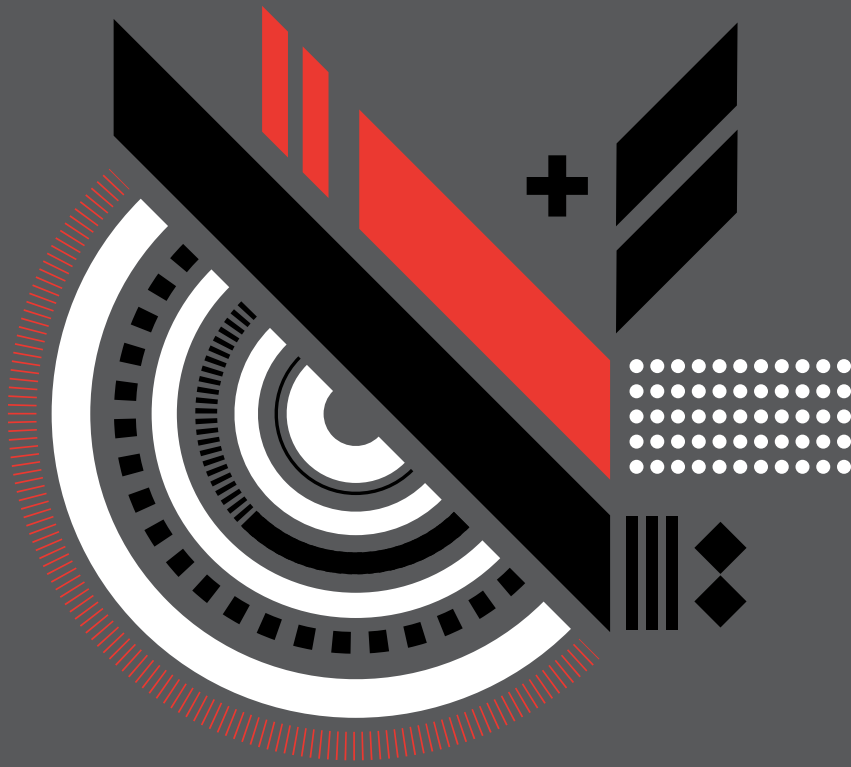
eBook



MULTIPLE ACCOUNTS, MAXIMUM SECURITY

SECURING MULTI-ACCOUNT AWS ENVIRONMENTS WITH AWS CONTROL TOWER AND CROWDSTRIKE FALCON CLOUD WORKLOAD PROTECTION

CROWDSTRIKE | aws

TABLE OF CONTENTS

DON'T LET SHADOW IT DARKEN MULTI-ACCOUNT VISIBILITY

Under pressure to continually innovate, today's enterprise relies on numerous cloud services to stay agile and responsive. But when departments outside of IT decide to fulfill technology needs on their own, security can weaken as the surface area for attacks grows. Shadow IT accelerates sprawl across corporate networks, leaving organizations vulnerable to malicious activity.

In an enterprise that runs multiple Amazon Web Services (AWS) accounts to handle its many compute instances—including cloud workloads and containers—maintaining comprehensive visibility at scale is crucial.

Real-time insights about AWS workloads help uncover and mitigate risks related to shadow IT, reducing the attack surface area.

CROWDSTRIKE AND AWS HAVE TEAMED UP TO HELP ORGANIZATIONS MANAGE, GOVERN, AND PROTECT MULTI-ACCOUNT AWS ENVIRONMENTS.

AWS Control Tower helps you set up and govern multi-account AWS environments

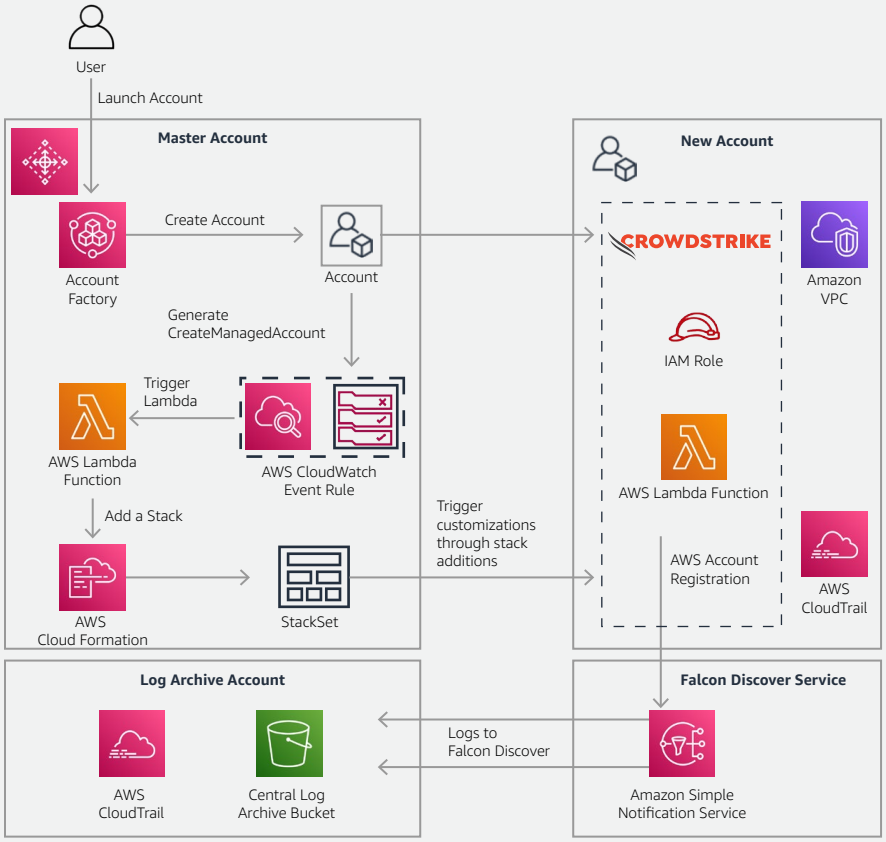
- Deploy new AWS environments that automatically align with best practices
- Stick to guardrails for easier policy management
- View policy-level summaries through an integrated dashboard

CrowdStrike Falcon Cloud Workload Protection provides full security against breaches

- Gain visibility into your AWS multi-account footprint, enabling detection, response, and proactive threat hunting
- Automate workload protection for each new account created
- Improve compliance with holistic asset management

COMPREHENSIVE VISIBILITY WITH AWS CONTROL TOWER AND THE CROWDSTRIKE FALCON SUITE

Falcon Cloud Workload Protection seamlessly integrates with AWS Control Tower via a rich set of APIs, ensuring automatic protection, compliant environments across the enterprise, and an enhanced security posture. Falcon Discover for Cloud and Containers, available as part of the Falcon Cloud Workload Protection suite, offers a comprehensive view across all Amazon Elastic Cloud Compute (Amazon EC2) resources, plus valuable AWS insights, and helps you quickly understand and prioritize instances for holistic protection.



FALCON DISCOVER FOR CLOUD AND CONTAINERS WORKS ACROSS AWS ASSETS:

- Leveraging read-only access to your **Amazon EC2 metadata** to prioritize detections and enable a faster response. Read-only access also minimizes the security impact to your AWS infrastructure.
- Continuously monitoring events to provide visibility into activities inside containers running on **Amazon Elastic Container Service (Amazon ECS)** and **Amazon Elastic Kubernetes Service (Amazon EKS)**
- Monitoring and analyzing **AWS CloudTrail logs**, then making an API call to gather information about events and resources.
- Crossing boundaries to see **Amazon Virtual Private Clouds (Amazon VPC)** and subnets and collecting data from all endpoints—even those that are unmanaged.

As the leading cloud-native, next-generation security solution, Falcon Cloud Workload Protection offers streamlined integration not available with other third-party solutions and saves you the time and expense of trying to develop these capabilities in house.

AUTOMATE WORKLOAD PROTECTION FOR EACH NEW ACCOUNT CREATED

The combination of Falcon Cloud Workload Protection plus AWS Control Tower automates much of the manual tasks associated with setting up and securing new AWS environments. AWS Control Tower uses blueprints to standardize the setup of each new instance or workload, while Falcon Discover for Cloud and Containers is automatically attached to new environments—immediately monitoring at the account level for improved visibility.

AUTOMATE ONGOING POLICY MANAGEMENT

Control Tower provides mandatory and best practices enforced by guardrails that help prevent undesirable actions through service control policies, and detect violations using AWS Config rules. These rules remain in effect as you create new accounts or make changes to your existing accounts.

DEPLOY INSTANTLY FOR FULL PROTECTION

As a cloud-native security tool, Falcon Discover for Cloud and Containers deploys instantly and scales easily with no hit to performance and no reboots required. You'll have immediate visibility and control over existing endpoints and Amazon EC2 instances, without requiring additional agents or manually installing scripts.

ELIMINATE MANUAL TASKS SUCH AS

- Creating accounts
- Making configuration changes
- Creating API calls (AWS CloudTrail)
- Integrating with AWS SSO
- Enabling baseline security posture for all accounts
- Leveraging lifecycle hooks
- Centralizing logging across all accounts
- Automating monitoring into all accounts

IMPROVE COMPLIANCE WITH HOLISTIC ASSET MANAGEMENT

An AWS environment where different teams own multiple accounts across an enterprise, likely leverages a variety of AWS resources—from containers to cores—running in both staging and production. This sprawling, fragmented ownership of AWS assets can hinder compliance, leaving organizations open to misconfigurations in their environment that violate security policies.

By creating a managed standard in AWS Control Tower to specify how Falcon Discover for Cloud and Containers will be configured for new instances, you can ensure new environments are in compliance with security best practices from the get-go.

VIEW POLICY-LEVEL SUMMARIES

AWS Control Tower provides top-level summaries of your policies via an integrated dashboard. Details on the accounts provisioned, guardrails enabled across your accounts, and account-level status showing guardrail compliance provide a full picture of policy adherence in the collective AWS environment.

ENSURE COMPLIANCE ACROSS ALL ASSETS

By uniquely combining information from the Falcon sensor and AWS metadata, security teams can baseline existing EC2 deployments instantly across all regions and subsequently monitor AWS CloudTrail logs for any modifications to the environment. This holistic asset management across all datacenters and AWS resources allows you to identify unmanaged assets—pinpointing security gaps like mismatched IAM roles and closing them.

ENHANCE OVERALL SECURITY POSTURE WITH PROACTIVE THREAT HUNTING

By integrating Falcon Cloud Workload Protection with AWS Control Tower, you introduce an additional security layer into your multi-account AWS environment that proactively stops threats and enhances your overall security posture. Falcon platform detects and investigates attacks that span environments and workloads, pivoting from endpoints to instances to containers.

SEE INSIDE CONTAINERS TO STOP BREACHES

Falcon Discover for Cloud and Containers provides visibility into the container footprint and shows container usage, including trends, uptime, images used, and configuration to identify risky and misconfigured containers. You can capture information like container start, stop, and runtime even if the container only runs for a few seconds.

REAL-TIME DETECTION AND PREVENTION

Powered by Threat Graph intelligence, Falcon platform delivers proactive threat hunting and effective, real-time detection and prevention of security risks. Workloads are protected from adversaries 24/7.

FALCON CLOUD WORKLOAD PROTECTION:

- Includes behavior-based indicators of attack that detect sophisticated threats such as fileless and malware-free attacks
- Provides exploit protection
- Includes custom IOAs, whitelisting and blacklisting to tailor detection and prevention
- Offers integrated threat intelligence to block known malicious activities and deliver the complete context of an attack, including attribution
- Provides 24/7 managed threat hunting to ensure that stealthy attacks don't go undetected
- Delivers machine learning and artificial intelligence to detect known and unknown cyber threats

DEPLOY CROWDSTRIKE FALCON WITHIN AWS CONTROL TOWER

Ready to bring the proactive security of Falcon Cloud Workload Protection and the visibility of Discover for Cloud and Containers to AWS Control Tower? This **deployment guide** provides step-by-step instructions on how to get started.

For more information on CrowdStrike and AWS solutions, visit **CrowdStrike** or the **AWS Marketplace**.