CrowdStrike: Falcon Horizon CSPM

Streamlines security for multi-cloud environments

Why Falcon Horizon?

- Provides complete multi-cloud visibility with a single source of truth for cloud.
- Prevents cloud misconfigurations and application vulnerabilities automatically.
- Assesses the security of cloud accounts and eliminates compliance violations.
- Reduces alert fatigue and accelerates incident response.
- Improves code quality and shortens release cycle times.
- Delivers agentless cloud-native protection.

Product overview

Falcon Horizon streamlines cloud security posture management across the application lifecycle for any cloud, enabling you to securely deploy applications with speed and efficiency. CrowdStrike Falcon cloud-native platform provides visibility into your entire cloud infrastructure, continuous monitoring for misconfigurations, and proactive threat detection - allowing DevOps and DevSecOps teams to fix issues faster and be more productive.

Key capabilities

Discovery and visibility

Provides discovery and visibility into cloud infrastructure and resources:

- Access a single source of truth for cloud assets and security configurations across multi-cloud environments and accounts.
- Discover cloud resources and details automatically upon deployment, including misconfigurations, metadata, networking, security, access control and change activity. Supported services include:

<table>
<thead>
<tr>
<th>AWS Services</th>
<th>Amazon Elastic Container Service for Kubernetes (Amazon EKS)</th>
<th>Amazon RDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon API Gateway v1</td>
<td>Amazon ElastiCache</td>
<td>Amazon Redshift</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>Elastic Load Balancing (ELB)</td>
<td>Amazon Route 53</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>Amazon EMR</td>
<td>Amazon S3</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>Amazon GuardDuty</td>
<td>Amazon Simple Email Service (SES)</td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS Identity and Access Management (IAM)</td>
<td>Amazon Simple Notification Service (Amazon SNS)</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>Amazon Kinesis</td>
<td>Amazon Simple Queue Service (SQS)</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (EBS)</td>
<td>AWS Key Management Service (AWS KMS)</td>
<td>AWS Systems Manager (SSM)</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>AWS Lambda</td>
<td>Amazon VPC</td>
</tr>
<tr>
<td>Amazon Elastic Container Registry (ECR)</td>
<td>Network Load Balancer (NLB)/Application Load Balancer (ALB)</td>
<td></td>
</tr>
</tbody>
</table>
Key capabilities (continued…)

Prevents cloud misconfigurations and eliminates compliance violations
Falcon Horizon provides intelligent monitoring of cloud resources to proactively detect misconfigurations, vulnerabilities, and security threats, along with guided remediation to resolve security risks and enable developers with guardrails to avoid costly mistakes and ensure compliance across multi-cloud environments.

Reduces alert fatigue with targeted threat detection
Falcon Horizon continuously monitors for anomalies and suspicious activity and integrates seamlessly with security information and event management (SIEM) solutions. This enables security teams to gain visibility, prioritize threats, and reduce alert fatigue by eliminating noise and responding and fixing issues faster.

How it works
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 4 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.

Differentiators
• **Discovery and visibility**: Discover cloud assets and security configurations across multi-cloud environments and accounts automatically.
• **Misconfiguration management and remediation**: Continuous monitoring to protect and eliminate security risks due to misconfigurations or open vulnerabilities.
• **Threat detection**: Proactive threat detection across application development lifecycle against malicious activity, unauthorized behavior, and access to cloud resources.
• **Continuous compliance monitoring**: Assesses the security of cloud accounts and eliminates compliance violations. Continuously monitor the compliance posture of all your cloud resources from a single console.
• **DevSecOps integration**: Employs cloud-native, agentless posture management to reduce overhead and eliminate friction and complexity across multi-cloud providers and accounts.

Solution available in [AWS Marketplace](https://aws.amazon.com/marketplace)