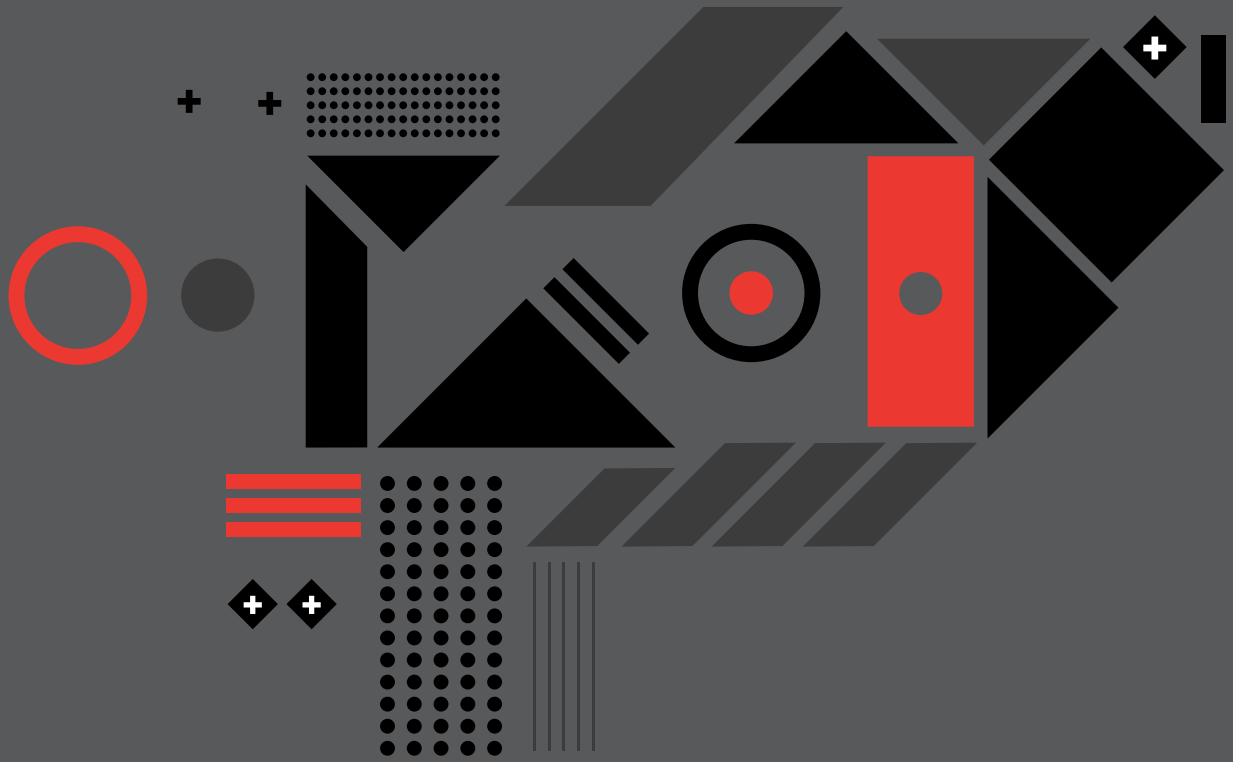
eBook



SECURING THE REMOTE REVOLUTION

PROTECT YOUR REMOTE WORKFORCE AND BOLSTER BUSINESS RESILIENCY WITH THE CROWDSTRIKE FALCON PLATFORM ON AMAZON WORKSPACES

CROWDSTRIKE | aws

TABLE OF CONTENTS

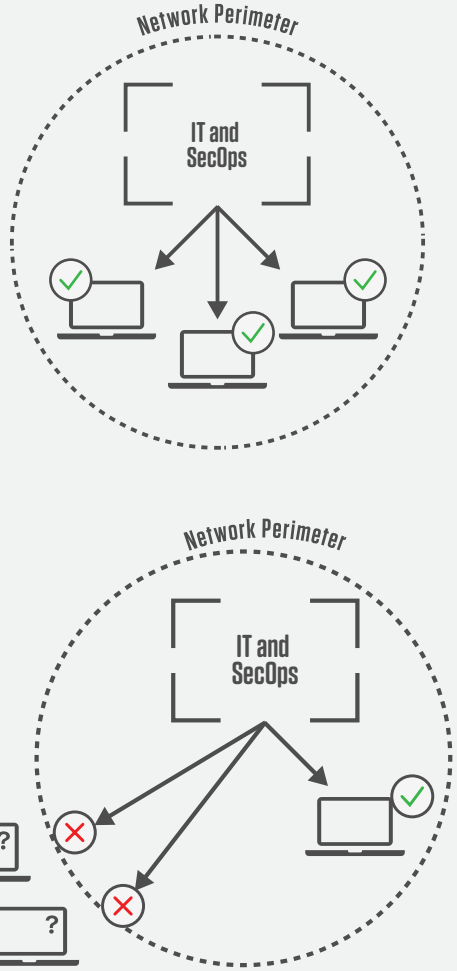
A REMOTE WORKFORCE PUNCTURES SECURE PERIMETERS

Falcon integration with AWS Security Hub enables a comprehensive, real-time view of high-priority security alerts. CrowdStrike's API-first approach brings together Falcon and AWS Security Hub, making it easier for your entire team—including DevOps, CISO, cloud architects, and operations—to automate security tasks and improve overall protection.

THE NEW PERIMETER PARADIGM

With a remote workforce, employees work from different locations across company-issued and personal devices. For security teams, the challenge is how to secure and monitor a sprawling, widened perimeter that now has a greater surface area for attacks. Remote-workforce hurdles include:

- Physical access to systems and endpoints is limited or even prohibited
- Host recovery and remediation now happens remotely
- Incident workflows are decentralized
- Difficulty in updating and managing on-premises endpoints
- Remotely collecting, analyzing, and remediating endpoints is challenging if not impossible



ENABLING A SECURE REMOTE WORKFORCE

With Amazon WorkSpaces, remote employees have a secure desktop-as-a-service solution that provides access to their desktops from wherever they work. Installing the CrowdStrike Falcon sensor into an Amazon WorkSpaces environment further enhances your security posture to help mitigate risks from adversarial, cybersecurity threats.

AMAZON WORKSPACES PROVIDES A DESKTOP-AS-A-SERVICE SOLUTION FOR REMOTE WORKERS

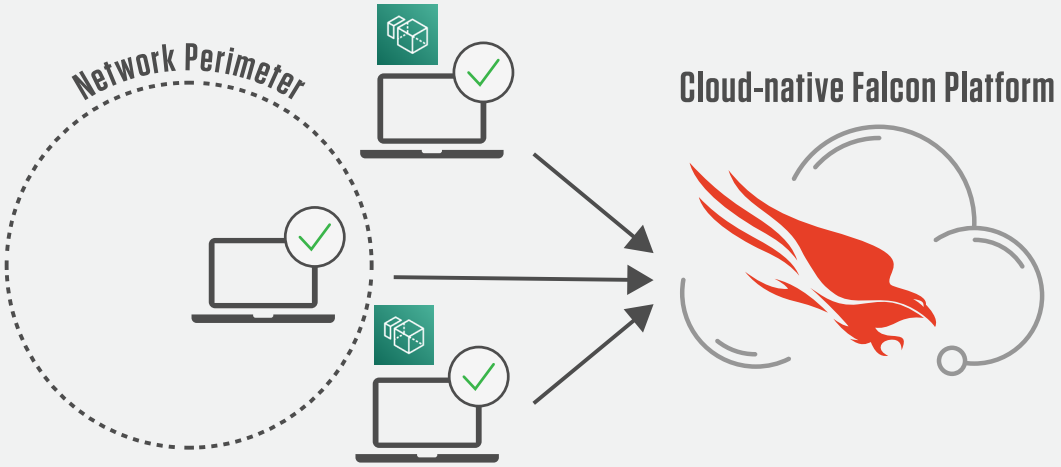
- Deliver a cloud desktop that is accessible anywhere with an internet connection
- Run directly on a wide range of devices, including PCs, Macs, and iPads
- Eliminate administrative tasks such as provisioning, deploying, and maintaining desktops

CROWDSTRIKE FALCON PLATFORM STOPS BREACHES THROUGH CLOUD-NATIVE ENDPOINT PROTECTION

- Install quickly from the cloud through a SaaS solution to keep all devices secure, no matter where they're located
- Pivot seamlessly to secure the full range of potential work models without sacrificing performance
- Reduce complexity with a cloud-delivered SaaS solution that requires no hardware and helps drive down operational costs

PROTECT REMOTE WORKERS WITH FALCON AND AMAZON WORKSPACES

The lightweight Falcon sensor easily installs into an end user's WorkSpaces environment, for a secured work-from-anywhere setup. Combined, these cloud-native solutions help maintain business continuity by protecting against emerging threats, enabling a secure remote solution, and cutting costs through reduced overhead.



SQUELCH PREDATORY ADVERSARIES

With new threats targeting remote-workforce vulnerabilities, the security of an Amazon Virtual Private Network (VPC) plus endpoint protection from Falcon is key. Secure your remote workers with a cybersecurity solution that combines machine learning, artificial intelligence, behavioral analytics, and proactive threat hunting.

RESPOND, RECOVER, AND REMEDIATE REMOTELY

Falcon enables remote protection to safeguard your workers' data, workloads, and devices no matter where they work. Remediate remote hosts quickly with a powerful, cloud-native solution.

OFFSET COSTS TO BOLSTER RESILIENCY

Desktops-as-a-service via WorkSpaces and the cloud-native architecture of Falcon significantly reduce your hardware and the need to provision devices and software. Adopt a fully managed approach for less overhead and improved business resiliency.

ENHANCED THREAT PROTECTION TAKES DOWN EMERGING ADVERSARIES

Unfortunately, in times of crisis, adversaries often exploit the situation, prey on the public's fear, and escalate attacks. As organizations transitioned to a predominantly remote workforce, serious cybersecurity threats cropped up, taking advantage of the dynamic nature of remote environments.

- **Phishing threats** are on the rise, using lures that mimic official business communication such as human resources documents
- **eCrime campaigns** aligned with health-related activity have targeted vulnerable populations
- **Voice phishing** (or vishing), **robocall scams**, and **technical support scams** are taking advantage of employees who increasingly rely on phone communications for remote work

CrowdStrike keeps its finger on the pulse of emerging threats and has designed the Falcon sensor to deliver deep visibility into vulnerabilities. As a sensor integrated with Amazon WorkSpaces, Falcon helps you stay vigilant to secure remote workers.

SECURED FROM THE CLOUD UP

Amazon WorkSpaces are deployed within Amazon VPCs, which provide each user with access to persistent, encrypted storage volumes in the AWS Cloud, and integrate with AWS Key Management Service. No user data is stored on the local device, improving the security of user data and minimizing risk surface area even for remote workers.

REAL-TIME DETECTION AND PREVENTION

Powered by Threat Graph, Falcon delivers the most effective, real-time detection and prevention of known and unknown threats. Endpoints are protected from adversaries 24X7.

Falcon focuses on more than malware, which only accounts for 40 percent of all attacks, employing an adversary approach that not only identifies indicators of compromise, but also indicators of attack.

NEW CYBERSECURITY STRATEGIES FOR A FULLY REMOTE WORLD

Cybersecurity in a work-from-anywhere world takes a different approach than traditional measures. Systems that secure users in an office require high-bandwidth scanning to identify systems, assess patches, and view vulnerabilities. In a remote-work scenario, that setup is no longer feasible. When workers are out of the office for months on end, it creates massive blind spots for IT security staff, introducing unknown risks that can slow down efforts to remediate threats.

REMOTE RESPONSE, RECOVERY, AND REMEDIATION

Attacks and intrusions are not going to stop, and you need to ensure you have the resources and capabilities to respond remotely to protect your organization. The cloud-based architecture of Amazon WorkSpaces and Falcon ensures you can protect every workload everywhere, including those outside a firewall, providing real-time security functionality.

DESKTOP DELIVERY SIMPLIFIED

As a cloud service, there is less hardware inventory to manage with Amazon WorkSpaces, and no need for complex virtual desktop infrastructure deployments that don't scale. Amazon WorkSpaces is available in 13 AWS Regions and provides access to high-performance cloud desktops wherever your teams work.

REAL-TIME RESPONSE FROM ANYWHERE

With only remote access to a corporate system, visibility and quick remediation can be challenging. Falcon provides deep endpoint visibility so you can rapidly investigate incidents and fully understand emerging threats. Direct system access and the ability to run a wide variety of commands enables you to remediate remote hosts and quickly return them back to a known good state.

BUILDING A SAFETY NET STARTS WITH MANAGING COSTS

Businesses around the world are grappling with uncertainty. Scrambling to bolster business resiliency, organizations have paused growth initiatives, locked down budgets, and begun to build up cash reserves. With Amazon WorkSpaces and Falcon, companies have a way to securely enables business operations and keep costs low.

COST-EFFECTIVE CLOUD ARCHITECTURE

The cloud architecture of Amazon WorkSpaces and Falcon flexes with demand and provides enormous storage and computing power to drive real-time protection, regardless of where your employees connect from. As you pivot to support remote employees, there is no need to plan, prepare and provision hardware and software to keep pace, saving you time and money. In addition, Amazon WorkSpaces eliminates the need to over-buy desktop and laptop resources by providing on-demand access to cloud desktops that include a range of compute, memory, and storage resources to meet the performance needs of your remote workers.

FULLY MANAGED FOR LOWER OVERHEAD

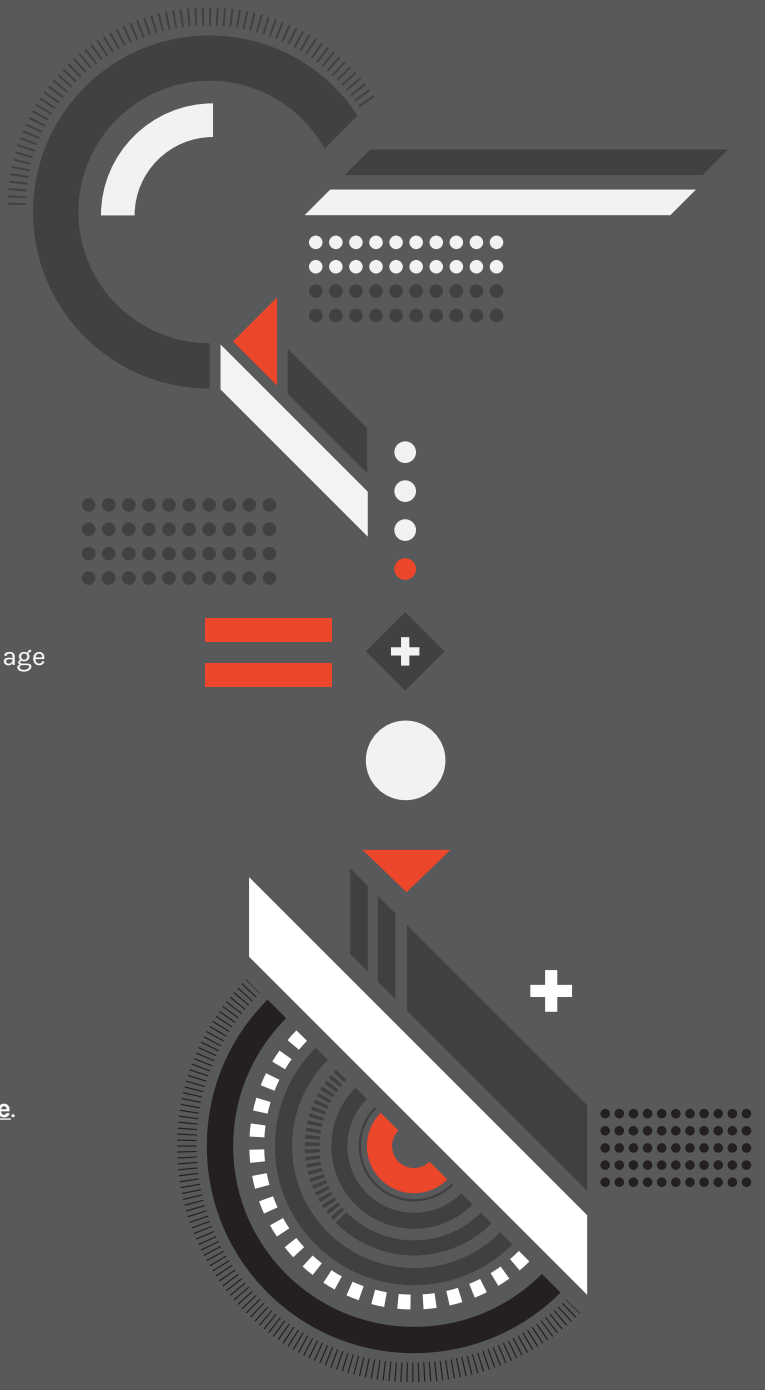
Organizations have the option to bolster their cybersecurity efforts by deploying Falcon's endpoint protection as a fully managed service. This worry-free solution allows you to entrust the implementation, management, and incident response of endpoint security to CrowdStrike's proven team of security experts. The result is an instantly optimized security posture without the burden, overhead, and cost of internally managing a comprehensive endpoint security program.

DEPLOY FALCON ON AMAZON WORKSPACES

Once you've launched a WorkSpaces environment, you can take your current WorkSpaces golden image and create a new image with the CrowdStrike Falcon sensor installed. Then you can use additional WorkSpaces secured by Falcon. Here are the steps to launch a WorkSpace that has a Falcon sensor. For more detail, download the **deployment guide**.

1. Install the CrowdStrike Falcon sensor from your Falcon console
2. Decide between a yearly or metered billing pricing model via the Amazon Marketplace
3. Create a golden image of WorkSpaces
4. Create a bundle in the WokSpaces console
5. Deploy a WorkSpaces environment using the new bundle that includes a Falcon sensor
6. Validate the sensor is installed and running

For more information on CrowdStrike and AWS solutions, visit **CrowdStrike** or the **AWS Marketplace**.



CROWDSTRIKE | aws