



Solution Brief

CROWDSTRIKE AND AKAMAI INTEGRATION: ENTERPRISE APPLICATION ACCESS

Enabling more granular secure application access with real-time endpoint events

CHALLENGES

Today's users, devices, applications and data are more distributed than ever, and enabling secure access for remote users is critical. Delivering the right level of application access, regardless of where users and applications reside, is key to ensuring corporate security posture.

SOLUTION

The integration of the CrowdStrike Falcon® platform with Akamai's Enterprise Application Access enables endpoint telemetry, including threat detections, from CrowdStrike to enrich existing context and deliver more intelligence for enhanced secure access to corporate applications.

BUSINESS VALUE

Use Case/Challenges	Solution	Benefits
Organizations may lack coordinated security controls across applications and user endpoints.	Akamai's application access solution enables comprehensive visibility into all endpoint events and grants application access based on security posture and events telemetry.	Conditional access for endpoints into applications is granted and continuously monitored for better security.
Standalone siloed threat data that lacks integration can prevent breach detection and remediation.	Correlated data with enhanced threat signals improves detection and response.	Applying CrowdStrike® threat intelligence to Akamai's policy enforcement point enables faster time-to-detection and better decision-making for secure application access in real time.
Traditional secure application access is on-premises, VPN-based, and difficult to maintain, scale and secure.	Akamai's edge platform and CrowdStrike Falcon are cloud-based, making them easier to scale, manage and maintain with minimum downtime.	The solution is easy to deploy and manage, with no need to maintain or update legacy-based systems.

KEY BENEFITS

Enhances Zero Trust network access by leveraging real-time endpoint telemetry for application access decision-making

Grants deeper visibility into real-time application access for end-user devices

Provides console integration for easier reporting and faster response and remediation



**CROWDSTRIKE AND AKAMAI INTEGRATION:
ENTERPRISE APPLICATION ACCESS**

TECHNICAL SOLUTION

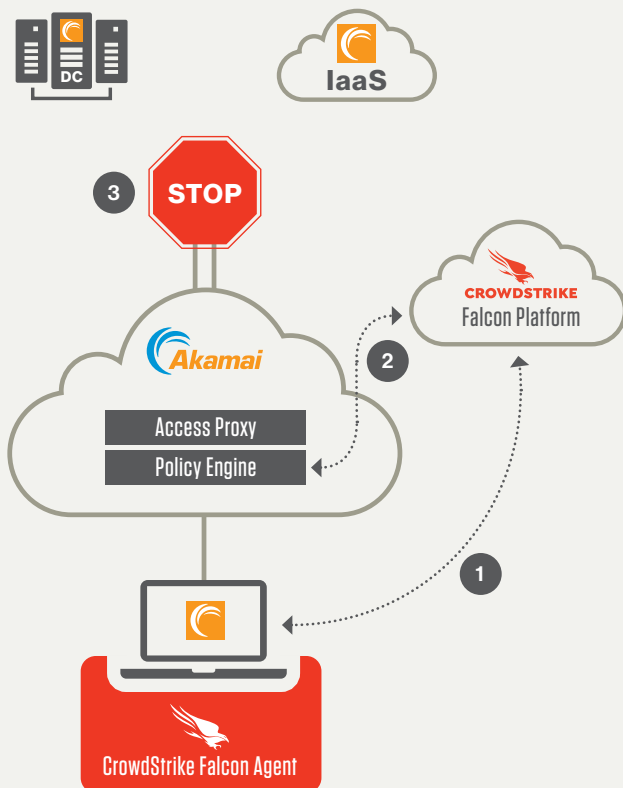
The CrowdStrike and Akamai API integration functions as follows:

The CrowdStrike Falcon agent sends endpoint telemetry to the CrowdStrike Falcon platform. Akamai's Enterprise Application Access device posture functionality accesses this information from the Falcon platform on the customer's behalf, using APIs and customer credentials.

Akamai uses Falcon agent signal values to classify the risk posture of devices as low-, medium- or high-risk and determines application access authentication. This reduces security exposure to enterprise applications by limiting access from high-risk devices, in addition to securing critical data.

Granular visibility into the Falcon agent from within Enterprise Application Access is enabled by independent validation with the Falcon agent. This visibility includes the version of the Falcon agent and identifying information about the agent and user, as well as the health of the sensor based on its recent contact with the Falcon platform. It also includes details on the timing of the contact between the sensor and the cloud platform for deeper threat visibility. Reporting can be created within the Enterprise Application Access console for users with enabled Falcon agents.

This integration helps organizations make better, more granular application access decisions within their environments. In the event that an endpoint device may have been compromised, this joint solution prohibits the potentially compromised device from accessing corporate applications and sensitive data.



- 1 The CrowdStrike Falcon agent sends data to the CrowdStrike Falcon platform and enables posture validation.
- 2 Akamai Enterprise Application Access, configured with customer credentials, accesses the Falcon platform on the customer's behalf.
- 3 Akamai Enterprise Application Access can use "poor" CrowdStrike signal values to classify devices as medium- or high-risk and block application access.

**CROWDSTRIKE AND AKAMAI INTEGRATION:
ENTERPRISE APPLICATION ACCESS**

ABOUT AKAMAI

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com and @Akamai on Twitter.

Find global contact information at www.akamai.com/locations.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Learn more www.crowdstrike.com

