CrowdStrike Solutions

CROWDSTRIKE

CROWDSTRIKE
THREAT GRAPH
BREACH PREVENTION ENGINE

Stopping breaches through the power of cloud analytics, artificial intelligence (AI), and real-time visibility

STOP ADVERSARIES WITH CLOUD ANALYTICS

Today's adversaries are becoming more sophisticated. Most of today's observed attacks are non-malware based, hands-on-keyboard activity, command line or running a shell-script. These cannot be prevented reliably by scanning files and searching for known signatures. Sophisticated attacks of this nature require a mix of automation and human expertise in the form of elite threat hunting, reviewing content and adding context to detections.

Security effectiveness is directly related to the quantity and quality of data you're able to collect and your ability to analyze it. Preventing breaches requires taking this data and applying the best tools , including AI, behavioral analytics and human threat hunters. It leverages this massive data to continuously predict where the next serious threat will appear, in time to act.

This is an ambitious undertaking, requiring massive levels of high-performance computing resources, deep threat intelligence and advanced analytics. It also requires that you build and maintain a staff with specialized, advanced skills.
Such a scenario is simply outside the reach of all but the largest and most sophisticated organizations.

INTRODUCING CROWDSTRIKE THREAT GRAPH

CrowdStrike® Threat GraphTM is the brains behind the Falcon cloud-native platform.

The CrowdStrike Security Cloud leverages Threat Graph to correlate trillions of security events per day with indicators of attack, threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations.

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.

Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.

CROWDSTRIKE THREAT GRAPH: SECURITY ANALYTICS AND REAL TIME VISIBILITY

Capture: Preventing breaches starts with collecting high-fidelity trillions of high-fidelity security telemetry from customer endpoints, workloads, and identities around the globe, and indexing them for quick and efficient access.

Enrich: Raw data is useless without context. Graph databases represent
the ideal structure for enrichment, as they make it feasible to capture relationships between data points, as well as external sources such as threat intelligence.

Analyze: Today's best detection techniques leverage AI, behavioral analytics and human threat hunters to identify and block advanced threats as they emerge.

Act: Incident responders and threat hunters require fast, frictionless access to data.
This allows them to detect and respond quickly, and prevent the mega breach.

BUILDING BLOCKS FOR BREACH PREVENTION

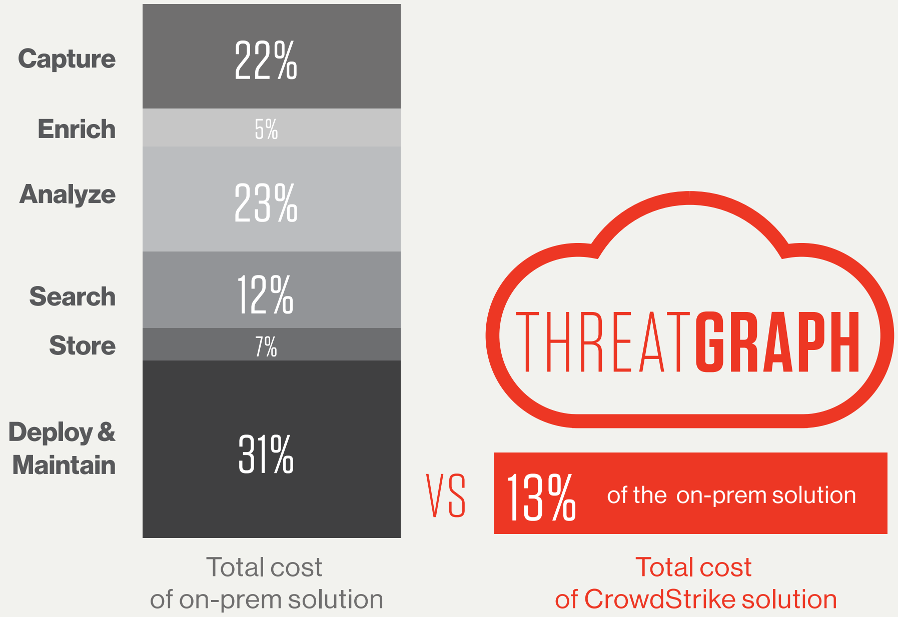
Stopping breaches using cloud-scale data and analytics requires a tightly integrated platform. Each function plays a crucial part in detecting modern threats, and must be designed and built for speed, scale, and reliability.

Function	Description
Capture	Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data
Enrich	Threat intelligence, context, and correlation markers
Analyze	Hardware and software for a cloud-scale data analytics platform to hunt for suspicious and malicious activity
Search	Query engine to deliver real-time search capabilities across the entire body of stored data
Store	High-redundancy, high-performance enterprise storage
Deploy & Maintain	Staff required to perform hardware and software deployment, integration maintenance and upgrades

STOP BREACHES. SPEND LESS

As adversaries advance their tradecraft to bypass legacy security solutions, the combination of world-class technology combined with expert threat hunters is absolutely mandatory to see and stop the most sophisticated threats. Autonomous machine learning alone is simply not good enough to stop dedicated attackers. CrowdStrike Threat Graph offers a comprehensive platform for preventing breaches that delivers instant value on Day One, without costly consulting services and with zero maintenance overhead. Threat Graph predicts, investigates, and hunts at a fraction of the cost.

THREAT GRAPH DELIVERS 7.5X LOWER TCO



CrowdStrike Falcon delivers automated detection and remediation to stop known and emerging threats. Powered by AI, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the Threat Graph to automatically prevent threats in real time across global customer base.

KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches high-fidelity telemetry on trillions of security events across endpoints, workloads, identities. Graph database captures and reveals relationships between data elements.
Integrated Threat Intelligence	Enriches telemetry with context about real-world threats, which helps identify new campaigns associated with known threat actors.
Deep Analytics	Deep AI and behavioral analysis identifies new and unusual threats in real time. Falcon identifies threat activity in real time and then alerts or blocks it based on policies.
Search Engine	Robust, industry-standard query and search engine. Provides easy and powerful capabilities for incident responders and threat hunters, ensuring frictionless access to data needed to get answers fast.
APIs	Enables tight integration with third-party and custom security solutions. Unlocks security orchestration, automation and other advanced workflows.
Falcon Data Replicator	Regularly extract enriched security data sets to support compliance, long-term archival or integration with third-party analytics engines and data lakes.
Cloud-delivered	Part of the CrowdStrike Falcon integrated solution, delivered with no on-premises infrastructure. The solution scales with zero effort, providing all necessary storage and compute resources for fast and efficient interactions. Complete set of enriched data is continuously available for security responders, even for systems that are ephemeral, offline or destroyed.

THREAT GRAPH RETAINS MORE DATA, LONGER

Detecting threats is not just about what happened in the moment. It can be just as critical to know what happened yesterday, or recall what adversaries you encountered months ago. CrowdStrike Threat Graph maintains a wide range of data for you in the cloud, where it is secure from tampering and data loss. This ensures you are always armed with the knowledge you need to effectively understand the threats of today.

Data type	Data Description	Industry	CrowdStrike
Detection Summaries	On-demand access to metadata related to all threats generated from the Falcon platform	30 days	1 year
Detection details	On-demand access to full forensic details for all threats detected by the Falcon platform	30 days	90 days
Enriched Sensor Data	On-demand access to a complete historical record of more than 400 event types — used for retrospective detection, threat hunting and investigations	N/A	7 to 90 days
Enriched Sensor Data Archive	Optional offline replica of enriched sensor data for use in local data warehouse or data lake, and correlation against logs collected from other systems	Varies	Unlimited

Start Free Trial
of Next-Gen AV

STOP BREACHES WITH CROWDSTRIKE THREAT GRAPH

PREVENT threats in real time, with AI-powered analytics and threat intelligence.

INVESTIGATE threats quickly, reducing time-to-respond.

HUNT proactively for stealthy threats.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform 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/