Inform your zero trust access policies with device security posture from Crowdstrike

Axis Security with CrowdStrike integration combines endpoint with access controls to offer organizations a zero trust architecture solution with the agility and flexibility to succeed today and in the digital future.

Zero Trust from Endpoint to Application

Zero Trust architecture requires more than a single login check against an access list. Modern attacks take advantage of static perimeter-based access security. They hijack endpoints and use malformed requests to foil static access control points or to gain internal network access via VPNs, and often there is no subsequent monitoring of activity with the target application.

A more solid approach involves Zero Trust Network Access (ZTNA) Secure Access Service Edge (SASE) solutions like Axis Security's Application Access Cloud, which integrates with CrowdStrike's Falcon Platform to ensure only secured, protected endpoints can access your applications locally or in the cloud – and then brokers every request and monitors the entire connection session.

The Application Access Cloud enforces full zero trust access controls no matter where the applications live or where the users are logging in from. It's end-to-end protection from device to network to app, including features like adaptive access controls, user monitoring, and the ability to revoke access and end sessions if risks are identified.

The Axis Security and CrowdStrike Integration

Unlike network layer access solutions such as VPNs, Axis operates at the application layer to enforce permission controls over user requests such as login, view, edit, upload, download, copy/paste, print, and delete. Axis screens these granular application requests inline and queries CrowdStrike's Zero Trust Assessment API to identify if a device is currently protected. This informs the Axis policy enabling it to admit only Crowdstrike protected, sanctioned endpoints if that is specified in the policy.

Rogue endpoints, unknown sources, and even IP-spoofed addresses without the CrowdStrike Endpoint Protection product can be automatically blocked and Axis will track that a request to access has been denied.

- Ensure only Crowdstrike protected endpoints can access critical applications and resources.
- Enforce centralized access policies through granular, zero trust controls with device posture checks.
- Integrate with SIEM and SOAR systems with intelligence to accelerate investigations and incident response.
- Continuously monitor user behavior, log granular user requests at the application layer, and capture real-time recordings of full user sessions.
- Reduce overhead by eliminating the need for costly and complex VPN and/or VDI solutions.
- Improve overall access security posture to a zero trust model.

Benefits

- **Reduce Complexity** – The App Access Cloud and CrowdStrike are both architected and implemented 100 percent in the cloud. An integration is simple and fast to implement. Security access policies are managed from a simple, intuitive interface that secures not only the connection, but continuously authorizes and monitors every user request.

- **Reduce Risk** – The Axis Security Application Access Cloud eliminates inbound attack surfaces for an organization; doesn't enable users directly onto the internal network; isolates potentially vulnerable applications from direct contact with users, devices, networks, and the public internet; and strictly enforces least privilege access by placing every access session into a zero trust model.

- **Gain Behavioral Awareness** - Axis continuously monitors every user request and gives you visibility over specific behavior from a user or users. Does that user session look like reconnaissance with lots of views? What SSH commands did the user enter? What database tables did they access? Did the user create new assets, content, or accounts? Did the user download anything? Axis lets you see what was accessed by which accounts and devices, with the ability to export incident data or integrate with your SIEM as well.

- **Gain Consistency** - Enable, control, and manage secure remote access for all your users to every application, port, and protocol they need through one unified zero trust solution.

Automate Adaptive Controls – and Faster Revocation

The Application Access Cloud operates inline at the cloud edge. Through API integration, incoming application requests are correlated against endpoint data from CrowdStrike Falcon to automatically identify unsanctioned endpoints and facilitate granular allow/deny/limit policy controls based on endpoint hygiene.

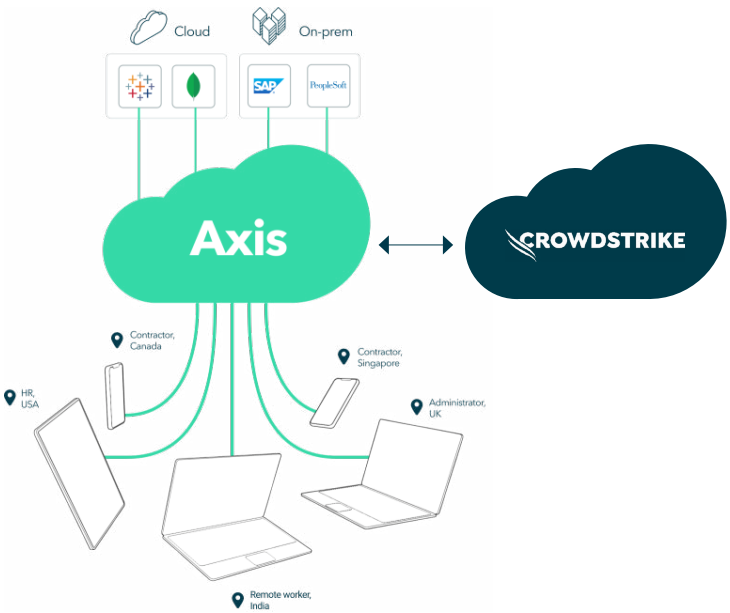
In the scenario of a trusted user attempting to connect to an application via an untrusted device, Axis Security's easy to configure policies can still allow the connection but restrict usage to read only without the ability to download, upload, copy/paste, or print from the untrusted device. In this way, only CrowdStrike endpoint-protected devices can be given full application access and permissions.

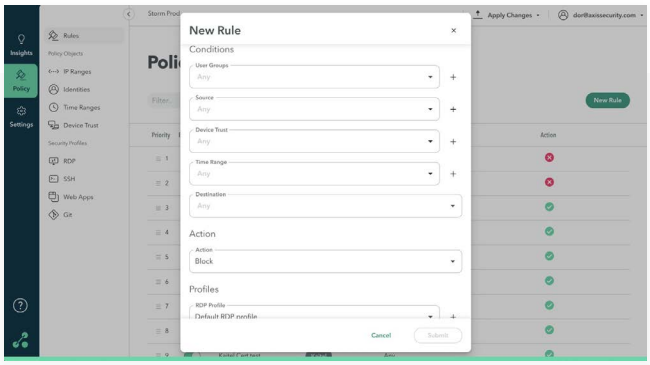
Once connected, Axis continuously monitors user activity to keep a record of which user coming from which device performed which actions in the event of incidents.

App Access Cloud policies can enforce conditional access to business-critical applications using an API integration with Crowdstrike. Axis Security policies use device security posture data on Crowdstrike protected endpoints to inform policy decisions. Instead of traditional all-or-nothing access, Axis policies are flexible and granular so access can be completely restricted, increased monitoring can be initiated, or access can be limited to read-only when users request access from a device not protected by Crowdstrike.

Protection for Any App, Any Device, Anywhere

1. App Access Cloud provides context-based access informed by device posture
2. Unsanctioned devices are denied access, or subject to other restrictions.
3. App Access Cloud establishes the session and brokers the allowed activity of the user to each application
4. App Access Cloud continuously authorizes each user request. Unauthorized requests are not transmitted to the application. Policies are continuously enforced so if context for access changes App Access Cloud can enforce a policy change mid-session.





+

Adding Device Posture Policies

App Access Cloud policy rules are simple to create and manage. It only takes a few minutes to set up an integration with Crowdstrike Falcon and then it is a simple point and click to add the Crowdstrike device posture check to an access policy.

Endpoint to App Protection in the Cloud

Axis Security's Application Access Cloud is a revolutionary new solution that makes business access amazingly simple. App Access Cloud connects users to apps without ever touching the network or the apps themselves. This eliminates the need for VPNs, agents, or appliances, which reduces the attack surface and allows access controls to be simpler and safer. By collecting and analyzing real-time user behavior, App Access Cloud continuously ensures the right users access the right apps for authorized tasks.

3 East Third Ave, Suite 203
San Mateo, CA 94401

+1.650.850.8991
info@axissecurity.com

© **2021** All rights reserved to Axis Security