FLASHPOINT

THE BEST DATA FOR THE BEST INTELLIGENCE

Flashpoint Account Takeover

Flashpoint monitors billions of stolen credentials, detecting hidden risks in cookies, domains, and malware. Get the insights you need to respond quickly and confidently.

HOW WE HELP

Flashpoint's Account Takeover provides proactive monitoring to detect compromised credentials across your organization and customer base before they are used in attacks. Our extensive database contains over 48 billion stolen and leaked credentials, gathered from various sources such as open sources, illicit communities, marketplaces, and infostealer malware logs.

While usernames and passwords are a critical data point, Flashpoint goes beyond just credential monitoring by also collecting and analyzing additional components of an account takeover attack, including:

- **Cookies** containing session IDs that allow threat actors to bypass multi-factor authentication controls, increasing risk.
- **Host attributes** like machine names, IP addresses, and installed software provide insight into the scope of a breach.
- **Affected domains** monitors for any compromised organization or customer-base domains. This tracking helps to identify instances of when either enterprise or customer credentials have been breached.
- **Malware family attribution** links stolen data to specific known cybercriminal groups and theft campaigns, to identify recurring patterns using historical infostealer data and attack trends.

By leveraging this extra host, cookie, contextual, and technical data, Flashpoint gives security teams a more comprehensive view of breach risks facilitating faster, more informed actions to better protect you from advanced credential theft schemes and potential account takeover attacks.

WHY IT MATTERS

Account takeover attacks are increasingly sophisticated and damaging, posing devastating risks for users and organizations alike. Attackers have shifted their focus to stealing user credentials using information stealers, allowing them to bypass traditional security measures and directly take over accounts, often undetected. These stolen credentials are then sold on the black market, fueling a lucrative industry of account takeovers. For organizations, account takeover incidents pose significant risks including data breaches, financial losses, and reputational damage.

By proactively monitoring for compromised credentials using Flashpoint Account Takeover, organizations can prevent unauthorized access and protect sensitive information from falling into the wrong hands. This approach offers several benefits:

- Reduces the risk of account takeover and financial loss.
- Improves threat detection and prevention capabilities.
- Enables faster investigation and identification of compromised accounts.
- Confidently prioritize risks with high-fidelity infostealer data
- Saves time and resources on the aggregation, correlation and advanced analysis of information.

HOW IT WORKS

Flashpoint Account Takeover solution offers two levels of protection, allowing users to monitor for exposure and compromises of both their enterprise domains and credentials, as well as customer-base domains and credentials.

Account Takeover for Enterprise Credentials

Abuse of enterprise credentials allows attackers onto your network and exposes sensitive business and personal data.

Account Takeover for Enterprise Credentials allows you to search and monitor our large database in order to flag accounts, reset employee passwords, and restrict permissions. It offers four powerful capabilities: Enterprise Credentials, Credential Breaches, My Credential Exposure, and API access.

- Enterprise Credentials
  Find a clear overview of your organization's credential details and recent breaches. Powerful search functionality lets you delve deeper, analyzing specific breaches and their impact on your data. Each breach entry reveals compromised users, the source, date identified, breach sightings, cookies, host attributes and affected domains when available.

- Credential Breaches
  A high-level view of the current breach landscape, keeping you information about new and total compromised credentials, year-to-date stats, and the number of affected devices. Dive into the interactive list of top analyst-identified breaches for deeper exploration. Filter by title, access relevant links for context, and seamlessly switch between overviews and detailed information, ensuring you have a complete understanding of each threat.

- My Credential Exposure
  Assess your organization's risks on a granular level. See specific details and impact of various breaches, allowing you to prioritize mitigation efforts based on their potential harm. View cookies, host attributes and affected domains within each breach, when available. Analyze your

organization’s overall password complexity to identify areas for improvement and implement stronger password policies.

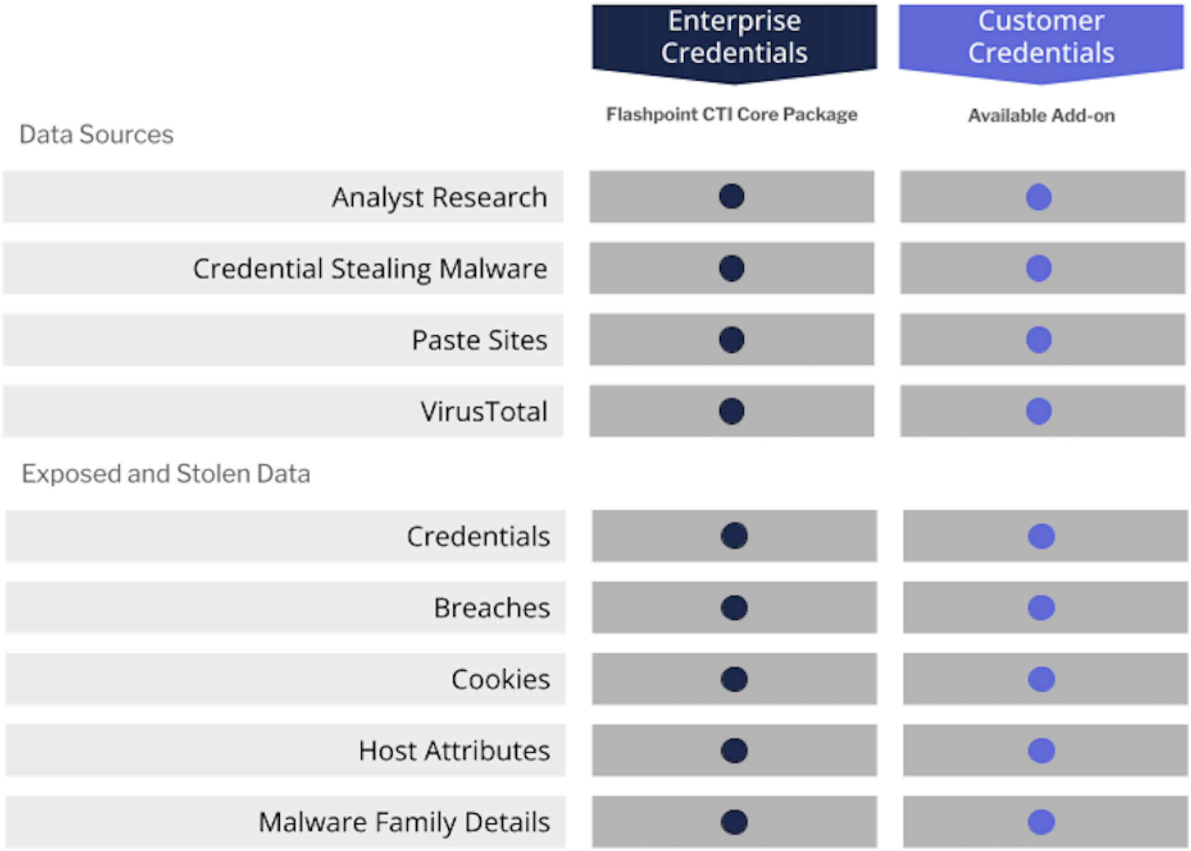
Account Takeover for Customer Credentials

Organizations often have large customer bases spread across multiple platforms and channels, making it a challenge to effectively monitor all accounts for signs of compromise.

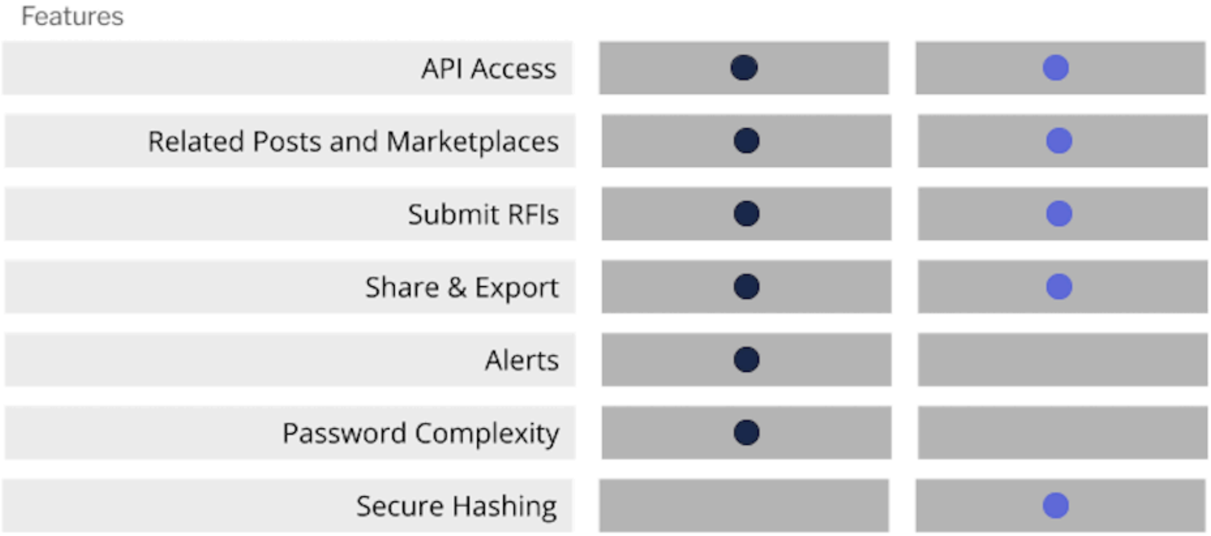
Account Takeover for Customer Credentials provides proactive monitoring of potentially compromised accounts across your customer email addresses and domains, allowing for quick action against fraudulent activities, helping to protect your organization and client base. It offers two powerful capabilities: Customer Credentials and API access.

- Customer Credentials
  Simplified search functionality provides a fast and convenient way to check customer credentials, whether examining a single entry or a bulk list. Verify if a credential has been breached with a quick credential search or dive deeper into the details, accessing contextual data including source, date identified, breach sighting, cookies, host attributes, and affected domain, when available. Analyze your organization’s domains to see if they've been involved in a breach and determine if any, or specific, customer credentials are associated with the breach.

OFFERINGS



	Enterprise Credentials	Customer Credentials
	Flashpoint CTI Core Package	Available Add-on
Data Sources		
Analyst Research	●	●
Credential Stealing Malware	●	●
Paste Sites	●	●
VirusTotal	●	●
Exposed and Stolen Data		
Credentials	●	●
Breaches	●	●
Cookies	●	●
Host Attributes	●	●
Malware Family Details	●	●



Features		
API Access	●	●
Related Posts and Marketplaces	●	●
Submit RFIs	●	●
Share & Export	●	●
Alerts	●	
Password Complexity	●	
Secure Hashing		●

ABOUT FLASHPOINT

Flashpoint is the pioneering leader in threat data and intelligence. We empower commercial enterprises and government agencies to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives. Discover more at **flashpoint.io.**