CROWDSTRIKE | aws

Work from anywhere with security everywhere

Protect your hybrid workforce, secure your data, and bolster business resiliency with the CrowdStrike Falcon platform on Amazon WorkSpaces

aws PARTNER

- Public Sector
- Amazon Linux Ready
- Marketplace Seller
- Security Software Competency

CrowdStrike eBook

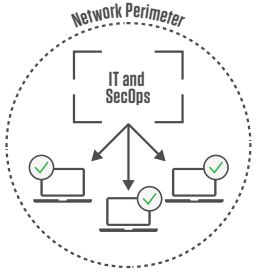
Table of Contents

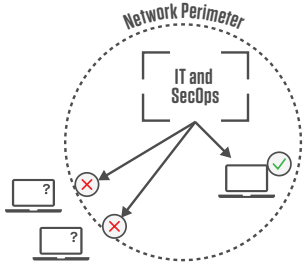
A remote workforce punctures secure perimeters

Remote work is here to stay. The model gaining the most traction is a hybrid one, in which some staff stay fully remote, others return to the office, and still others combine the two, coming into the office for some portion of the week. In this work-from-anywhere world, the challenges of maintaining security and ensuring business resiliency are multiplied at a time when most companies are still struggling to do more with less.

Accelerating cloud adoption meets a growing hybrid workforce

As companies have pivoted to remote work, many have been forced to accelerate their adoption of cloud technologies to keep up, including shifting their cybersecurity models from on-premises to cloud solutions. Now that hybrid work is the new normal, these companies are finding that the approaches they adopted out of necessity under extreme time and operational pressure are not enough to safeguard their hybrid workers—or their data—long term.





In response, forward-thinking companies are adopting a cloud-native cybersecurity approach based on a framework that protects anyone, anywhere.

Real-time protection

Prevent threats, detect suspicious activity and respond to incidents—all in real time, no matter where your users or devices are.

Cloud-delivered

Eliminate complexity, simplify your security stack and deploy in record time. Instantly activate Vulnerability Management and IT Hygiene with Falcon Spotlight™ and Falcon Discover™.

For every device

The single lightweight Falcon agent works everywhere, including across cloud workloads and data centers — protecting users on both company-owned and personal devices.

Six key factors that can help ensure remote worker cybersecurity

1. Make sure you have a current cybersecurity policy that includes remote working.
2. Plan for BYOD (bring your own device) devices connecting to your organization.
3. Be aware that sensitive data could be accessed through unsafe Wi-Fi networks.
4. Cybersecurity hygiene and visibility are critical.
5. Continuous end-user education and communication are extremely important and should include ensuring that remote workers can contact IT quickly for advice.
6. Crisis management and incident response plans need to be executable by a remote workforce.

Protect hybrid workers with Falcon and Amazon WorkSpaces

Securing your workforce identities and your data

With Amazon WorkSpaces, work-from-anywhere 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 cybersecurity threats.

Amazon WorkSpaces provides a desktop-as-a-service solution for hybrid workers

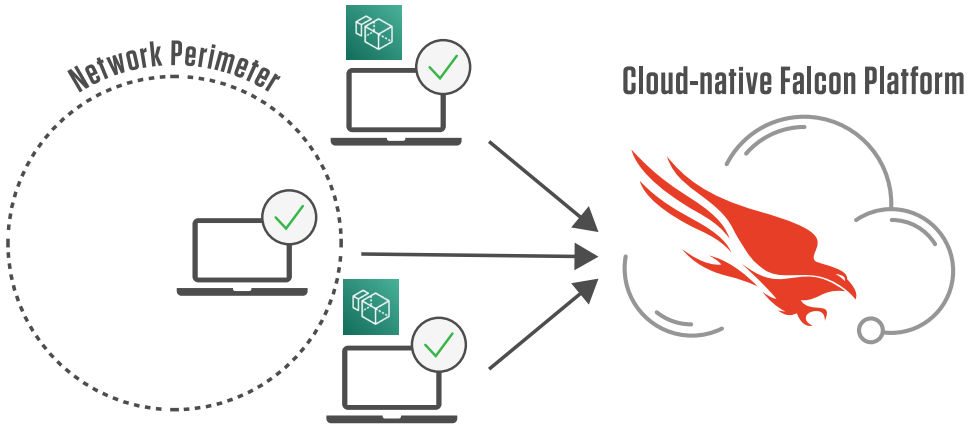
- Deliver a cloud desktop that is accessible anywhere with an internet connection
- Run directly on a wide range of devices, including PCs, Macs, and iPads
- Eliminate administrative tasks such as provisioning, deploying, and maintaining desktops

CrowdStrike Falcon platform stops breaches through frictionless security and 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

CrowdStrike's security approach defends against breaches

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 hybrid solution, and cutting costs through reduced overhead.



80%

of breaches involve compromised credentials

Squelch predatory adversaries

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

Defend against emboldened adversaries

At the heart of every attack is a human adversary. Those threat actors are constantly evolving and using relevant events to disguise their attacks.

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 both your hybrid workers and your cloud data.

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 hybrid workers.

Real-time detection and prevention

Powered by Threat Graph intelligence, Falcon delivers the most effective, real-time detection and prevention of known and unknown threats. Endpoints are protected from adversaries 24/7.

Falcon focuses on more than malware, employing an adversary approach that not only identifies indicators of compromise, but also indicators of attack.

Cybersecurity best practices for a hybrid world

Cybersecurity in a work-from-anywhere world requires a different approach. Systems that secure users in an office require high-bandwidth scanning to identify systems, assess patches, and view vulnerabilities. In a hybrid-work scenario, that setup is no longer feasible. Workers who are in and out of the office, accessing your data on managed and unmanaged devices, create massive blind spots for IT security staff, introducing unknown risks that can slow down efforts to remediate threats.

To meet the cybersecurity challenges of the new world of work, CrowdStrike's experts offer the following best practices:

Empower workers and enlist technology

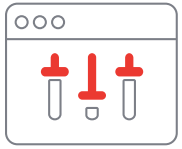
Crafting a comprehensive and effective cybersecurity strategy starts with considering your policies, processes, and technologies across every business function. The most effective cybersecurity strategies blend human resources with advanced technological solutions, such as artificial intelligence, machine learning, and other forms of intelligent automation to better detect anomalous activity and decrease response and remediation time.

Choose your cloud carefully

Not all clouds are equal when it comes to reaping the benefits of cloud technology without compromising security. Amazon Web Services (AWS) was built with the highest standards of data security, with fine-grained identity and access controls for superior visibility. CrowdStrike's industry-leading prevention and detection capabilities for Amazon WorkSpaces support your remote workforce without affecting business continuity.

Enable 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 from anywhere 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.



Simplify desktop delivery

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.

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 enable business operations and keep costs low.

Cost-effective cloud architecture

The centralized management capabilities of Amazon WorkSpaces for remote workers helps scale access to cloud desktops. As you continue to support your hybrid workforce, 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 hybrid workers. The CrowdStrike Falcon platform scans all endpoints to help keep them secure no matter where they're located and without performance impact.

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.

It's time to secure your work-from-anywhere world

CrowdStrike makes it easy to get started. To learn more about implementing CrowdStrike Falcon platform, and/or Amazon WorkSpaces, **try our 15-day Free Trial.**

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