CROWDSTRIKE

Protecting your cloud workloads with defense-in-depth security from CrowdStrike and AWS

As businesses expand their cloud investments, their security strategies should stay one step ahead of the threats that target their expanded environments. Managing, securing, and tracking endpoints, networks, and workloads—all of this is no easy feat.

Defense-in-depth is an architectural design that originates from a military strategy. In the context of protecting cloud workloads, defense-in-depth relies on mechanisms to protect valuable data, information, and intellectual property.

How CrowdStrike and AWS deliver defense-in-depth

The CrowdStrike and Amazon Web Services (AWS) partnership brings together a principled approach to defense-in-depth cloud security. CrowdStrike's threat intelligence as well as endpoint and workload protection directly integrate with AWS services.

CrowdStrike Falcon capabilities such as the Falcon Agent, Hosts, Detections, Event Streams, and Custom Indicators of Attacks operate in concert with AWS services like AWS CloudTrail, VPC Flow Logs, Amazon EventBridge, AWS Control Tower, AWS Lambda, AWS Security Hub, and many more to address the three principles of defense-in-depth.

Visibility

Gain clarity into the current state of your environment.

Prevention

Detect anomalous behavior in your workloads and use aggregation and correlation to send alerts.

Remediation and response

Understand and effectively act on a security event.

aws PARTNER

- Public Sector
- Amazon Linux Ready
- AWS Graviton Ready
- Authority to Operate
- AWS PrivateLink Ready
- AWS Marketplace Seller
- Security Software Competency

Drive workload and asset clarity with visibility

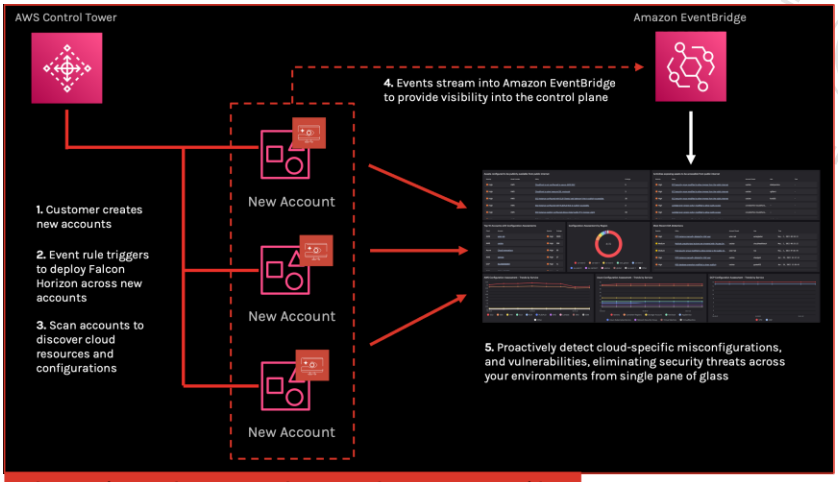
The CrowdStrike and AWS tools that enable visibility allow teams to view configurations of all components, aggregate network traffic entering and leaving the workload, audit API calls, and provide runtime visibility of apps in an Amazon Elastic Cloud Compute (Amazon EC2) instance or a container.

Falcon Discover for Cloud and Containers + AWS CloudTrail

Gain visibility of your compute and container workloads hosted across your on-premises and cloud infrastructure from one dashboard. Integrate your account landing zone with AWS Control Tower to ensure out-of-the-box visibility across your entire cloud footprint as your cloud adoption grows.

Falcon Horizon and AWS Control Tower + Amazon EventBridge

Events from Amazon EventBridge deliver continuous discovery and visibility of cloud-native assets, providing valuable context and insights into the overall security posture. Integrate new accounts created through AWS Control Tower into Falcon Horizon to proactively detect cloud-specific misconfigurations, vulnerabilities, and security threats, along with guided remediations to resolve them .



Falcon Horizon and AWS Control Tower and Amazon EventBridge

Falcon CWP and Amazon Elastic Container Registry (Amazon ECR)

Get complete visibility into all your container images hosted in Amazon ECR from one dashboard, allowing you to find hidden malware, embedded secrets, and vulnerabilities from outdated libraries. Seamlessly integrate with AWS CodeBuild, GitHub, Jenkins, or other build tools to allow your company to shift left in your security strategy.

Visibility and your solution

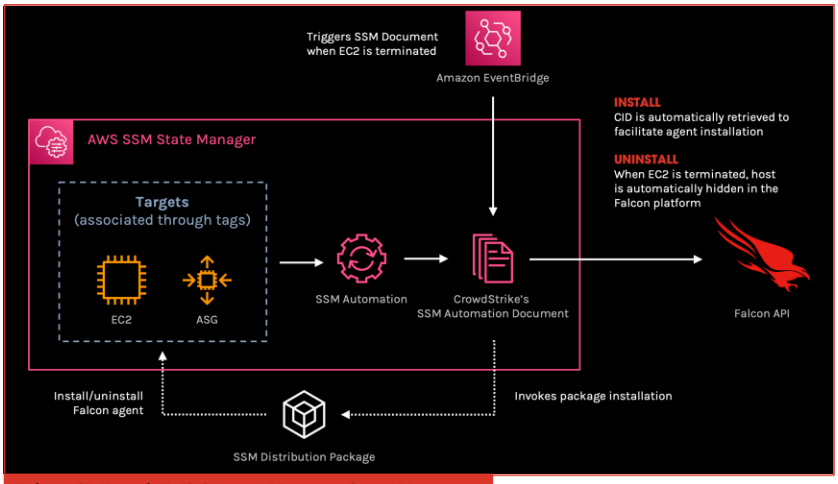
CrowdStrike network detection and response partner solutions complement the visibility principle of the CrowdStrike and AWS solution. For example, combining visibility of network communication with device telemetry gives customers broad visibility into and oversight of their networks, devices, and users, thus removing blind spots.

Prevent attacks by detecting anomalies in workloads and sending actionable alerts

Bring sensors, discovery, and audit information together with runtime visibility from multiple sources, such as Amazon EC2, Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate, and AWS Lambda, and alert teams to anomalous behavior.

Falcon CWP and AWS Systems Manager State Manager

Automate the deployment of the Falcon agent across your Amazon EC2 fleet by integrating with State Manager to protect your long-living, auto-scaling, and ephemeral workloads. Address configuration drifts across your environment by building your packages in AWS Systems Manager Distributor and deploying them at scale with SSM Automation Documents to enforce a policy-driven security posture in your organization.



Falcon CWP and AWS System Manager State Manager

Falcon CWP and Amazon Elastic Container Service (Amazon ECS) / Amazon Elastic Kubernetes Service (Amazon EKS) / AWS Fargate

Gain visibility into container applications to uncover details surrounding file access, network communications, process activity, and block exploitable vulnerabilities at runtime. CrowdStrike has developed Kubernetes Operator and Helm Charts to provide administrators with the flexibility they need using the tools they are familiar with . Whether you're using Amazon ECS to deploy containers or you're running Kubernetes clusters on Amazon EKS, your workloads stay secure through a seamless experience. For workloads running on AWS Fargate, our Falcon Container agent can provide you with the protection you need to secure your managed workloads.

Falcon CWP and AWS PrivateLink

Utilize AWS PrivateLink to provide private connectivity between your CrowdStrike Falcon protected workloads and the CrowdStrike cloud. By using the AWS infrastructure instead of the public internet, you can secure your communication and reduce your exposure to distributed denial-of-service attacks, along with many other threats.

Falcon X and Amazon S3

Secure your Amazon S3 buckets through automated file scanning as they're uploaded to the CrowdStrike cloud. Once uploaded, the files are executed in our sandbox environment for analysis. Malicious files are automatically deleted from the bucket, and a security event is generated in AWS Security Hub for your security team to investigate and triage the event.

Falcon X and AWS Network Firewall

Automatically block malicious domains and IP addresses in your AWS Network Firewall policy rules based on CrowdStrike's domain-based Indicators of Attacks (IOAs). AWS Network Firewall works with AWS Firewall Manager, so you can leverage the policy you create to manage and apply them across your entire AWS footprint centrally.

Prevention and your solution

Using machine learning with aggregation of contextual network and endpoint telemetry to create customized policies and real-time behavior-based discovery results in faster detection of anomalous behaviors and threats between devices and the network edge and within internal network traffic.

Automate remediation to scale security teams

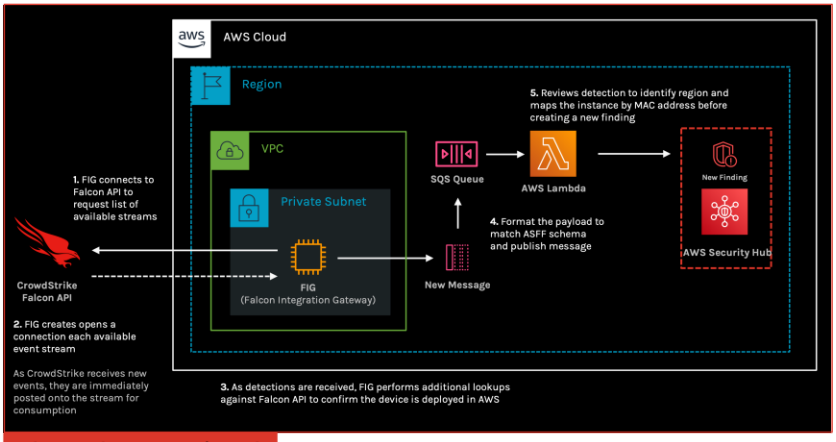
Response teams can only respond to 3-5 percent of the security events they receive each day. Configuration assessments and runtime visibility, along with their correlation, can provide effective preventative controls. However, organizations need to be able to understand and effectively act on a security event, which is where CrowdStrike and AWS solutions for remediation and response come in .

Falcon + AWS Security Hub

Detections identified by the CrowdStrike agent are delivered automatically into AWS Security Hub to enable a comprehensive, real-time view of high-priority security alerts. Once Detections are in AWS Security Hub, security teams can use them to investigate, remediate, and automate security-related problems to stop breaches in their environment.

Response and remediation and your solution

When you integrate your solutions with the CrowdStrike and AWS defense-in-depth approach, customers get a full range of incident information to inform their triage, investigation, response capabilities. Ultimately, this speeds up incident response and further mitigates risk.



Falcon and AWS Security Hub

CrowdStrike and AWS deliver comprehensive, consistent workload protection

Workload protection requires tight integration between security solutions and services to provide end-to-end visibility and the ability to defend against threats wherever they are —from the network edge to the cloud and across endpoints and workloads.

With an integrated security solution, organizations gain visibility of their AWS accounts, inventory and configuration information, runtime activity, and correlation of events. The result is actionable measures for preventing and responding to security events, along with a framework for centralizing logging of security events and automating remediation workflows.

Get started with CrowdStrike and AWS today

Access CrowdStrike to experience how the defense-in-depth principles come together to mitigate and remediate threats.

Sign up for a free trial.