YOU NEED TO SEE IT TO PROTECT IT:

HOW REAL-TIME VISIBILITY AND IT HYGIENE DRIVE AMAZON ELASTIC COMPUTE (AMAZON EC2) SECURITY
Proactive endpoint security is a daily business reality. In 2018 alone, 64% of organizations were compromised by endpoint attacks.¹ Today's data systems are being scaled at unprecedented rates, and this progress has come with its own set of security challenges.

Organizations are increasingly connecting mission-critical applications and data to Amazon Web Services (AWS) and taking advantage of its highly scalable Elastic Compute Cloud (EC2). Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, enabling organizations to quickly scale compute capacity up and down as requirements change. With such speed and scalability, managing and securing your own EC2 environment can become a challenge. To improve your overall security posture, you need real-time visibility and good IT hygiene.
IT HYGIENE

IT HYGIENE ENABLES COMPLETE NETWORK TRANSPARENCY

A cluttered IT environment can cause organizations to miss the warning signs of a breach. Visibility and a bird’s eye view of the network are essential to helping IT teams proactively drill-down and clean up the environment. An effective IT hygiene solution will deliver complete visibility and discoverability over all EC2 instances, so organizations can address blind spots and eliminate risk as they journey to cloud. The following is what to look for in an IT hygiene solution for Amazon EC2.

ACCOUNT MONITORING

Choose an IT hygiene solution that monitors accounts, shows who is working in the environment and ensures that they are not violating their credential permissions. System administrators, especially, are highly targeted and poor password renewal policies are rife in most organizations, so credential theft is an ongoing threat. By providing insight into password updates, a good IT hygiene solution should help prevent credential theft by identifying old administrative accounts for removal and ensuring current users regularly update passwords. The solution should also reveal unusual admin behavior or privilege elevation, in order to prevent silent failure.

APPLICATION INVENTORY

Opt for an IT hygiene solution that identifies outdated and unpatched applications and operating systems. This will not only help with the management and cost control of application inventory but also prevent exploits related to patches and system updates. Choose a solution that optimizes software configuration, provides real-time and historical views of application usage and identifies unused software that can be removed.

ASSET INVENTORY

An effective IT hygiene solution should identify all machines that are running on the network, so security architecture can be effectively deployed, suspicious systems addressed and threats mitigated. The solution should also identify any unmanaged assets so that vulnerabilities can be identified and valuable assets protected.

CrowdStrike® Falcon Discover™ for AWS is the IT hygiene solution that addresses all three of the above key areas, which are vital to keeping a network clean and secure. It monitors and inventories systems application usage and user activity across the environment in real time, enabling organizations to close gaps and eradicate threats.
**VISIBILITY AND CONTEXTUAL DATA ARE ESSENTIAL FOR SECURITY**

EC2 is fast and flexible, enabling organizations to launch applications when needed and quickly obtain, configure and scale capacity. With such speed and flexibility, it is easy to lose sight of who and what is active on the network. Falcon Discover for AWS solves two significant challenges that hinder EC2 management and security:

### VISIBILITY CHALLENGES

Fragmented ownership of AWS assets can cause blind spots, leaving organizations open to security violations.

### CONTEXTUAL CHALLENGES

AWS customers require detailed metadata, so that detections can be prioritized and responded to quickly and efficiently.

Falcon Discover for AWS provides visibility, context and control from one console, so organizations can instantly assess and manage security. John Visneski, Director of Information Security and Data Protection Officer at The Pokémon Company International comments, “In every organization, whether they know it or not, their biggest problem is visibility into their environment. Specifically when it comes to visibility within AWS environments, the rate that you’re spinning up and taking down EC2 instances means that your security posture needs to be able to react awfully quickly.” He continues, “Having a platform and having a service that gives us visibility on demand as quickly as CrowdStrike’s product can, has been huge for us.”

By providing complete transparency and visibility, Falcon Discover for AWS empowers organizations to react quickly and mitigate security risk throughout the enterprise. “We are excited about the future, especially around Falcon Discover for AWS,” Visneski concludes.

Falcon Discover for AWS is able to cross boundaries to collect data from all endpoints and EC2 instances. It quickly enumerates existing EC2 deployments across all regions, including instances without the Falcon sensor installed. It then monitors cloud trail logs for any modifications to the environment. The data capture is presented in a dashboard, so users can quickly identify all EC2 assets running across all AWS accounts and regions in one centralized view. Armed with this rich intelligence, organizations are able to quickly triage, understand and prioritize instances, dramatically improving security.

Sajawal Haider, CISO at Oak Hill Advisors, a global investment firm that manages over $30 billion, praised the in-context visibility that Falcon Discover for AWS provides. The tool delivers a comprehensive overview of AWS, virtual private clouds (VPCs), security groups and EC2 instances. Haider comments, “Those capabilities are indispensable, as it takes a lot of time for security teams to acclimate to and access in-depth knowledge of the complex AWS platform. That’s where CrowdStrike is truly valuable for us. Our security team can continue to work on what they need to work on.”

Falcon Discover for AWS can be deployed in hours. It hits the ground running, monitoring and recording immediately upon installation without requiring reboots, query writing, baselining or complex configuration.
SECURITY

MANAGING INSTANCES AND ENDPOINTS IMPROVES SECURITY POSTURE

The cost of endpoint attacks increased by 42% in 2018, and the average time to patch endpoints was 102 days. It comes as no surprise that as many as 69% of organizations said they regularly re-evaluated the effectiveness of their endpoint security due to epidemic levels of threats. What is surprising is that 58% of data breach victims were small businesses – so no one was immune.

As the only cloud-native, next-generation security solution of its kind, Falcon Discover for AWS offers organizations, large and small, the following security benefits.

SECURITY BENEFITS OF FALCON DISCOVER FOR AWS

IDENTIFIES SECURITY GAPS
By combining information from Falcon Discover and AWS metadata, security teams are able to instantly baseline existing EC2 deployments across all regions and subsequently monitor cloud trail logs for any modifications. The solution takes a holistic approach to asset management, reaching across all data centers and AWS cloud resources to efficiently identify unmanaged assets and security gaps.

PRIORITYIZES DETECTIONS
Falcon Discover for AWS delivers rich metadata on EC2 instances, so that unprotected assets and impacted systems are quickly prioritized. It provides the critical answers to questions such as:

- Is this system internet accessible?
- Does it have identity and access management roles applied with elevated privileges?
- Is it on the same AWS virtual private cloud as critical assets?

Armed with this information, organizations can apply proactive measures to dramatically improve their security posture.

ENSURES SECURITY ACROSS HYBRID ENVIRONMENTS
As organizations move to the cloud, they are implementing hybrid data centers with workloads running on-premise and in the cloud. This can erode security. Falcon Discover for AWS provides visibility across all assets, whether on-premise or EC2 instances. Since this visibility extends to both managed and unmanaged assets, organizations can take steps to ensure that all are protected.
CONSERVES SECURITY RESOURCES

76% of organizations have multiple unique security products deployed to protect their endpoints. This only serves to weaken overall visibility and security. Falcon Discover for AWS is a single tool that provides instant visibility and control over endpoints and EC2 instances, without requiring additional agents or scripts that can burden teams and reduce performance. As a cloud-native security tool, Falcon Discover deploys instantly and scales easily without affecting performance or requiring a reboot. Powered by the Falcon sensor, it is a single lightweight agent managed via the unified Falcon console.

Reporting unauthorized systems and applications in the environment and identifying gaps, Falcon Discover for AWS enables organizations to address any and all issues ahead of attacks.
CONCLUSION

With today’s organizations scaling their data systems at breakneck speed, managing these evolving and heterogeneous environments can be challenging. By providing complete visibility and context, Falcon Discover for AWS enables good IT hygiene and empowers organizations to react quickly and mitigate security risk throughout the enterprise.

Find out how Falcon Discover for AWS can help your organization.

BOOK YOUR MEETING NOW!

CROWDSTRIKE®

The CrowdStrike Falcon platform provides comprehensive, cloud-delivered endpoint protection that safeguards your organization while satisfying your mission requirements. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Visit: www.crowdstrike.com/aws-and-crowdstrike

SOURCES

KEY BENEFITS

› Track computers and applications on the network.
› Gain real-time and historical visibility.
› Monitor and inventory usage and user activity.
› Detect unwanted and vulnerable applications.
› Rectify unprotected and rogue systems.
› Stop admin account abuse.
› Satisfy compliance requirements.
› Eliminate threats.

CAPABILITIES

A simple, intuitive and nimble IT hygiene solution, Falcon Discover for AWS enables organizations to:

› Control all endpoints, whether running on-premise or in the cloud.
› Discover and manage unprotected/unmanaged assets and put under protection as needed (with Falcon Sensor™ installed).
› Receive enriched context and metadata on each EC2 instance to achieve better outcomes.
› Ensure good IT hygiene and mitigate risk with application inventories, asset inventories and account monitoring.

Powered by the Falcon agent and the CrowdStrike cloud, Falcon Discover for AWS meets the dynamic challenges of EC2 instances with no hit to performance.