CrowdStrike FAQ

CROWDSTRIKE

TRUSTING ZERO TRUST

How CrowdStrike makes a complex security architecture less complex and more effective

Q WHAT IS A ZERO TRUST SOLUTION ARCHITECTURE AND MODEL?

A Zero Trust is a holistic approach to an overall contextual-based security architecture for protecting all customers' computer assets, applications and data, regardless of who or where the user is, or where assets are located. The fundamental concept of Zero Trust is "don't trust anybody or anything operating inside or outside your network at any time." To use Zero Trust successfully, organizations must be able to constantly validate, with confidence, that both the user and the computing asset have the right identity, privileges and attributes for access. Zero Trust takes into account continuous, real-time attributes encompassing user identity, organizations' associations, endpoints, networks and more before allowing or maintaining user access to an organization's networks, applications and data. In the Zero Trust world, there is no concept of inside or outside of the customer's network. Since threats and security posture attributes are temporary by nature, attribute collection and selection of who gets access to what must be a continuous, near real-time process. Fundamentally, the Zero Trust model is a set of design principles and not something that can be implemented using a single product.

Q WHY ARE U.S. GOVERNMENT AGENCIES AND OTHERS TRENDING IN THE DIRECTION OF A ZERO TRUST MODEL?

A Legacy security architectures carry significant risks that have resulted in public breaches of information from both internal and external threats. Zero Trust security is an emerging approach that promises to better mitigate these risks. However, because it is a new approach, the risk of implementation failure is high and is compounded by factors such as implementation complexity. One area that increases complexity is adding more tools, agents and consoles that can drive the need for additional integrations, operations and updates. Having a consolidated platform, agent and application program interface (API) strategy will dramatically lower the risks associated with implementing, operating, updating and maintaining a successful Zero Trust approach.

Q WHAT IS THE CROWDSTRIKE FALCON SOLUTION?

A The CrowdStrike Falcon® platform is a cloud-delivered, FedRAMP-authorized (Commercial and EU Clouds), modular cybersecurity intelligence and endpoint security solution that uses an open API platform with a single lightweight agent to provide visibility and security across Windows, Linux, Mac, iOS and Android operating systems. It protects all workloads regardless of whether they are running on mobile devices, laptops, desktops, servers, virtual machines or IoT devices, or in containers or the cloud — AWS, Google Cloud Platform and Microsoft Azure. The Falcon platform operates on- or off-network, even in disconnected, intermittent or limited-bandwidth environments and includes a robust suite of APIs for third-party integration.

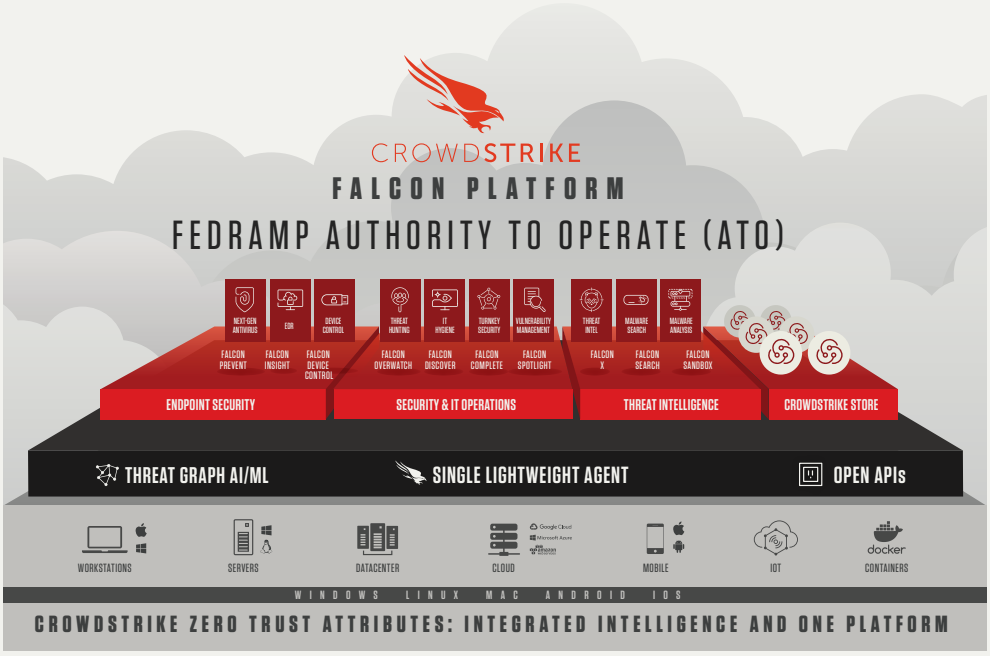
Q HOW DOES THE CROWDSTRIKE FALCON PLATFORM HELP IMPLEMENT ZERO TRUST?

A The CrowdStrike® Falcon platform provides real-time, continuous visibility and security across your assets regardless of whether they are on or off your enterprise network. Based on the modules you select, Falcon provides access to the attributes needed to make Zero Trust policy enforcement decisions. Some of the Zero Trust attributes that Falcon can provide include endpoint hardware type, firmware version, operating system version, patch level, vulnerabilities, applications installed, user logins, and security or incident detections. It is important to note that the collection of these attributes is not a one-time scan or event for compliance. The continuous efficient collection of visibility and security attributes is extremely important, as endpoints and people change and adversaries never give up.

Q WHAT SORT OF ECOSYSTEM DOES ZERO TRUST NEED?

A Zero Trust requires the right leadership, policies, architecture, products, integrations and operations to be successful. With fewer products needed for your Zero Trust implementation, there will be less complexity required to build, operate and maintain it. The CrowdStrike cloud-delivered Falcon platform with its single universal agent architecture provides the capabilities needed to replace multiple legacy products from vendors such as Symantec, McAfee, Trend Micro and others. The CrowdStrike partner ecosystem enables an effective, holistic approach using integrations that are easily accessible via the CrowdStrike Store. Current ecosystem partners include Zscaler, Netskope, Okta, Proofpoint, Forescout, Splunk, AWS, Google, Vectra Networks and many others. Using CrowdStrike's Falcon platform — with its open JSON/RESTful APIs and additional standards-based integration capabilities such as SAML (Security Assertion Markup Language), OAuth 2 and others — makes adding mission-specific integrations easy.

The CrowdStrike Falcon platform offers government entities next-generation visibility and security across all endpoint types used for your mission and includes a seamless path to help support your Zero Trust initiatives.



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 3 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.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**