CrowdStrike Products

CROWDSTRIKE

CROWDSTRIKE FALCON HAS YOU COVERED WITH THE WHITE HOUSE CYBERSECURITY EO

The White House released their Executive Order (EO) on Improving the Nation's Cybersecurity on May 12th, 2021. There are three major technology themes in the EO: 1) Zero Trust while pushing cloud adoption, 2) unified endpoint detection and response (EDR) and vulnerability management, and 3) responding to incidents while enabling threat sharing. At CrowdStrike, we stop breaches and this is in our DNA. Let us help secure and harden your environment against today and tomorrow's threats.

ZERO TRUST AND CLOUD ADOPTION

CrowdStrike provides comprehensive and frictionless Zero Trust capabilities, capabilities, securing the most critical areas of enterprise risk – endpoints and cloud workloads, identity, and data – to keep customers ahead of today's threats and stop breaches. CrowdStrike's **Falcon Identity Protection** integrates with the top Identity Providers (IdP), enabling you to enforce multi-factor authentication (MFA). This integration with our unique visibility, while being in-line to the authentication flows, empowers our customers to apply the same MFA to on-premises authentication flows—and those who wish, can have multiple IdPs. If Falcon Identity Protection identifies an identity as compromised, via deterministic or machine learning, it can prevent it from authenticating and accessing other resources, on-premises or in the cloud. This automatic response helps contain breaches in real-time and can trigger additional automation and remediation steps, thanks to the CrowdStrike Security Cloud's Falcon Fusion capability.

The EO also pushes Departments and agencies (D/a) towards faster cloud adoption. CrowdStrike provides the industry's only Adversary-focused Cloud Security Solution. **Falcon Horizon** is a cloud security posture management (CSPM) solution that detects and prevents misconfigurations and control plane threats, eliminates blind spots, and ensures compliance, across AWS, Azure, and Google Cloud. **Falcon Cloud Workload Protection** provides comprehensive breach protection for workloads, containers, and Kubernetes enabling organizations to build, run, and secure cloud-native applications with speed and confidence. Identity Analyzer helps identify potential backdoors and misconfigurations for both cloud users and applications, which was instrumental in identifying backdoors related to Sunburst.

In addition to providing best-of-breed EDR, **Falcon Endpoint Protection** continuously calculates a Zero Trust Assessment score for Windows and Mac. Through integrations with Secure Access Service Edge (SASE), IdPs and other vendors can use this score to evaluate if they should allow an action. For example, without the Falcon Agent or with a low device score, the SASE can block traffic from accessing its intended destination, keeping internal and cloud resources secure.

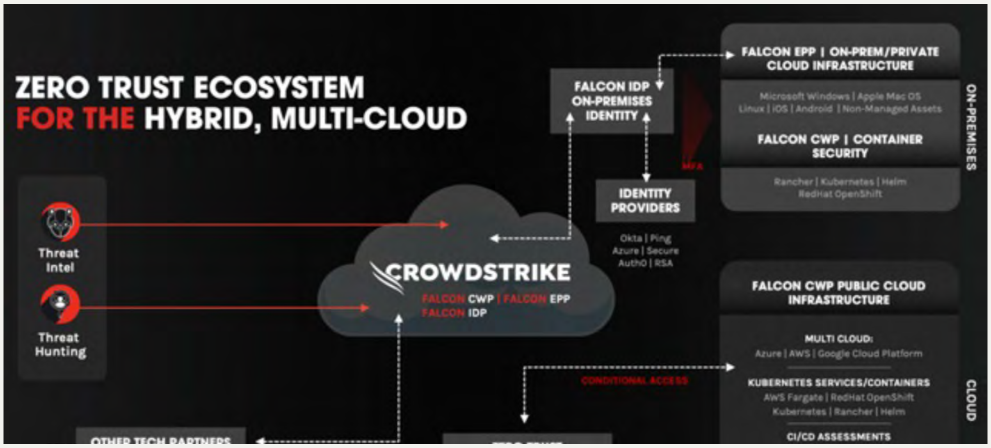
ZERO TRUST ECOSYSTEM
FOR THE HYBRID, MULTI-CLOUD
Threat Intel
Threat Hunting
CROWDSTRIKE
FALCON CWP | FALCON EPP
FALCON IDP
FALCON IDP ON-PREMISES IDENTITY
IDENTITY PROVIDERS
Okta | Ping
Azure | Secure
Auth0 | RSA
MFA
FALCON EPP | ON-PREM/PRIVATE CLOUD INFRASTRUCTURE
Microsoft Windows | Apple Mac OS
Linux | iOS | Android | Non-Managed Assets
FALCON CWP | CONTAINER SECURITY
Rancher | Kubernetes | Helm
RedHat OpenShift
ON-PREMISES
FALCON CWP PUBLIC CLOUD INFRASTRUCTURE
MULTI CLOUD:
Azure | AWS | Google Cloud Platform
KUBERNETES SERVICES/CONTAINERS
AWS Fargate | RedHat OpenShift
Kubernetes | Rancher | Helm
CI/CD ASSESSMENTS
CLOUD
CONDITIONAL ACCESS
OTHER TECH PARTNERS

Figure 1: CrowdStrike's Zero Trust eXtended (ZTX) platform uniquely integrates its best-of-breed products to maximize visibility and control for our customer's digital estates while enabling external integrations and automation to further their Zero Trust Architecture.

UNIFIED ENDPOINT DETECTION AND RESPONSE AND VULNERABILITY MANAGEMENT

CrowdStrike **Falcon Endpoint Protection Platform (EPP**) provides unified protection, delivered from the cloud, with cutting edge and real-time machine learning applied at both the device and the cloud. It has the industry's best feature parity across Windows, Mac and Linux. It has better feature parity across Windows 10 build versions compared to even the Windows 10 vendor, providing device control and firewall management capabilities to all Windows clients. Falcon Endpoint Protection continues to get the highest ratings from Gartner, Forrester and MITRE, thanks to our unique focus on Indicators-of-Attack (IOA) vs solely Indicators-of-Compromise (IOCs). This helps detect and prevent never-before-seen attacks such as Sunspot, with high-confidence. In addition, **Falcon Intelligence** is an automated threat intelligence solution that augments SOC and Incident Response teams with built-in adversary intelligence to help your organization get ahead of the attacker's next move.

Included in EPP is **Falcon Spotlight**, Falcon Spotlight is a scanless vulnerability management solution that provides real-time visibility across your enterprise. Spotlight enumerates common vulnerabilities and exposures (CVEs) all with the same agent while prioritizing vulnerabilities based on prevalence and availability as seen in the wild. Vulnerabilities being exploited in the wild should take precedence. With "one-click patching," customers can deploy Windows Update patches to specific hosts, enabling customers to identify and patch in a single console.

RESPONDING TO INCIDENTS AND ENABLING THREAT SHARING

CrowdStrike provides unrivaled visibility and protection across the most critical areas of enterprise risk – endpoints and cloud workloads, identity, and data. With **Falcon Intelligence**, customers can leverage the Indicator Graph to visually see attackers, attacks and observables on their endpoints. This extends to intel from the dark web via **Falcon Intelligence Recon**. This leads to market-leading visibility, decreasing the time-to-triage and respond. Unlike other vendors, raw Threat Intel can be applied to other vendors' data such as network appliances.

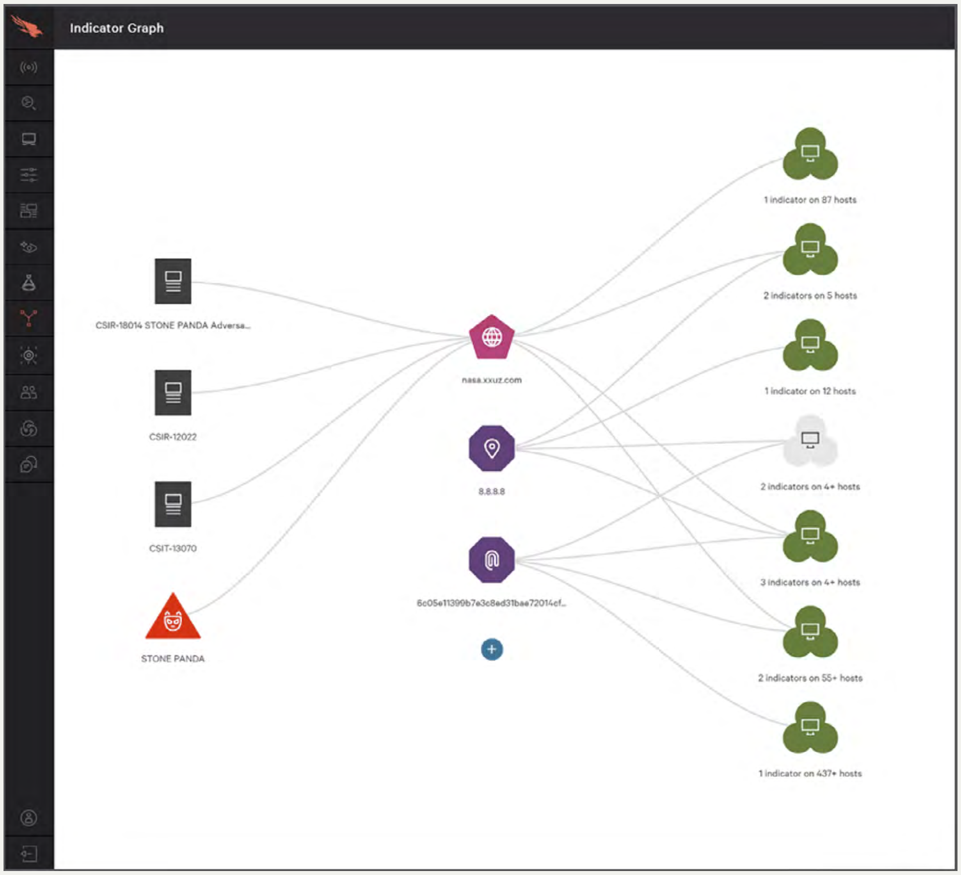

Figure 2: CrowdStrike Falcon Intelligence's Indicator Graph, enabling customers to visualize the relationship of IOCs, adversaries and your endpoints.

Falcon Fusion and **Real Time Response** enable customers to interact with devices and drive automation to speed and enhance investigation and remediation steps. CrowdStrike's Services can provide support, as needed to develop Incident Response (IR) Playbooks while aiding investigations and performing proactive security assessments. CrowdStrike's IR services are National Security Agency (NSA) certified for the National Security Cyber Assistance Program (NSCAP).

Since CrowdStrike was built with complex organizational environments in mind, our customers can remain empowered with complex role-based access controls (RBAC), across environments, without the need for a SIEM. This means built-in roll-up reporting, faster incident response and recovery efforts. For our most critical public sector customers, with best-of-breed technologies at your fingertips, it means mission resiliency in the face of a capable cyber adversary. Threat sharing is enabled via APIs and can be automated via complex workflows internally on the CrowdStrike platform or externally via the SIEM or SOAR of your choosing.

Section	CrowdStrike
Section 2: Removing Barriers to Sharing Threat Information	**Falcon Intelligence** Sandbox can detonate potential malcode with customized OS configurations. Any threats and all observables can be outputted in industry acceptable formats, including: TAXII, STIX, MAEC, CSV, JSON. Furthermore, the entire CrowdStrike **Falcon Security Cloud** has industry-leading APIs, which **Falcon Fusion** further enables via orchestration, automation and tagging to enable Security Operations Center (SOC) to meet the demand.
Section 3: Modernizing Federal Government Cybersecurity	CrowdStrike's **Falcon Platform** includes multiple facets of Zero Trust, focused on device security (**Falcon Endpoint Protection**) and hygiene, identity (**Falcon Identity Protection**; on-premises and cloud) security and risk-scores and cloud-security across the leading Cloud Service Providers. In addition, CrowdStrike can build comprehensive automation workflows to quarantine and remediate threats thanks to **Falcon Fusion** while providing all raw data, to any destination, thanks to **Falcon Data Replicator**. CrowdStrike is the only security company with either device or Identity security products that integrates into multiple best-of-breed vendors, including SASE and Identity Providers—and we do this for both our Device (Falcon Endpoint Protection) and Identity (Falcon Identity Protection) products. It's also the only company which can apply 2FA to on-premises authentication flows, finally giving you more control over Service Accounts and IT/Security Administrators (i.e., PowerShell, WMI, etc.). **Falcon Cloud Workload Protection** helps secure customers clouds, by measuring Cloud Security Posture Management (CSPM) as well as against run-time attacks. This can be integrated into CI/CD pipelines to help secure DevSecOps practices. It can also be integrated into the Cloud Service to ensure all machines have CrowdStrike's agent.
Section 4: Enhancing Software Supply Chain Security	CrowdStrike is committed to government standards and authorizations to help secure its most critical customers. CrowdStrike is committed to Cybersecurity Maturity Model Certification (**CMMC**), to help secure the Defense Industrial Base (DIB) and the Federal Governments supply chain. CrowdStrike was one of the first **FedRAMP** authorized clouds and maintains its FedRAMP authorized status.
Section 6: Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	**Falcon Endpoint Protection** includes **Falcon Spotlight**, Falcon Spotlight, a scanless vulnerability management solution that provides real-time visibility across the enterprise, including Mac and Windows environments, using the same light-weight Falcon agent. In addition, it prioritizes vulnerabilities not just based on CVSS (critically) score, but also exploitability-likelihood; vulnerabilities which are actively exploited in the wild or have proof-of-concept code in the wild should be prioritized against those which don't. In addition, through **Falcon Fusion**, customers can standardize on orchestration and automation, triggered by both CrowdStrike and non-CrowdStrike solutions, to aid operations, track and tag investigations, measure time to respond and remediate, challenge and ask. With **Falcon Intelligence,** customers can accelerate alert triage and response, and with raw Threat Intelligence, get ahead of eCrime and nation-state actors.
Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks	CrowdStrike continues to be identified as the industry-leading best-of-breed company providing Endpoint Detection and Response capabilities by both Forrester and Gartner. **Falcon Endpoint Protection** leads the market in agent performance and feature parity across operating systems. In addition, it has industry leading feature parity across Windows operating system—only requiring its customers to update the ~40mb agent vs the entire Operating System, without ever requiring a reboot. It's attention to operational feasibility in complex organizations provides a frictionless solution for even complex organizations and role-based-access control (RBAC) requirements. The Falcon Platform is underpinned by the CrowdStrike Security Cloud, one of the world's largest unified, threat-centric data fabrics. The Security Cloud correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. Using cloud-scale AI and machine learning, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the patented Threat Graph to automatically prevent threats in real time across CrowdStrike's global customer base.
Section 8: Improving the Federal Government's Investigation and Remediation Capabilities	CrowdStrike has unparalleled visibility on the Endpoint and Identity-plane while providing run-time security in the cloud. All of this data is more comprehensive than traditional logging, which is vastly insecure and can usually be disabled leaving defender's blind. With CrowdStrike's **Falcon Data Replicator**, we do not keep your data hostage nor do we charge by storage costs. Optionally, with Humio's industry-leading index-free logging capability, collecting, analyzing and automating from other datasets (i.e., Network Operations (NETOPS) data) in the spirit of eXtended Detection and Response (XDR) is possible with CrowdStrike.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

Start Free Trial
of Next-Gen AV