SAFEGUARD ENTERPRISE ACCESS

Appgate SDP integrates with CrowdStrike to provide dynamic and intelligence-aware Zero Trust access.

CROWDSTRIKE

THE PROBLEM

Organizations are experiencing a profound shift in the way people work. The workforce is transient, working anywhere, connecting a multitude of devices to resources in the cloud and data centers. These factors have increased the attack surface immeasurably, and conventional, perimeter-centric security models may not be equipped to handle the complexity and sprawl of today's IT environment.

At the same time, digital transformation—driven by growth in cloud computing, software as a service (SaaS), mobile devices, the Internet of Things (IoT) and similar technologies—has changed the nature of cybersecurity risks by increasing the number of entry points to the network.

To secure network access, you need a modern approach that protects all remote and on-site workers; modern, legacy and custom apps in distributed cloud, hybrid cloud and multi-cloud environments; and all locations including HQs, branch offices and data centers.

You need a solution that meets today's threats head-on and one that can future-proof your environment for tomorrow's risks.

THE SOLUTION

Appgate SDP offers endpoint intelligence-aware integration with CrowdStrike, providing a flexible, scalable mechanism that gives enterprises a frictionless path to achieving Zero Trust.

Appgate SDP integrates with CrowdStrike Falcon® Zero Trust Assessment (ZTA) to enable scalable endpoint risk scores, provided by CrowdStrike, to dynamically restrict access of risky endpoints or users, even during an established session. Admins can dynamically grant, restrict or block access via Appgate SDP, an industry-leading Zero Trust Network Access solution (ZTNA), to corporate resources based on real-time risk detections and indicators of compromise.

Get secure access with confidence and zero compromise for all private applications, workloads and resources. No matter your users' ultimate destination, protection and security are assured.

BENEFITS

Improve security posture by extending conditional access to compliant devices

Automatically assess risk by ensuring that only low-risk devices and authenticated users are granted access

Simplify administration and improve operational efficiency while achieving Zero Trust access

Streamline response and containment should a threat be identified

APPGATE SDP ADVANTAGES

Ability to overlay on top of systems that have already been deployed, allowing customers to leverage existing security investments

Support for hybrid IT environments, including on-premises and remote workforce

Easy to configure risk-based access matrix

"Organizations deploying a Zero Trust security architecture need full visibility into their risk environment, even as it continuously evolves. Appgate SDP works with CrowdStrike Falcon ZTA to dynamically assess user, device and workload risk postures not only at the time of authentication but throughout each user interaction."

- Leo Taddeo, CEO, Appgate

DEPLOYMENT OVERVIEW

In the combined solution, the CrowdStrike Falcon platform collects enriched security telemetry, powered by the CrowdStrike Security Cloud and world class AI, at regular intervals. These include continuous real-time security posture assessments across all endpoints via Falcon ZTA. During user sessions, appgate SDP can be configured to query CrowdStrike on a programmable basis for Falcon ZTA risk scores. This information can be re-evaluated at multiple times, including at the time of authentication and at the point of access.

The Appgate SDP risk model makes it easy to create dynamic entitlements based on a simple matrix interface to allow, prompt for action or deny access based on a low, medium or high ZTA risk score measured against the sensitivity of the resource being accessed.

Falcon ZTA device risk scores are captured in Appgate SDP as claims and used in policies, entitlements and conditions.

Device claims are used by Appgate SDP administrators to make conditional, dynamic, just-in-time access decisions and grant entitlements based on risk. Actions can be configured to allow, limit or deny access, including prompting the user for multi-factor authentication (MFA).

The integration between Appgate SDP and CrowdStrike Falcon ZTA reduces the attack surface and security exposure to enterprise applications by limiting access from high-risk devices and keeping critical resources secure.

SAMPLE USE CASE

Security professionals and network administrators can achieve a more mature Zero Trust security posture by integrating ZTNA with their endpoint protection technology. Appgate SDP, integrated with Falcon ZTA intelligence, can dynamically grant, restrict or fully block access to corporate resources based on real-time risk detections and indicators of compromise.

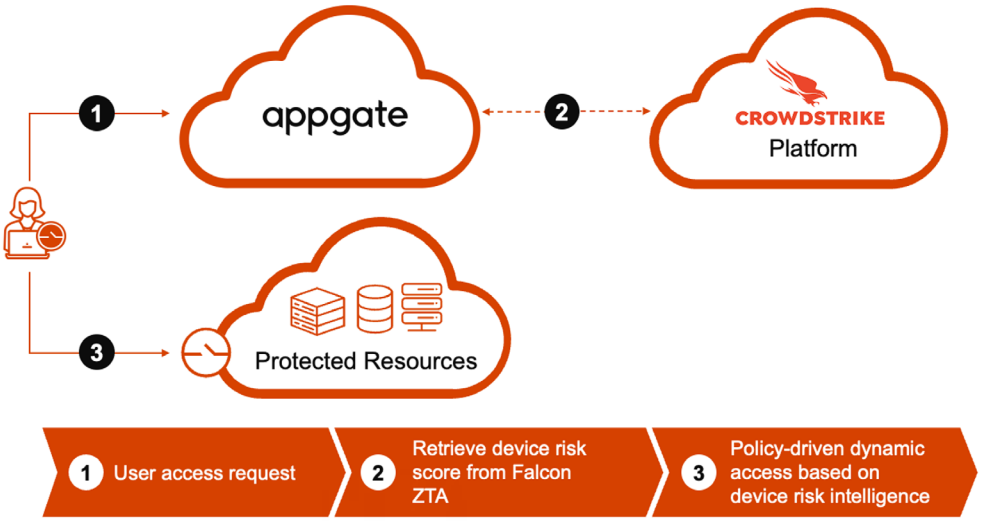
Dynamic Endpoint Posture Adjustment

In this scenario, Appgate SDP retrieves the device risk score from Falcon ZTA to gather device risk and compliance posture for endpoints requesting access through Appgate SDP. When Falcon ZTA detects an at-risk device, Appgate SDP automatically adjusts conditional access entitlements of the affected devices based on policy.

Entitlements are now adjusted based on the risk levels reported by Falcon ZTA dynamically. This reduces risk without disrupting business.

Appgate SDP and CrowdStrike Falcon ZTA

CrowdStrike and Appgate Integration



About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com

appgate