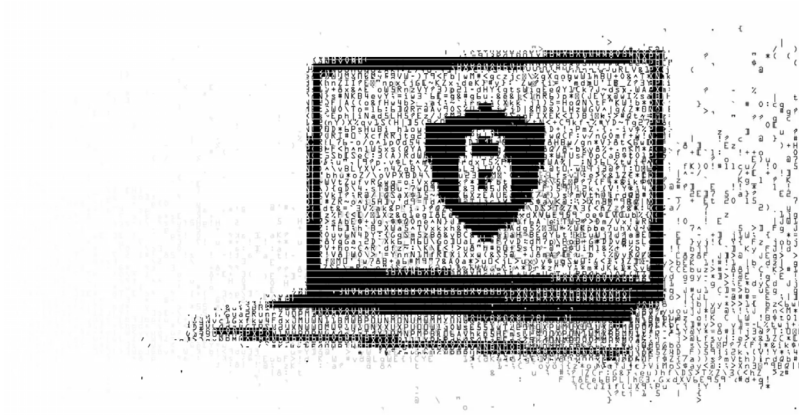
Flashpoint Account Takeover

Detect and Mitigate Credential Exposure Before Attackers Act



Account takeover attacks are becoming increasingly sophisticated. Threat actors steal credentials through **infostealer malware, phishing campaigns, and breach data**, then use or sell access to compromise accounts. Flashpoint Account Takeover provides proactive monitoring to detect compromised credentials across your **enterprise and customer environments**, enabling security teams to respond before stolen access is used. Flashpoint's extensive dataset contains **billions of stolen and exposed credentials**, enriched with critical context that helps organizations quickly assess risk and take action.

How We Help

Flashpoint monitors stolen and leaked credentials across open sources, illicit communities, infostealer malware, breach data, and active phishing infrastructure, detecting hidden risks across domains, cookies, hosts, and user credentials.

Flashpoint credential records provide deep contextual intelligence, allowing analysts to move beyond basic credential exposure and understand the full environment in which credentials were stolen.

Credential intelligence may include:

- **Credential Exposure Details:** Identify compromised usernames, associated domains, affected URLs, and password-complexity indicators to quickly assess risk and credential-reuse exposure.
- **Session & Authentication Artifacts:** Analyze stolen authentication cookies and session identifiers that may allow attackers to bypass multi-factor authentication (MFA) and maintain active access.
- **Source & Breach Intelligence:** Understand where the credential originated, including breach source, collection method, discovery time, and attribution to specific credential-stealing malware campaigns.
- **Phishing Infrastructure Intelligence:** Identify credentials captured directly from phishing kits, malicious landing pages, and credential-exfiltration channels, providing earlier visibility into compromised accounts.

- **Infected Host Context:** Investigate infected machines associated with credential theft, including host identifiers, IP addresses, system configuration, and device metadata.
- **Device & System Telemetry:** Access detailed endpoint information, including operating system, hardware profile, language settings, computer name, and system configuration.
- **Installed Software Inventory:** Review software installed on infected machines to better understand user activity, potential attack surfaces, and indicators of compromise.
- **Geolocation & Network Intelligence:** View geographic location, ISP information, and network attribution to help identify compromised infrastructure and assess regional threat activity.
- **Malware Attribution:** Link credentials to specific malware families and infection campaigns, providing insight into attacker tooling and distribution patterns.
- **Affected domains** monitors for any compromised organization or customer-base domains. This tracking helps identify instances in which either enterprise or customer credentials have been breached.

Why It Matters

Account-takeover attacks are increasingly sophisticated and damaging, posing devastating risks for both organizations and their customers. Threat actors commonly obtain credentials through **infostealer malware, phishing kits, and exposed breach data**, allowing them to bypass traditional security controls and gain direct access to user accounts.

Once compromised, these credentials are often sold or shared across cybercriminal communities, fueling a large underground economy that enables fraud, account takeover, and unauthorized access at scale.
For organizations, these incidents can result in **data breaches, financial loss, regulatory exposure, 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 enables security teams to:

- Reduces the risk of account takeover and financial loss.
- Detect credential theft earlier, including credentials harvested from phishing campaigns and malware infections.
- Accelerate investigation and identification of compromised accounts
- Prioritize response efforts using high-fidelity credential and host intelligence
- Save time and resources by eliminating the need to manually aggregate and correlate credential exposure data

How It Works

Flashpoint Account Takeover provides multiple layers of protection, allowing organizations to monitor credential exposure across enterprise users, customer accounts, and malware-infected hosts.

Account Takeover for Enterprise Credentials

Compromised enterprise credentials can give attackers direct access to internal networks and sensitive data.

Account Takeover for Enterprise Credentials allows you to search and monitor Flashpoint's credential intelligence database to quickly identify compromised accounts, enforce password resets, and restrict access where needed.

The solution provides four key capabilities: **Enterprise Credentials, Credential Breaches, My Credential Exposure, and API Access.**

- Enterprise Credentials
  Gain a clear view of credential exposures associated with your organization. Powerful search functionality allows analysts to investigate credential records and assess their potential impact. Each record may include compromised users, breach sources, discovery dates, cookies, host attributes, affected domains, and, when available, associated malware campaigns.
- Credential Breaches
  Understand the broader breach landscape impacting your organization. This view highlights newly compromised credentials, total compromised credentials, year-to-date breach statistics, and the number of affected devices. Analysts can explore Flashpoint-identified breaches, filter by breach title, and access contextual intelligence to understand the scope and origin of credential exposure.
- My Credential Exposure
  Assess credential exposure specific to your organization. This capability provides detailed visibility into compromised accounts associated with your domains, enabling teams to prioritize remediation efforts by risk. Analysts can review cookies, host attributes, affected domains, and password complexity indicators to

Account Takeover for Customer Credentials

Organizations often manage large customer bases across multiple platforms and digital services, making it difficult to monitor all accounts for potential compromise.

Account Takeover for Customer Credentials provides proactive monitoring of compromised customer emails and domains, enabling organizations to quickly detect exposed accounts and prevent fraud or unauthorized access.

Customer Credentials is available in **Core and Lite packages**, designed to support different levels of monitoring and automation.

Customer Credentials LITE

Provides a streamlined, UI-based solution for quickly identifying compromised customer credentials. Organizations can:

- Verify whether individual or bulk credentials have been exposed
- Access contextual intelligence, including source, discovery date, cookies, host attributes, and affected domains
- Monitor organizational and customer domains for credential exposure across breach, malware, and phishing datasets

Customer Credentials CORE

Provides comprehensive credential monitoring with both UI and API access. Core enables organizations to:

- Verify credentials during authentication workflows, such as login or account registration
- Detect compromised credentials that may bypass traditional authentication mechanisms such as MFA
- Monitor credential exposure across enterprise and customer domains
- Track compromised accounts and devices to prevent unauthorized sessions

Infected Host API

Flashpoint's Infected Host Intelligence provides critical insights into malware-compromised machines, offering context that extends far beyond credentials to support advanced security operations.

- **Infected Host Data**
  Access detailed information on compromised hosts, including cookies, machine identifiers, IP addresses, and other host-based indicators.

  This intelligence helps analysts trace malware infections, understand attacker activity, and connect infected machines to compromised credentials.

- **Advanced Investigation and Threat Hunting**
  Security teams can query and analyze infected-host intelligence to investigate host-specific threats and the broader context of credential theft.

  This capability supports deeper investigations for organizations that need to understand how credentials were stolen and which systems may still be compromised.

- **Beyond Credential Monitoring**
  By monitoring indicators beyond simple credential exposure, Flashpoint enables a deeper level of threat assessment.

  Organizations can correlate compromised credentials with infected hosts, malware activity, and phishing infrastructure, allowing security teams to trace attacker activity and better understand the scope of a compromise.

Offerings

	Enterprise Credentials	Customer Credentials CORE	Customer Credentials LITE	Infected Host
	Flashpoint CTI Core Package	*Available Add-ons*		
Data Sources				
Analyst Research	●	●	●	●
Credential Stealing Malware	●	●	●	●
Paste Sites	●	●	●	●
VirusTotal	●	●	●	●
Phishing Kits & Infrastructure	●	●	●	●
Exposed and Stolen Data				
Credentials	●	●	●	●
Breaches	●	●	●	●
Cookies	●	●	●	●
Host Attributes	●	●	●	●
Affected Domains	●	●	●	●
Source Context	●	●	●	●
Features				
API Access	●	●		●
Unrestricted Domain Search		●	●	
Infected Host Search				●
Infected Host Credential Extraction				●
Related Posts and Marketplaces	●	●	●	

Features (continued)	Enterprise Credentials	Customer Credentials CORE	Customer Credentials LITE	Infected Host
	Flashpoint CTI Core Package	*Available Add-ons*		
Submit RFIs	●	●	●	
Share & Export	●	●	●	
Alerts	●			
Password Complexity Settings	●			
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

Get a Demo