CROWDSTRIKE

CROWDSTRIKE ZERO TRUST

A frictionless Zero Trust approach for the enterprise

CHALLENGES

In flat networks and hybrid enterprises, conventional Zero Trust technologies with static policies built around hardware firewalls, VPNs and VLANs have limited efficacy, scalability and manageability. The traditional perimeter has dissolved — users, endpoints, applications and workloads are distributed across on-premises and multiple clouds. When users access applications and resources that reside anywhere, from a mix of company-issued and unmanaged endpoints from any location, the enterprise becomes more vulnerable to sophisticated threats.

SOLUTION

The CrowdStrike Zero Trust solution secures the modern enterprise with its cloud-delivered approach to stop breaches in real time on any endpoint, cloud workload or identity, wherever they are. CrowdStrike does all of the heavy lifting for enterprise security teams to enforce frictionless Zero Trust with its industry-leading Security Cloud. The CrowdStrike Security Cloud processes trillions of events per week, enabling high-fidelity attack correlation and real-time threat analytics and response that can scale any deployment model, whether they are multi-cloud or hybrid enterprises that may also run legacy and proprietary applications.

KEY BENEFITS

Start the Zero Trust journey in a phased manner (e.g., starting with identity protection and extending to cover endpoints and workloads, or vice versa)

Realize value from Day One by enabling instant protection without hardware or storage provisioning, reboots and complex configurations

Eliminate the security complexity involved with managing terabytes of data, threat intelligence feeds, and hardware and storage management with a unified, cloud-native approach

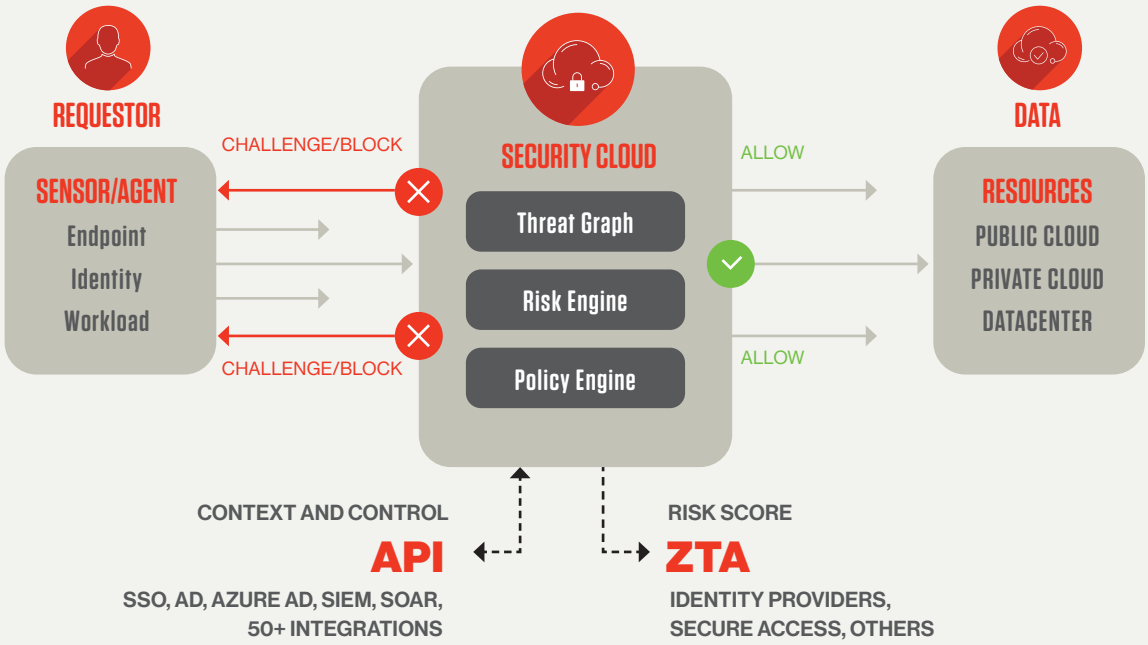
Stop breaches such as supply chain attacks, ransomware exploits and other sophisticated threats in real time from any endpoint, workload and identity

Realize frictionless Zero Trust security with high-fidelity cloud-delivered attack correlations, behavioral risk analytics and policy enforcement, and reduce the blast radius across on-premises and multi-cloud data centers

Improve security operations center (SOC) analysts' mean time to detect and respond to sophisticated threats by reducing the need for cumbersome log analysis

KEY CAPABILITIES

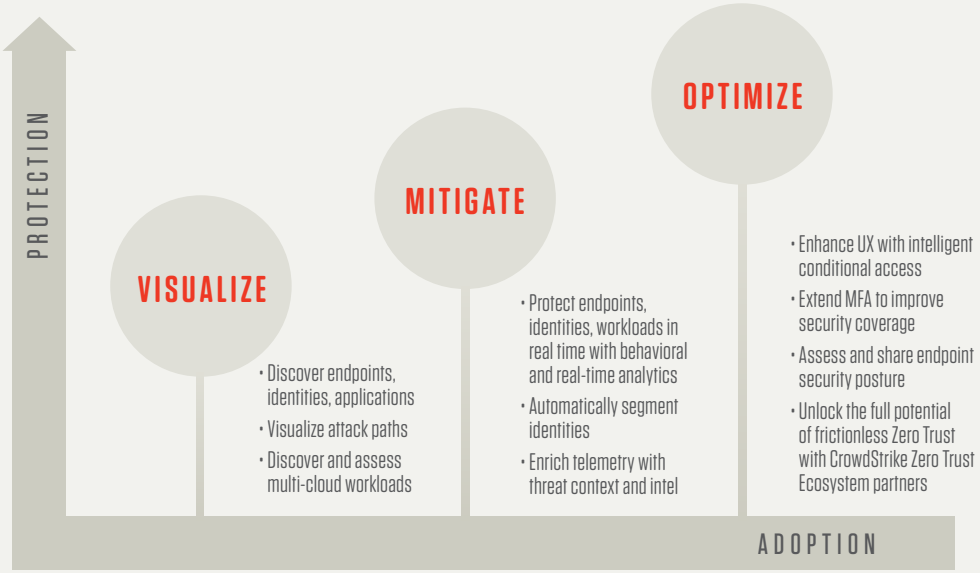
CrowdStrike follows the **NIST SP 800-207 framework**, widely followed by governments and private organizations, to enable security in the cloud-first, work-from-anywhere environment.



KEY PRINCIPLES OF ZERO TRUST

- **Understand behavioral data:** Are users accessing the applications or resources they are supposed to? Is there protocol misuse such as a regular user doing Remote Desktop Protocol (RDP) to a Domain Controller (DC)? Is there suspicious behavior using privileged credentials?
- **Limit the attack surface with segmentation:** Limit the scope of what applications can do; control where regular users, third-party contractors and privileged users can go; and limit what service accounts can access with segmentation. Apply the principles of least privilege and dynamic risk assessment to reduce the attack surface.
- **Automate security tied to context:** Use signals from users, devices, networks and workloads to gain unified visibility, improve analytics, enforce policies and automate security — all tied to context to improve the fidelity of alerts and incident response.
- **Continuously verify accesses with the least friction:** Verify every access to applications, resources and workloads with deep knowledge of the risks and deviations, and not based on trust or access timeouts (i.e., continuously monitor what's happening even after granting access to a resource). The key is to verify access continuously without degrading the user experience or affecting business productivity.

SCALABLE AND FLEXIBLE FRICTIONLESS ZERO TRUST JOURNEY



The CrowdStrike Zero Trust Journey

By adopting frictionless CrowdStrike Zero Trust aligned with the key principles described, the enterprise can realize maximum coverage across its hybrid enterprise by protecting endpoints, identities, and applications and workloads.

The CrowdStrike Zero Trust journey involves only two components: the **CrowdStrike Falcon® sensor** and the **CrowdStrike Security Cloud** that provides security automation and analytics to intelligently enforce policies with the least friction for users and IT and security teams. With industry-leading sets of endpoint, workload, container and identity telemetry, threat intelligence and AI-powered analytics, security teams can automatically predict and prevent modern threats in real time. CrowdStrike's cloud-native approach is the only solution that empowers security teams to achieve Zero Trust protection without the combined overhead of managing terabytes of data, threat feeds, hardware and software, and related ongoing personnel management costs.

The enterprise can start the Zero Trust journey with CrowdStrike identity protection and extend the CrowdStrike Zero Trust solution to cover the other most vulnerable areas such as endpoints or workloads. Falcon sensors can be deployed in minutes to tens of thousands of endpoints in a day.

Existing CrowdStrike customers can easily continue their Zero Trust journey with the power of the CrowdStrike Security Cloud, without additional hardware, storage provisioning and personnel costs.

VISUALIZE

CrowdStrike Zero Trust provides granular visibility across endpoints, users and multi-cloud workloads to help security teams understand what's happening in hybrid environments and accurately assess threats and attack paths.

Discover all endpoints, identities and applications: Discover managed and unmanaged endpoints and identify systems that could be a risk on the network, such as unprotected "bring your own device" (BYOD) or third-party systems, with the inventory of all systems in the network. Discover privileged account activity with complete visibility of the usage and creation of administrator credentials to identify unusual behavior across on-premises and cloud environments. Understand application inventory along with unwanted and vulnerable applications. Identify all applications that are running in your enterprise, along with versions, hosts and users. Visualize suspicious applications in the network, and pinpoint unprotected or unmanaged applications that impact security posture.

Get full attack visibility across endpoints, identity stores, workloads and container environments: Unravel an entire attack happening across endpoints in an intuitive process tree with complete context enriched with threat intelligence data. Gain multi-directory identity store visibility to understand the scope and impact of identities and their privileges across Microsoft Active Directory (AD) and Azure AD. Integrate with single sign-on (SSO) and federation solutions, such as Active Directory Federation Services (AD FS), PingFederate and Okta to get the big picture of what users are doing in the organization. Get visibility into cloud workloads and container environments, identify images, registries and libraries, and understand file access, network communications and process activity with full visibility into running containers.

Discover and assess multi-cloud workloads: Automatically discover existing cloud workload deployments with real-time information about workloads including context-rich metadata about system size and configuration, networking, and security group information for AWS, GCP and Azure. Understand the security posture by identifying workloads that are not protected by the Falcon platform. Get complete visibility into the container footprint across on-premises and cloud deployments.

MITIGATE

Powered by the CrowdStrike Security Cloud, detect and stop threats in real time with automatic segmentation and high-fidelity threat correlations.

Protect endpoints, identities and workloads from malicious attacks: Protect Windows, Windows Server, macOS and Linux endpoints from ransomware, malware and fileless attacks by combining machine learning, artificial intelligence (AI), indicators of attack (IOAs), exploit blocking and more. Protect hybrid identity stores, assess directory configuration and continuously analyze every user account across on-premises and cloud identity stores with visibility into live authentication traffic and encrypted protocol usage (e.g., LDAP/S). Protect cloud workloads and containers from malware, and investigate and stop malicious behavior early. Prevent attacks on container-based applications by uncovering hidden threats in open source packages and third-party images.

Detect and respond to incidents without manual threat correlations: Automatically detect and prioritize malicious and attacker activity with IOAs. Contain and investigate compromised systems with powerful response actions through intelligent endpoint detection and response (EDR). Mitigate identity threats in real time, without using logs and time-consuming analysis. Detect and prevent reconnaissance (e.g., LDAP, BloodHound, credential compromise attacks), lateral movement (e.g., RDP, Pass-the-Hash (PtH), Mimikatz tool, interactive service logins), and persistence (e.g., Golden Tickets, privilege escalation) with advanced analytics and correlation in the CrowdStrike Security Cloud.

Automatically segment identities: Automatically classify identities based on roles; privileges; human, service and shared accounts; and even hybrid (identities that are on on-premises and cloud AD) or cloud-only identities (identities that reside only on Azure AD or analogous location). Segment and identify privileged accounts and permissions on Azure AD deployments, and secure them by detecting misconfigurations linked to tactics, techniques and procedures (TTPs).

Reduce costs and management overhead: Reduce false positives with high-fidelity telemetry from endpoints, workloads and identities distributed across the hybrid enterprise. Powered by petabytes of data at scale, detect new and unusual threats in real time with deep AI and behavioral analysis from endpoints, identities and workloads, and take the appropriate action based on policies. Eradicate threats with precision using powerful response actions, and contain compromised systems to stop attacks before they become breaches. Reduce SIEM and UEBA costs by sending only those curated/analyzed authentication and incident logs, instead of gigabytes of data dump that require finding the needles in the haystack by writing the detection rules. Because authentication, endpoint and workload anomalies are monitored and detected by the CrowdStrike Security Cloud, there's no need to write correlation rules in SIEM and UEBA solutions.

Enrich telemetry with threat intelligence: Identify new campaigns associated with known threat actors by enriching the telemetry with context about real-world threats. Automatically identify and investigate nation-state, eCrime and related threats with reduced manual effort.

OPTIMIZE

Provide maximum Zero Trust security coverage across the organization, improve the user experience and leverage CrowdStrike's Zero Trust ecosystem partners as you scale up your Zero Trust journey.

Enhance the user experience with intelligent conditional access: Define and enforce access policies with simple rules, based on authentication patterns, behavior baselines and individual risk scores. Ensure consistent login experience for genuine users while enforcing identity verification when the risk increases.

Extend multifactor authentication (MFA) to improve security posture: Increase ROI and reduce the attack surface by extending MFA to any resource or application, including those on-premises legacy/proprietary systems and tools (e.g., PowerShell and protocols such as RDP over NTLM) that could not be integrated with MFA solutions.

Assess and share endpoint security posture: With real-time security posture assessment scores, determine endpoint health across the enterprise. Maximize security by identifying and updating sensor policies and OS settings that are non-compliant and increase risk. Enforce real-time conditional access to resources from compliant endpoints by sharing the assessment scores with CrowdStrike Zero Trust ecosystem partners.

Leverage APIs to connect your favorite tools: Integrate third-party and custom security solutions with the CrowdStrike Security Cloud. Unlock the full potential of frictionless Zero Trust with CrowdStrike Zero Trust Ecosystem partners. In addition to APIs, CrowdStrike Zero Trust Assessment (ZTA) provides pre-integrations with the CrowdStrike Zero Trust ecosystem partners including Zscaler, Okta, Proofpoint and Netskope.

ENABLE FRICTIONLESS ZERO TRUST

With CrowdStrike, realize frictionless Zero Trust to reduce risks and costs for the enterprise. Eliminate the overhead of managing terabytes of data, threat feeds, hardware/software and ongoing personnel investments. Protect your hybrid environments with continuous risk-based verification of user accesses (including contractors, partners and vendors) from managed and unmanaged endpoints to on-premises, cloud and legacy applications. By sharing contextual risk-based information from a single source of truth, enable Zero Trust access for distributed workforce without compromising productivity — regardless of physical location or network location, or based on whether they were managed or unmanaged (BYOD) endpoints.

ABOUT CROWDSTRIKE

CrowdStrike, 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 5 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.