CROWDSTRIKE

SOLUTION BRIEF

FALCON ENDPOINT PROTECTION PLATFORM (EPP) FOR AWS

Enabling your migration to AWS with real-time protection for AWS 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 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 within EC2 brings tremendous operational and business gains, however, practical security considerations are critical. Gaining comprehensive protection and visibility are key to maintaining an adequate security posture, but doing so is not without challenges:

- **Protection:** Organizations need to ensure security as they undertake any migration of workloads into AWS. It is imperative that AWS workloads and on-premises endpoints are protected against all threat types and have full prevention, detection and response capabilities.
- **Migration:** Moving to the cloud is not without security challenges. Organizations struggle to identify all assets that need to be transitioned. Workloads need to be secured so that no adversaries are transferred into the new cloud capability as part of the transition itself.

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.

FALCON ENDPOINT PROTECTION PLATFORM (EPP) FOR AWS

- **Time:** For IT and security teams, time is a scarce resource. 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, asking the core question, "Are we secure?" The complexity of spanning across different environments and tools results in a time-consuming approach that simply doesn't work.
- **Visibility:** The lack of visibility and context over cloud-hosted endpoints requires that organizations quickly identify unprotected / unmanaged assets and put them under management to reduce risk. For example, the instance was deployed, but did it have appropriate endpoint security running? Furthermore, would you be able to see if an endpoint has protection? These are critical questions for IT and security teams and having endpoint visibility is key to answering them.
- **Consistency:** As enterprises implement hybrid data centers, with workloads running on-premises and in the cloud, ensuring consistent security becomes challenging. For many organizations, security and IT processes and controls were established with the assumption that their infrastructure was "on-premises." As a result, they struggle to secure, manage and have visibility over endpoints deployed into cloud environments.
- **Complexity:** Left uncontrolled, cloud environments can spin into un-mangeable complexity. Typically, organizations have numerous cloud implementations and even multiple cloud providers. Public, private and hybrid clouds all coexist, serving different needs and applications, which creates challenges for cloud security.
- **Speed:** Security needs to match the speed and agility of DevOps engineers, many of whom view endpoint security products as a hindrance that drains performance and system resources. Security teams need to support deadlines for setting up the security configurations for increasing numbers of physical and virtual machines. The cloud delivers unparalleled speed and scale to these teams and they need endpoint security that contributes their goals, not compromises them.
- **Scalability:** Traditional on-premises tools don't scale well and are too expensive. The approach was never designed to accommodate the ability to scale up and down large numbers of endpoints in real time. On-premises solutions also impact performance by draining system resources (CPU, memory and disk).

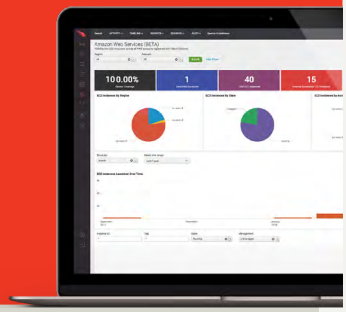
PROTECTION AND CONTROL FOR ALL OF YOUR ENDPOINTS

CrowdStrike Falcon® EPP for AWS brings cloud-delivered endpoint protection whether endpoints are on-premises, virtualized or Amazon EC2 — ensuring a consistent security posture. Falcon EPP delivers instant protection and visibility, preventing all attack types, whether malware or malware-free. It provides automated prevention and detection, alongside real-time centralized visibility and control. Falcon is cloud-native and scales elastically to meet the demands of security, development and operations teams as they dynamically deploy new applications and services. Simply put, Falcon EPP for AWS delivers security "in the cloud," from the cloud.

WHAT MAKES FALCON EPP UNIQUE?

An integral part of the CrowdStrike® platform, Falcon EPP extends protection and visibility over all endpoints whether on-premises, virtualized or Amazon EC2 instances, enabling security professionals to more quickly identify and stop threats:

- **Protection:** AWS workloads and on-premises endpoints are protected against all threat types and have full prevention, detection and response capabilities.
- **Visibility:** Falcon Discover™ for AWS provides visibility and context across AWS workloads so that unprotected / unmanaged assets are identified quickly.
- **Threat Hunting:** Falcon OverWatch™ provides an additional layer of oversight and analysis across your environment whether AWS, virtualized or on-premises.
- **Threat Intelligence:** Falcon Intelligence™ is natively integrated into Falcon EPP ensuring that you can understand all elements of an attack and optimize your protection.
- **Comprehensive Compliance:** CrowdStrike recognizes that compliance and certification frameworks are critical for your organization and the Falcon platform helps you addresses PCI DSS, HIPPA, NIST, FFIEC, SOC-2 and CSA-STAR and others.



FALCON ENDPOINT PROTECTION PLATFORM (EPP) FOR AWS

USE CASE: PROTECTION AND VISIBILITY

Challenge:	Organizations struggle to adequately protect their endpoints against increasingly sophisticated tactics, techniques and procedures (TTPs) employed by adversaries.
Solution:	CrowdStrike Falcon EPP for AWS is designed with your security needs in mind, providing an arsenal to protect against all attack types: ■ Falcon EPP blocks known and unknown malware as well as malware-free threats. ■ It's continuous monitoring of all endpoints allows for rapid detection and response to malicious activity. ■ The Falcon Discover IT Hygiene module provides 360-degree visibility into managed and unmanaged assets, users and applications.

USE CASE: OPTIMIZING APPLICATION PERFORMANCE WITHOUT COMPROMISING SECURITY

Challenge:	The ability to scale compute power elastically within EC2 brings with it tremendous operational and business gains, however, maintaining comprehensive protection and visibility are key and are not without challenges.
Solution:	The Falcon platform protects your enterprise as you scale by deploying across environments (EC2, virtualized and on-premises) and across operating systems ensuring compatibility with Docker platforms: ■ With a lightweight agent that deploys in minutes, CrowdStrike Falcon EPP ensures comprehensive protection with immediate time-to-value. ■ It's managed via the cloud, so no on-premises infrastructure is required. ■ It streamlines your operational efficiency, requiring no new installs, reboots or scans.

USE CASE: FINDING UNPROTECTED EC2 INSTANCES

Challenge:	Organizations can quickly deploy instances, however, their ephemeral nature can make it difficult to rapidly 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 agent 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.

USE CASE: THREAT HUNTING

Challenge:	Organizations need total visibility over their entire environment, so that they can efficiently and effectively hunt for attacks and intrusions, both retrospectively and in real time.
Solution:	Falcon records all activities of interest for deeper inspection, on-the-fly and after-the-fact, allowing you to quickly detect, investigate and respond to an attack: ■ Five-second search allows you to go back to one second, one day or even one year of activity — all at your fingertips. ■ Indicator of attack (IOA) behavioral protection ensures the automatic detection of IOAs to identify attacker behavior and stop attacks, with prioritized alerts sent to the Falcon web management console. ■ Immediate and powerful response actions allow you to contain and investigate compromised systems and eradicate threats with surgical precision. ■ Falcon OverWatch proactive threat hunting provides an additional layer of oversight and analysis of your environment, whether AWS, virtualized or on-premises, to spot intrusions and attacks before they can do harm.

BENEFITS

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.

CrowdStrike delivers an industry-leading solution that scales with your environment, providing comprehensive threat prevention and detection without impacting the performance of your systems and applications.

The ability to quickly and efficiently identify unprotected / unmanaged EC2 instances allows them to be put under management by installing the Falcon agent as needed.

CrowdStrike allows you to hunt for threats, detecting and blocking incidents by monitoring, analyzing and recording the details of what's happening in your environment, all in real time.

FALCON ENDPOINT PROTECTION PLATFORM (EPP) FOR AWS

ENDPOINT PROTECTION TRANSFORMED

CrowdStrike Falcon EPP for AWS brings cloud-delivered endpoint protection to your AWS deployments for EC2 as well as on-premises workstations and servers, ensuring a consistent and controlled security posture. Falcon is a cloud-native platform that scales to secure any EC2 instance with no impact on performance and no requirement to reboot. It provides protection against all advanced attacks that bypass traditional perimeter and signature-based approaches. Security and operations teams enjoy automated real-time protection, visibility and control via one console, allowing them to assess and manage security across their environment: AWS, virtual and on-premises.

Falcon is a cloud-native platform that scales to secure any EC2 instance with no impact on performance and no requirement to reboot. It provides protection against all advanced attacks that bypass traditional perimeter and signature-based approaches.

WHY CROWDSTRIKE

The CrowdStrike Falcon platform provides comprehensive, cloud-delivered endpoint protection 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 protect your environment:

- Phone: 1.888.512.8906
- Email: sales@crowdstrike.com
- Web: www.crowdstrike.com