CROWDSTRIKE

CrowdStrike Cloud Partner

Solution Brief

CrowdStrike and AWS: Zero Trust integration

Securing work beyond the perimeter with Zero Trust to modernize security across enterprise environments

Challenges

Hybrid and remote work environments have become a normal way of doing business for many organizations. Globally distributed workforces, business partners and their respective devices move on and off the office network. Many applications were once hosted in data centers, but they have been migrating to the public cloud or have been outright replaced with software as a service (SaaS) solutions. With the rise of remote work, cloud-hosted workloads, and SaaS applications, the corporate network as a security perimeter is no longer an effective model.

Traditional solutions that prioritize a secure network perimeter often do not consider device posture before allowing a device to access network resources. A castle-and-moat approach does not allow IT teams to control secure application access through the cloud. In tandem with strong identity-based access controls, security teams need to consider the security posture of the originating user endpoint to protect user-to-application connectivity from end to end. To deliver on this, organizations need advanced security capabilities to collect, correlate and analyze an increasing volume of endpoint telemetry and provide context at the right time.

Solution

Many organizations have begun adopting a Zero Trust model to protect beyond the perimeter. Zero Trust requires all users — regardless of location — to be authenticated, authorized and continuously validated for security configuration and posture before being granted access to applications and data. The applied model typically focuses on identity, user device posture and access policies as key criteria. Zero Trust is established by applying these criteria when a user tries to access a sensitive application and then adjusting access rights in response to security context changes.

CrowdStrike and AWS are working together to remove barriers and simplify the implementation of Zero Trust for organizations by delivering an integrated end-to-end security solution from endpoint to application. This security solution gives teams a real-time view of a device's security posture and bases access to critical applications on granular access policies. The CrowdStrike Falcon® sensor at the endpoint shares data with AWS Verified Access to automatically apply and adjust security policies based on user context, newly detected indicators of compromise (IOCs) and device health.

CrowdStrike Falcon® Insight XDR delivers continuous, real-time security and compliance checks for endpoints, ensuring authentication and authorization are only granted to devices when they comply with the organization's approved security posture.

AWS Verified Access securely connects users to applications hosted in private AWS VPC subnets based on a user-configurable policy and without requiring a VPN. The device posture score is derived from a CrowdStrike-provided dynamic CrowdStrike Falcon® Zero Trust Assessment (ZTA) score, which AWS can use to adaptively enforce policies to access applications. The Falcon ZTA security score is based on built-in endpoint operating system (OS) security configuration settings and package vulnerabilities as well as Falcon sensor status, including prevention, detection and real-time response policies.

As organizations look to enable more remote and hybrid work strategies, this joint CrowdStrike and AWS solution simplifies the requirement to provide users with safe, seamless and secure access to the business-critical applications employees need to do their jobs. All of these capabilities can be delivered with a foundation of Zero Trust.

Use Case

Consider a common scenario where a contractor is accessing a sensitive enterprise application. Given the time-bound nature of contractor engagements combined with budgetary constraints, companies frequently allow contractors to use their own laptops. Without a Zero Trust access capability, contractors typically connect by VPN and access what they need. This common practice typically exposes much more to the contractor than the single application they need. In most cases, companies do not check endpoint security posture scores as a condition for access, which makes contractor laptops a desirable target for adversaries looking to gain access to a target company. If an adversary can breach the defenses of an unmanaged laptop (which may not have adequate security controls or be subject to vulnerability patching requirements), a VPN gives them free rein to continue discovery and move laterally using the contractor's identity.

Together with AWS Verified Access, Falcon Zero Trust changes the game. After setting up AWS Verified Access once per private application, the company can provide a single-use key to the contractor to install the Falcon sensor, with simple directions to deploy the Native Messaging Host and Chrome plugin, which are both provided by AWS. Then, when the contractor connects to the web app using their Chrome browser, their access credentials and laptop posture score determine whether they are connected. If they are denied, the company's cybersecurity team can review findings in the Falcon console to determine how to improve the endpoint's security and posture score so that the contractor can safely access the application. Once the contractor gains access, adversary-based attacks against the contractor laptop are blocked in real time, and even if an adversary manages to steal credentials and log in, they will have a reduced access surface and little chance of lateral movement.

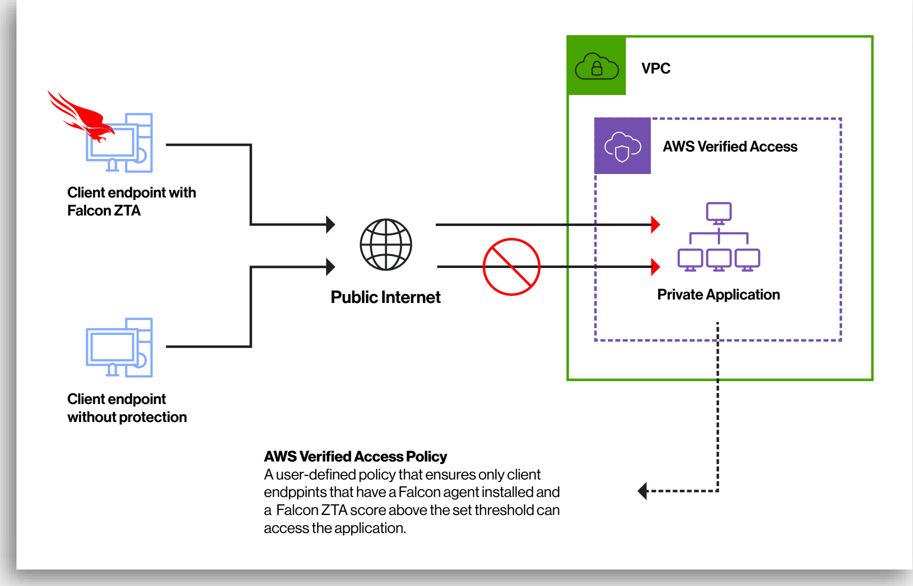
How It Works

STEP 1: THE CROWDSTRIKE FALCON PLATFORM EVALUATES DEVICE POSTURE WITH FALCON ZTA

With Falcon Insight XDR and Falcon ZTA scores enabled, the CrowdStrike Falcon platform collects OS and sensor settings from an endpoint device and calculates its Falcon ZTA score. Any changes in settings will automatically trigger a recalculation of the Falcon ZTA score. By comparing the Falcon ZTA score with the organization's baseline score, CrowdStrike can measure the health of the user's device relative to the organization's baseline and recommended best practices over time.

STEP 2: AWS VERIFIED ACCESS IMPLEMENTS ACCESS POLICIES

AWS Verified Access implements Zero Trust access policies in two layers. First, the AWS Native Messaging Host checks if the CrowdStrike Falcon sensor is running on the endpoint device. Next, the Native Messaging Host reads the device's Falcon ZTA score and compares it against the policy threshold defined for selected business-critical applications. If these conditions are met, access to applications is granted across a secure channel between the Chrome browser extension and AWS Verified Access. If not, then access is denied. Access policies on the AWS dashboard can be adjusted to change the threshold of the score based on the organization's requirements and changing conditions over time.


VPC
AWS Verified Access
Client endpoint with Falcon ZTA
Public Internet
Private Application
Client endpoint without protection

AWS Verified Access Policy
A user-defined policy that ensures only client endppints that have a Falcon agent installed and a Falcon ZTA score above the set threshold can access the application.

AWS is a trusted CrowdStrike Cloud Partner, providing integrated solutions with CrowdStrike to deliver comprehensive defense-in-depth protection from endpoints to the cloud.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.