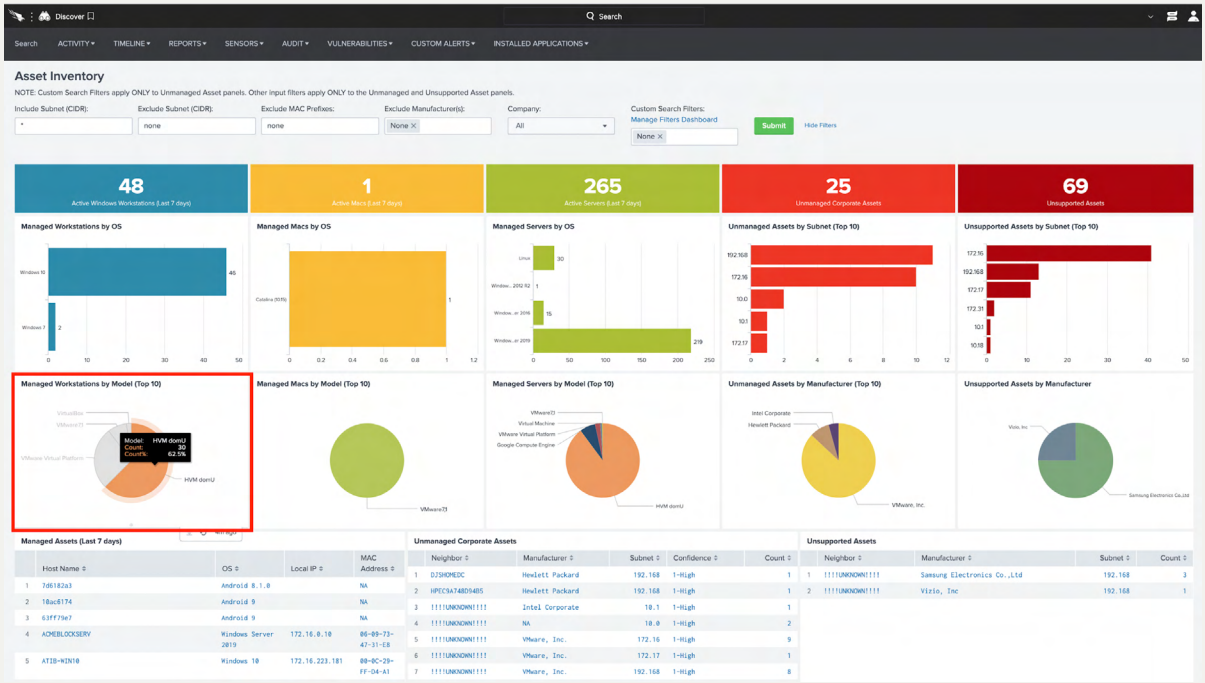
You can filter your search results by using the search fields above the charts.

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.





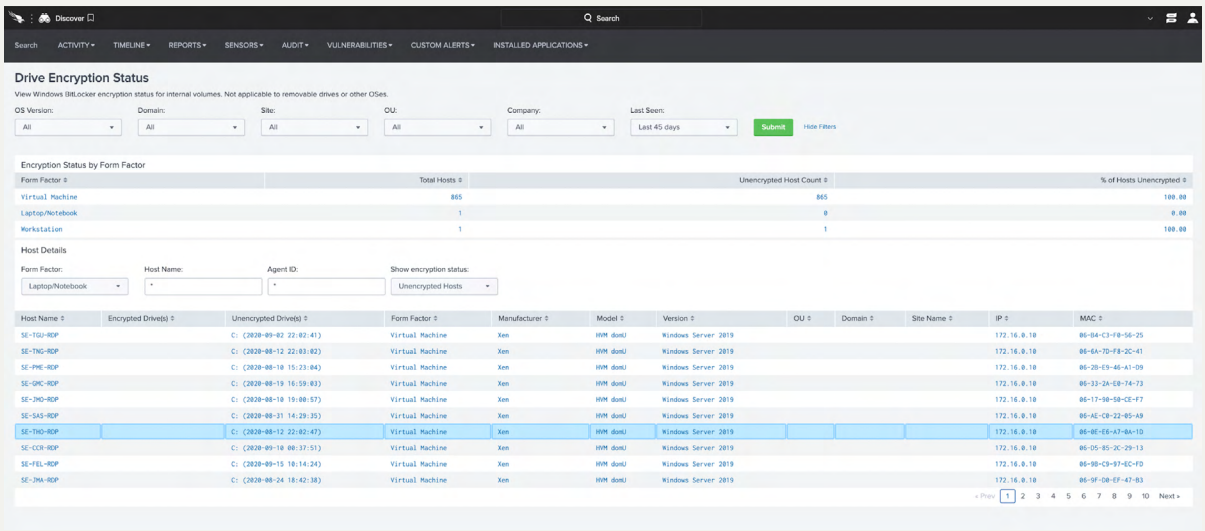
By hovering over the pie charts within the Asset Inventory dashboard, you can get additional quick stats about the model or manufacturer of an asset including count and count percentage. Export and Refresh buttons below each chart allow you to share and refresh the data respectively.



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.

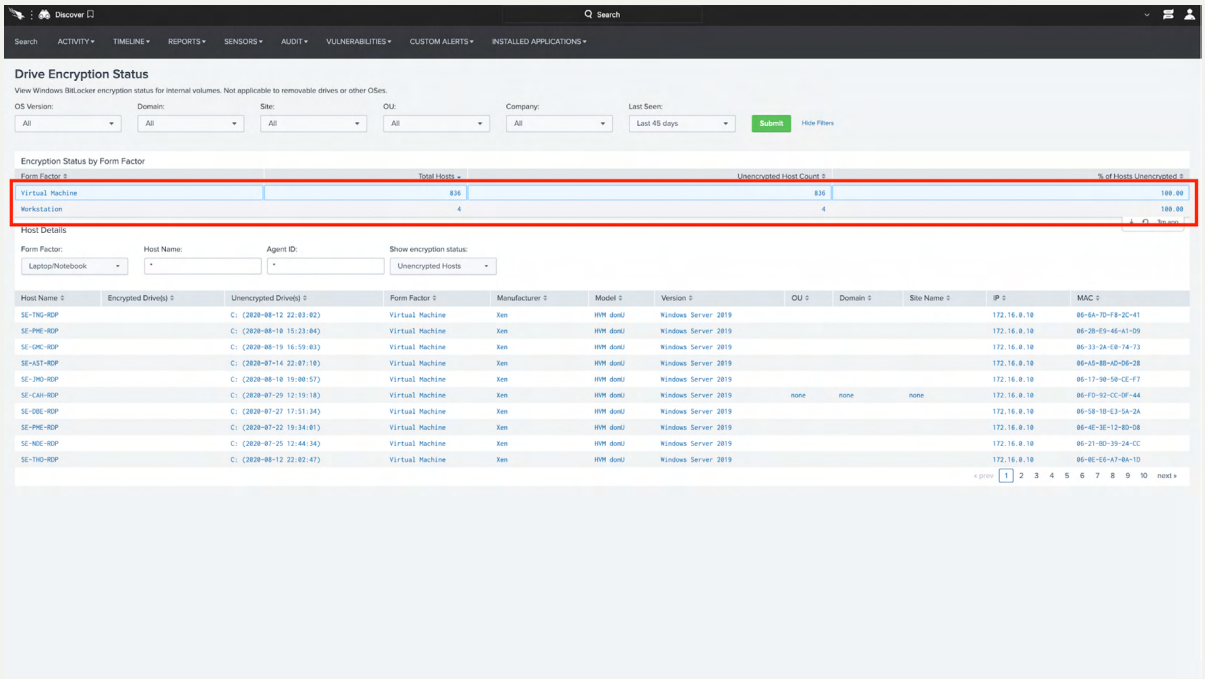
DRIVE ENCRYPTION

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.



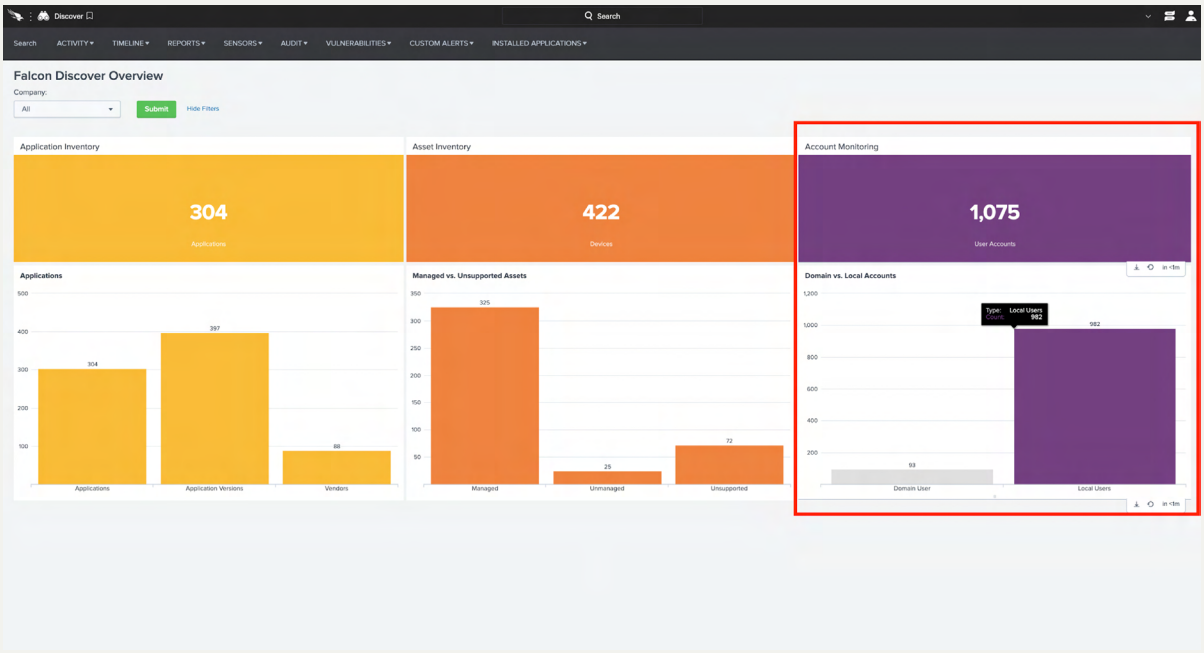
From here you can filter and search by Windows operating version, domain, site, organizational unit and company. Please note that this is only available for Windows operating systems.

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



ACCOUNT MONITORING

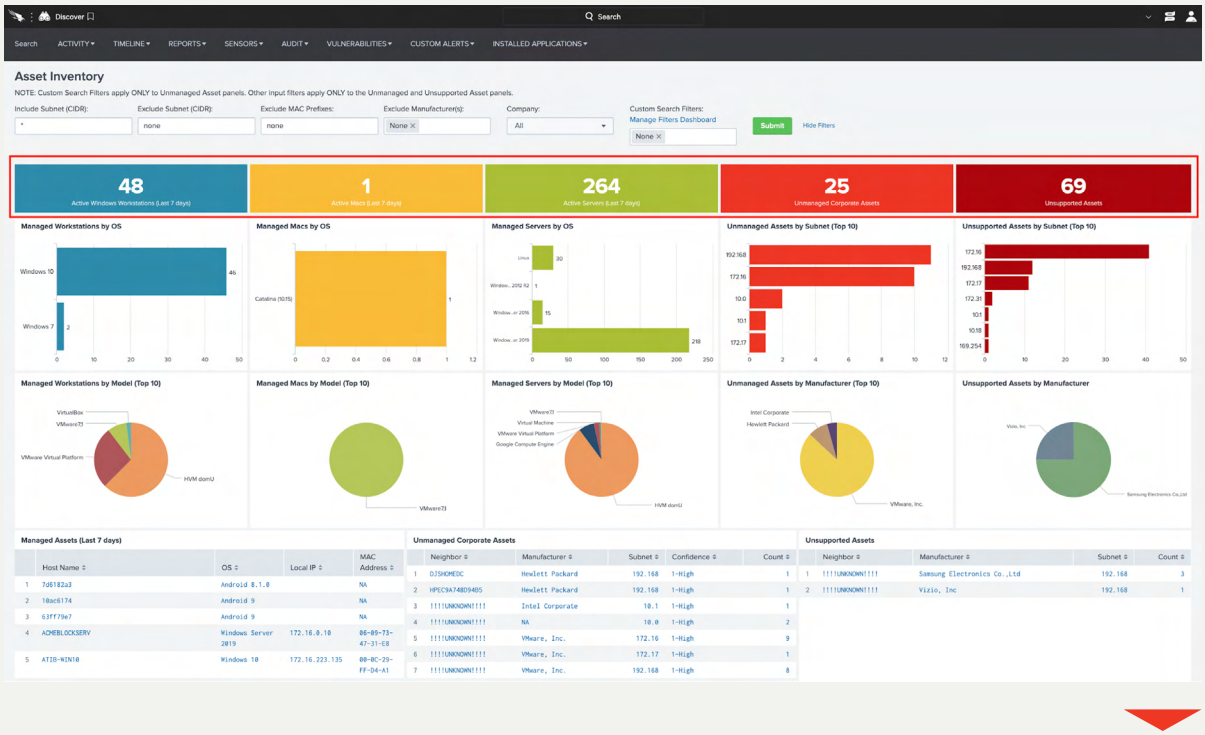
Last but not least, Falcon Discover provides you the ability to view detailed information around user accounts on Windows hosts. You are able to view the Account Monitoring dashboard either by clicking on the Account Monitoring chart in the Overview dashboard or by clicking the Account Monitoring link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

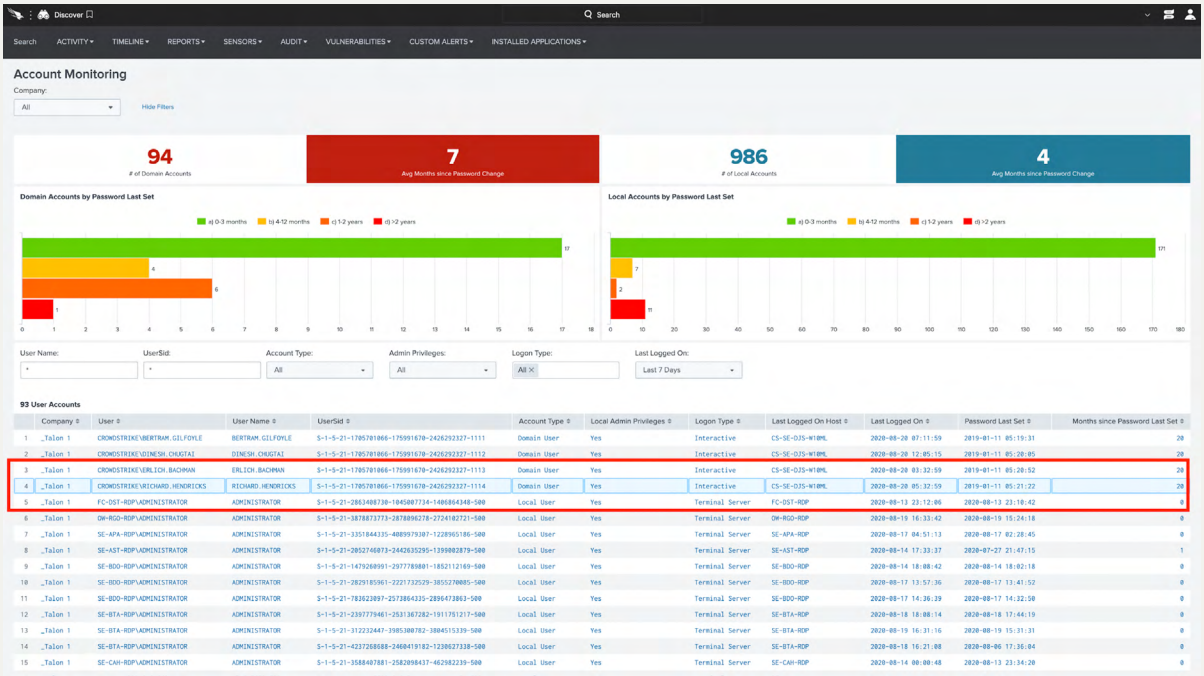


In this dashboard you can see quick data:

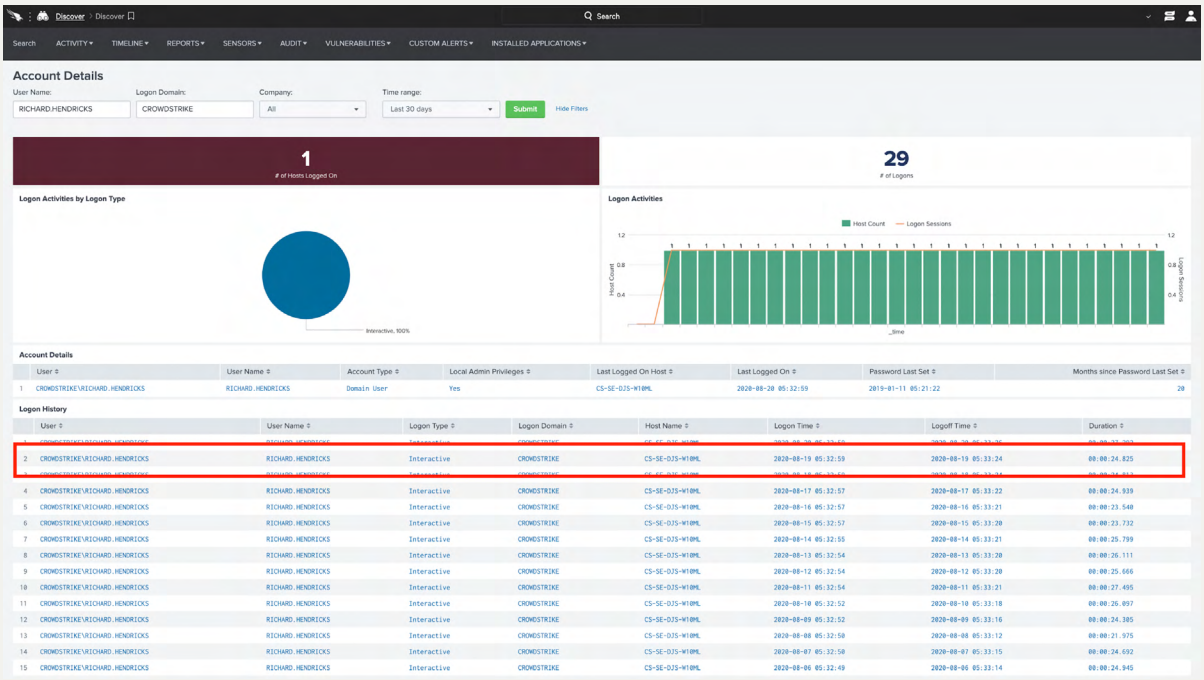
- The number of domain accounts
- Average number of months since a password change across domain accounts
- The number of local accounts
- Average number of months since a password change across local accounts

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





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.



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.**