CROWDSTRIKE

SOLUTION BRIEF

FALCON DISCOVER FOR AWS

Enabling your migration to AWS with real-time visibility and protection for Amazon Elastic Compute Cloud (EC2)

The advent of cloud technologies brings the opportunity to store, process and distribute vast quantities of data at the push of a button. Amazon Web Services (AWS) has been at the forefront of making this a reality. Organizations are increasingly moving mission-critical applications and data into AWS and taking advantage of the massive compute power of Amazon EC2.

Many of today's organizations maintain environments that are a combination of on-premises, virtual, and public cloud data center solutions, but such environments are dynamic and can pose unique security problems. The ability to scale compute power elastically and ephemerally within EC2 brings with it tremendous operational and business gains, however, practical security considerations are critical. Gaining comprehensive visibility and insight are key to maintaining an adequate security posture, but doing so is not without challenges:

- **Discoverability** — Organizations want to quickly and efficiently discover all EC2 instances and identify unprotected / unmanaged assets, allowing them to be put under management as needed.
- **Context** — As analysts triage detections, they may lack appropriate context about EC2 instances and need answers to questions such as: Is this system internet accessible? Does it have IAM roles applied with elevated privileges? Is it on the same VPC as other critical assets?
- **Consistency** — As organizations implement hybrid data centers, with workloads running on-premises and in the cloud, maintaining consistent security becomes difficult. Organizations need visibility and control over their endpoints whether they are running on-premises or as an EC2 instance in AWS.
- **Efficiency** — Time is a critical resource for operations and security teams because too often they find themselves having to pivot across a variety of tools and workflows, as they attempt to span physical, virtual and cloud environments. Ideally, teams want one tool that allows them to span their existing on-premises endpoints and Amazon EC2 instances, quickly and effectively.
- **Ease of deployment** — Security needs to match the speed and agility of DevOps. Visibility of an EC2 instance needs to be achieved instantaneously without having to install yet another agent and removing the need for DevOps to implement install scripts, etc.

FALCON DISCOVER FOR AWS SOLUTION BRIEF

REAL-TIME VISIBILITY AND CONTROL OF YOUR AMAZON EC2 INSTANCES

CrowdStrike® Falcon Discover™ for AWS provides extensive and detailed visibility over EC2 instances. It quickly enumerates existing EC2 deployments across all regions (including instances without the Falcon agent installed) and subsequently monitors cloud trail logs for any modifications to the environment. The data captured is presented in a dashboard in the Falcon Management Console, allowing users to quickly identify all EC2 assets running across all AWS accounts and regions in one centralized view. This dashboard will also highlight instances that do not have Falcon installed, allowing customers to quickly identify security gaps. In addition, rich AWS-specific context will be presented to allow for timely triaging and response to security events on EC2 instances.

USE CASE: GAIN ADDITIONAL CONTEXT SURROUNDING ALERTS

Challenge:	Typically, Amazon EC2 instances are running critical applications. When responding to an alert, analysts need a more complete picture of the impacted system.
Solution:	In the Falcon detections app, you can identify an alert on a server, drill into the alert, pivot into host details and highlight all the AWS information that's available, for example: ■ Who is the account owner of this system? ■ Is this system internet accessible? ■ Does it have IAM roles applied with elevated privileges? ■ Is it on the same VPC as other critical assets? ■ What are the rules of the security group associated with this instance? Armed with this information, you can take the appropriate action to deal with the alert.
Benefit:	The ability to make the appropriate triage and remediation actions based on complete information leads to accurate and faster decisions. This ensures that business operations are not negatively impacted and that an advanced persistent threat (APT) doesn't have time to spread laterally.

USE CASE: FINDING UNPROTECTED AMAZON EC2 INSTANCES

Challenge:	Organizations can quickly deploy instances, however, their ephemeral nature can make it difficult to quickly and efficiently discover all EC2 instances and identify unprotected / unmanaged assets.
Solution:	Falcon Discover for AWS quickly enumerates existing EC2 deployments across all regions — including instances without the Falcon sensor installed — and subsequently monitors cloud trail logs for any modifications to the environment. This allows you to: ■ Drill into unmanaged instances and use a tag to filter on all "prod" servers that are currently unprotected ■ Use filtered data to create a report and export it ■ Send that information to infrastructure teams to resolve identified security gaps ■ Filter the information based on account names to generate reports and track how security posture is trending for different account owners
Benefit:	The ability to quickly and efficiently identify unprotected / unmanaged EC2 instances allows them to be put them under management by installing the Falcon agent as needed.

WHAT MAKES FALCON DISCOVER FOR AWS UNIQUE?

An integral part of the CrowdStrike platform, Falcon Discover for AWS extends visibility over all EC2 instances, enabling security professionals to more quickly identify and stop threats:

- **Gap analysis:** Identifies protected and unprotected EC2 instances in your environment
- **Improved effectiveness:** Provides additional information and context about EC2 instances, improving protection and response actions
- **Real-time visibility:** Gain visibility across your entire environment, whether EC2, virtual or physical via the Falcon Management Console
- **Ease of deployment:** Falcon Discover for AWS is delivered via the lightweight Falcon agent without affecting performance
- **Cloud-native:** It scales easily to match the dynamic nature of ephemeral EC2 instances

USE CASE: MONITOR AND SEARCH METADATA TO IMPROVE SECURITY POSTURE

Challenge:	It can be difficult to ensure consistency across EC2 instances and their respective security groups. For example, how can you know with certainty the specific EC2 instances that are permitting remote desktop protocol (RDP)?
Solution:	Using the Falcon Discover for AWS dashboard allows you to: ■ See AWS-specific metadata including, Instance ID, Instance Type, State, Region, AZ, Security Groups, Subnets, AMI Id, Tags and more ■ Drill into security groups ■ Filter for those groups with internet access ■ Identify, filter and make changes to any group or EC2 instance in security groups that permit RDP ■ See both CrowdStrike and AWS information in the same host dashboard
Benefit:	The ability to quickly and effectively access AWS-specific metadata in real time and in one console gives analysts the information and confidence they need to take the appropriate corrective actions.

USE CASE: REVIEW RATE OF EC2 LAUNCHED OVER TIME

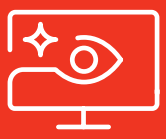
Challenge:	Given the ease of deployment and the ability to scale, it can be difficult to get an overview and track the rate at which EC2 Instances are being launched.
Solution:	Using the Falcon Discover for AWS dashboard allows you to: ■ See what EC2 instances have been launched by day, week or month ■ Review the rate at which EC2 instances are being launched across all accounts and then drill into specific accounts
Benefit:	The ability to quickly and effectively track EC2 instance launches in one dashboard and drill into specific accounts as needed offers both the overview and details analysts need.

EC2 VISIBILITY TRANSFORMED

The CrowdStrike Falcon® platform for AWS provides extensive and detailed visibility over EC2 instances, helping improve an organization's overall security posture. It quickly enumerates existing EC2 instances in one centralized view, allowing you to immediately identify security gaps. Rich AWS-specific context is presented to allow for timely triaging and response to security events on EC2 instances.

WHY CROWDSTRIKE

The CrowdStrike Falcon® platform provides a cloud-delivered solution that safeguards your organization while satisfying your mission requirements. The threats you face are constantly evolving and you require a solution that proactively detects and prevents these events from occurring. CrowdStrike has built its solutions around the ability to detect and prevent breaches by even the most sophisticated adversaries. With a platform that seamlessly deploys and scales with your enterprise and a dedicated team of security professionals, CrowdStrike protects your enterprise with a solution designed to stop the breach and evolve with you.



LEARN MORE AT WWW.CROWDSTRIKE.COM

Speak to a representative to learn more about how CrowdStrike can help you gain visibility over your EC2 instances.

■ **Phone:** 1.888.512.8906

■ **Email:** sales@crowdstrike.com

■ **Web:** www.crowdstrike.com