DELL Technologies

Dell SafeGuard and Response

CrowdStrike Falcon® Horizon™ Cloud Security Posture Management (CSPM)

Key Benefits

- Provides complete multi-cloud visibility with a single source of truth for cloud resources
- 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

Stop cloud breaches with unified visibility, threat detection and continuous monitoring and compliance for multi-cloud environments

The adoption of the cloud has fundamentally changed how businesses go to market and develop modern applications. Today's application development lifecycle places a premium on speed to market, requiring development teams to build cloud-native applications supported by a programmable infrastructure that enables businesses to change and reconfigure the cloud infrastructure on the fly.

This shift presents new challenges that make it difficult for security teams to keep up. The result is poor visibility and control of cloud resources, fragmented approaches to detecting and preventing misconfigurations, an increasing number of security incidents, and the inability to maintain compliance.

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

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE

DELL Technologies

Key capabilities

Discovery and Visibility:

- **Single source of truth**: Get up and running in minutes and access a single source of truth for all cloud assets and security configurations across multi-cloud environments and accounts.
- **See everything:** Discover cloud resources and details automatically upon deployment — including misconfigurations, metadata, networking security, access control and change activity — and eliminate security blind spots.
- **Simplified management and security policy enforcement:** Manage and enforce security group policies across accounts, projects, regions and virtual networks from a single console to reduce the attack surface.
- **Monitor the control plane:** Scale at will and gain insight into all control plane API calls and uncover security risks within managed Kubernetes clusters.
- **Identify unprotected resources:** Identify cloud resources not protected by Falcon and take immediate action.

Misconfiguration Management and Remediation:

- **Eliminate misconfigurations and compliance violations:** Compare cloud application configurations to industry and organizational benchmarks to identify violations and remediate in real time and ensure application availability.
- **Get guided remediation from security experts:** Fix issues that leave cloud resources exposed — such as misconfigurations, open IP ports and unauthorized modifications — with guided remediation and guardrails that enable developers to avoid critical mistakes.
- **Enforce permissions:** Monitor storage to ensure permissions are secure and not publicly accessible.
- **Prevent identity-based threats:** Reduce the number of tools required from three to one, and prevent users from putting your organization at risk by automating the detection and remediation of identity-based risks in Microsoft Azure, AWS and GCP.
- **Secure Azure Active Directory (AD):** Ensure Azure AD groups, users and apps have the correct permissions using the new Identity Analyzer reports.
- **Reduce alert fatigue:** Remediate issues faster and reduce SOC costs with enhanced policy management for cloud accounts, regions or specific resources.
- **Ensure resilience:** Monitor database instances and verify that high availability, backups and encryption are enabled, as well as security groups to limit exposure.

Real-Time Threat Detection:

- **Accelerate response:** Reduce the time it takes to detect and mitigate a breach from months to minutes by cutting through the noise of multi-cloud environment security alerts with an adversary-focused approach that saves time and allows teams to take the most effective action.
- **Identify malicious activity with confidence scoring and prioritization:** The patent-pending Confidence Scoring in Falcon Horizon continuously aggregates, assesses and scores control plane threats and configurations to accurately identify malicious activity, reducing the time to understand and respond.

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE

DELL Technologies

- **Integrate cloud indicators of attack (IOAs) with threat intelligence:** Gain access to realtime alerting and reporting on over 150 cloud adversaries based on CrowdStrike's market-leading threat intelligence and research for more effective response.
- **Benefit from continuous control plane threat detection:** Machine learning and behavior-based TTP/IOA detections and guided remediation are provided for all cloud accounts, services and users across the cloud estate, improving investigation speed by up to 88%.
- **Enable self-service threat hunting:** Cloud-scale data and analytics for all cloud activity enable security teams to proactively uncover hidden threats and take action.

Continuous Compliance Monitoring

- **Continuously monitor compliance:** Continuously monitor the compliance posture of all of your cloud resources from a single console.
- **Assess for CIS benchmarks:** Assess the security of cloud accounts against Docker and Kubernetes CIS benchmarks with up to 250 out-of-the-box, adversary-focused policies to save time and reduce operational costs.
- **Ensure audit-ready compliance:** Continuously monitor the compliance of all of your cloud resources and avoid costly fines using a single console for regulations, including PCI, NIST and more.
- **Eliminate compliance violations:** Identify policy violations and take immediate user-driven action to remediate.

DevSecOps Integration

- **Improve decision making:** With SIEM integration, streamline visibility for security operations and provide insights and context into misconfigurations and policy violations for faster incident response.
- **Integrate at the speed of DevOps:** Using the single API, achieve faster integration and remediation within the DevOps and collaboration tools you already use, such as email, Slack, PagerDuty and more.
- **Fuel business performance:** Through reporting and dashboards, drive alignment and a shared understanding across security operations, DevOps and infrastructure teams.

AWS		
ACM	EKG	RDG
API Gateway v1	ElastiCache	Redshift
CloudTrail	ELB	Route 53
CloudFront	EMR	S3
CloudFormation	GuardDuty	SES
Config	IAM	SNS
DynamoDB	Kinesis	SQS
EBS	KMS	SSM
EC2	Lambda	VPS
ECR	NLB/ALB	

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE

DELL Technologies

Azure	
Active Directory (AD)	Load Balancer
App Service	Monitor
Container Registry	Network Security Groups
Disk	PostgreSQL
File Service	SQL Server Virtual Machine
Identity and Access Management (IAM)	Storage Account
Key Vaults	Virtual Machine
Kubernetes Service	Virtual Network
GCP	
App Engine	Cloud Storage
BigQuery	Computer Engine
Cloud Load Balancing	IAM
Cloud Logging	KMS
Cloud SQL	VPC

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE