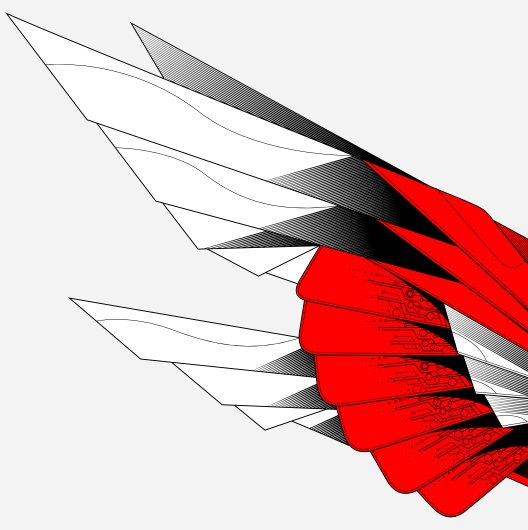
STAY ONE STEP AHEAD OF EMERGING WORKLOAD THREATS

- 92% OF ORGANIZATIONS CURRENTLY HOST THEIR IT ENVIRONMENTS IN THE CLOUD
- DATA LOSS, LACK OF VISIBILITY, IDENTITY, AND UNAUTHORIZED ACCESS WERE THE HIGHEST-RANKED CLOUD THREATS IN 2021
- RESPONSE TEAMS CAN ONLY RESPOND TO 3-5 PERCENT OF THE SECURITY EVENTS THEY RECEIVE EACH DAY



PROTECT YOUR CLOUD ENVIRONMENT WITH A MULTILAYERED DEFENSE-IN-DEPTH STRATEGY FROM CROWDSTRIKE AND AWS

Defense-in-depth is an architectural design based on military strategy that requires attackers to breach multiple lines of defense. In the context of protecting cloud workloads, defense-in-depth relies on layers of defensive mechanisms—visibility, prevention, and remediation—to safeguard your valuable data, information, and intellectual property.

CrowdStrike's leading endpoint and workload protection solutions and threat intelligence directly integrate with AWS services, creating an effective, defense-in-depth solution for staying one step ahead of threats.

VISIBILITY DRIVES CLARITY

Defense-in-depth starts with visibility—you can't protect what you can't see. Together, CrowdStrike and AWS provide insight into what data, applications, and assets are being used so you're ready to face attacks. CrowdStrike solutions enable you to view configurations of all components, aggregate network traffic entering and leaving the workload, audit API calls, and provide runtime visibility.

PREVENTION INSPIRES ACTION

Once you see the threats you're facing, you can act against them. CrowdStrike and AWS's defense-in-depth approach adds a layer of prevention, using aggregation and correlation to detect anomalous behavior in your workloads. CrowdStrike Falcon Discover and Falcon Sensors bring together discovery and audit information with runtime visibility from multiple AWS sources and provide alerts so you can act.

REMEDIATION SCALES RESPONSE

Take action where it counts. To reduce the burden on your security team, CrowdStrike Falcon Integration Gateway and Falcon API can push high-risk events into AWS Security Hub, kicking off remediation workflows and even blocking the specific domain or IP that is considered malicious.

START YOUR FREE TRIAL ON AWS MARKETPLACE

Staying one step ahead starts with taking the first step. Experience how CrowdStrike and AWS defense-in-depth layers come together to mitigate and remediate threats.

START FREE TRAIL