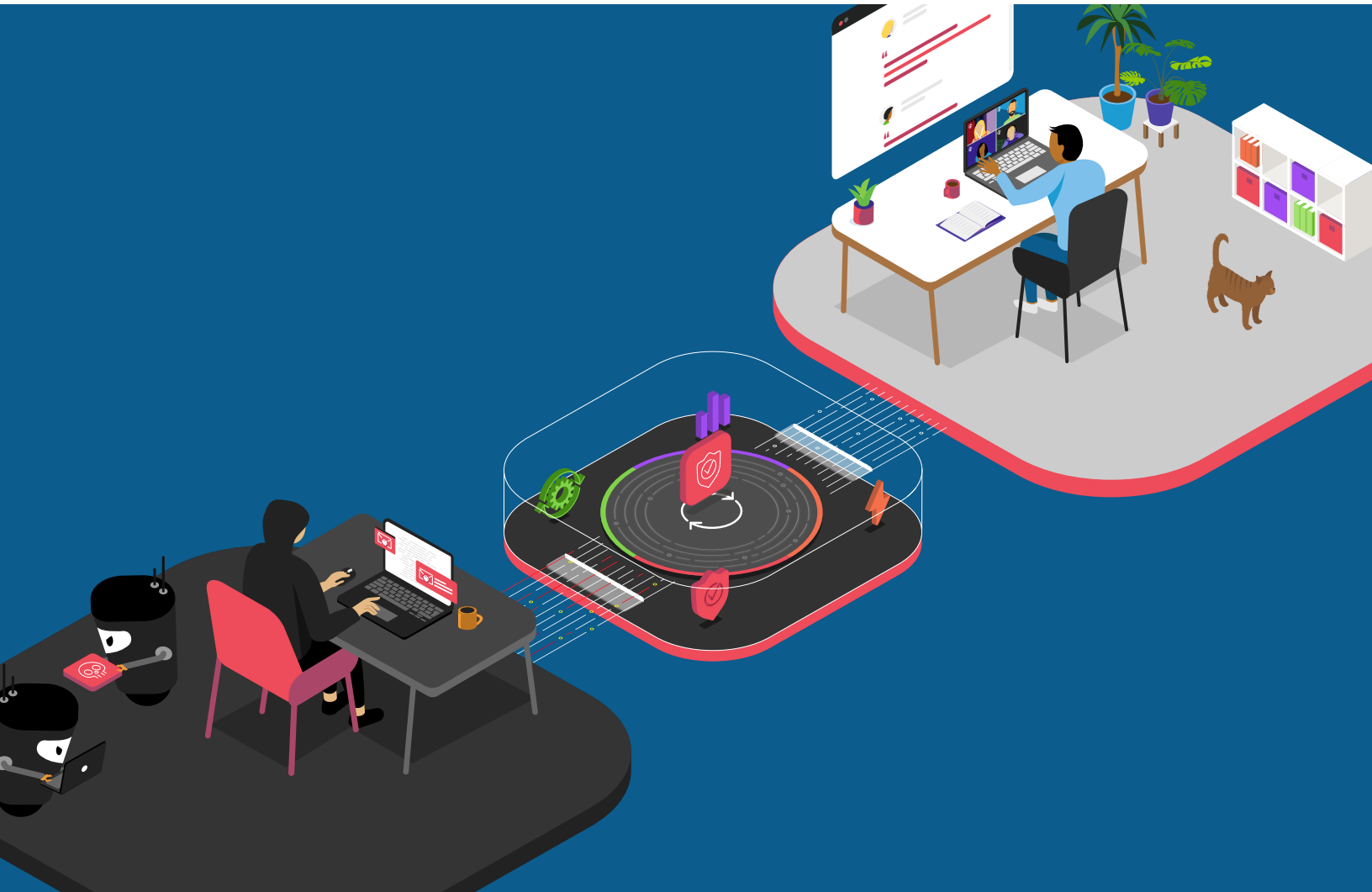
SOLUTION OVERVIEW

Protect User Credentials

Prevent credential compromise and subsequent credential-based attacks that cause ripple effects across the business–from missed revenue opportunities to fraud losses to damaged trust that can cripple operations.



KEY BENEFITS

Unmatched Credential Protection

F5 safeguards customer accounts by mitigating theft in real time and preventing unauthorized access using the most complete list of compromised credentials on the planet—over 9 billion publicly available and 500 million actively exploited credentials.

Highest Real-World Security Efficacy

F5 can uniquely provide long-term, persistent efficacy, because its artificial intelligence algorithms are trained on attack profiles and risk surfaces of similar organizations.

Stop Fraud Without Friction

Secure strategic business outcomes by removing unwanted automation and stopping human-driven fraud while preserving the customer experience.

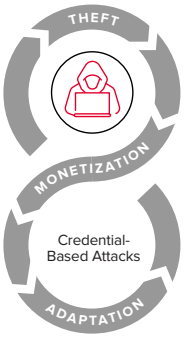
OVER 1.5 BILLION CREDENTIALS HAVE BEEN EXPOSED IN 2020 (AS OF NOVEMBER).[1]

Compromised credentials are commonplace and result in cascading disruption to the business. The frequency of data breaches, coupled with more targeted phishing campaigns and client-side attacks, has resulted in the fast monetization of credentials using automation. Readily available tools, infrastructure, and compromised credentials, often obtained by trickery and exploitation of the user runtime environment, provide for easy weaponization of credential-based attacks and attractive ROI.

This vicious cycle has significant, longstanding impacts across core business operations, and can quickly turn top line potential into bottom line losses.

Anatomy of Credential-Based Attacks

Credential-based attacks continue to evolve but typically follow a common blueprint involving theft, monetization, and adaptation stages.



Stage	Description	Business Impact
Theft	Obtain credentials	Lost customer trust
Monetization	Weaponize with automation Sell on dark web	Unauthorized access Account takeover (ATO)
Adaptation	Bypass security countermeasures	Fraud losses Damaged brand

First, attackers use targeted phishing campaigns to trick users into installing client-side malware and keyloggers that can eavesdrop and harvest credentials when entered into web and mobile applications. In other cases, users are tricked into entering credentials into a spoofed login form controlled by an attacker. Increasingly, the complexity of modern application development and reliance on third-party integrations and APIs allows for exploitation in the user runtime environment, bypassing centralized security controls in order to steal credentials.

CRIMINALS ATTEMPT TO USE STOLEN PASSWORDS WITHIN FOUR HOURS OF PHISHING A VICTIM.[2]

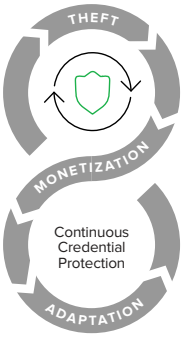
Next, because the value of compromised credentials decreases over time, attackers act swiftly by leveraging automation to carry out account takeover (ATO) and fraud. The attacker's arsenal consists of a variety of tools that escalate and circumvent mitigation countermeasures, including tools that imitate human behavior. The ROI is twofold, since after using actively exploited compromised credentials, attackers can sell them on the dark web.

Finally, if the target value is perceived to be high enough and the attacker is skilled, the next phase involves adaptation in order to bypass anti-automation defenses, typically through use of click farms and sophisticated manual attacks, leading to human-driven fraud.

This cycle has resulted in massive operational disruption, with estimated online fraud losses projected to exceed $48 billion per year by 2023.[3]

Continuous Credential Protection Deters Compromise

In order to protect user credentials, organizations must employ defenses across all stages of credential-based attacks that may lead to compromise.



Stage	Mitigation	Business Outcome
Theft	Real-time encryption and obfuscation	Safeguarded credentials Mitigated compromise
Monetization	Continuous monitoring	Improved security effectiveness Decreased operational burden
Adaptation	Resilient countermeasures	Abandoned attack Reduced fraud losses

First, credentials must be explicitly protected. Given the complexity of modern web and mobile applications, there are many ways in which attackers can circumvent centralized security controls and steal credentials directly from the client side of the digital interaction. The daunting challenge of identifying and securing every potential threat vector can be offset with real-time encryption and obfuscation, using advanced algorithms and techniques to secure credentials from keystroke input to login to any subsequent network and application communication.

BOTS ARE INCREASINGLY USED FOR COMMERCIAL AND RETAIL FRAUD.[4]

Second, in order to mitigate the threat of previously compromised credentials or automated attacks that leverage them, continuous monitoring for use of known compromised credentials must be coupled with durable device, network, and environmental telemetry analysis. This approach can detect and stop the first attempt of malicious use, regardless of whether the attacker is leveraging a previous credential spill or is attempting to weaponize actively exploited credentials using automation. A complete data set of known compromised credentials and telemetry combined with machine learning algorithms that detect actively exploited credentials will continuously deter credential compromise with maximum security efficacy.

Third, if the perceived value is high, and the attacker is skilled, the adaption phase of credential-based attacks results in an evolution of sophisticated techniques to emulate or exhibit human behavior in order to bypass anti-automation defenses. Countermeasures must adapt as attackers evolve and remain resilient as motivated adversaries attempt to bypass defenses. For the most critical environments, historical fraud records can be input into machine learning algorithms to better detect human-driven fraud and further increase efficacy. Because the fraudster may be using real customer credentials and advanced techniques to spoof anti-automation techniques, truth and intent must be continuously monitored across the entire customer journey—from login to account creation to all financial transactions.

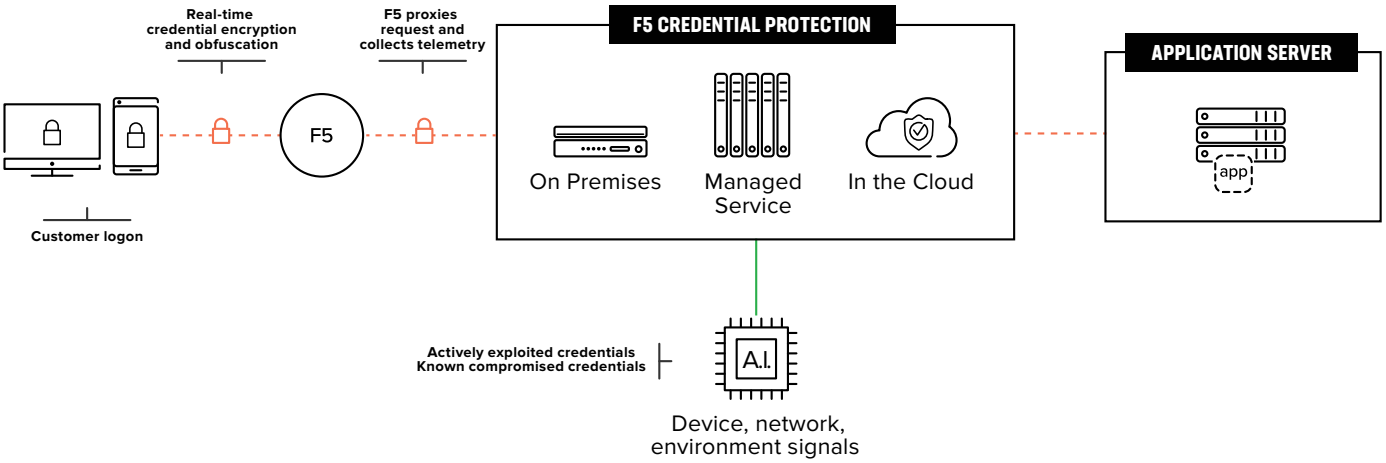


Figure 1: F5 credential protection continuously deters theft and compromise.

KEY FEATURES

- Perform real-time application-layer encryption and obfuscation to neutralize theft.
- Continuously monitor for compromise across a collective defense network without storing credentials or PII.
- Identify criminals' very first attempts to weaponize publicly available and actively exploited credentials.
- Stop imitation attacks that use sophisticated tools to emulate human behavior.
- Maintain accuracy and resilience as attackers retool and evolve to countermeasures.
- Remove unwanted automation to evaluate human traffic against proprietary telemetry signals and historical fraud records to maximize efficacy of closed-loop AI models.
- Reduce fraud while maintaining false positive baselines.
- Remove complex risk scoring and manual fraud rules.
- Improve the customer experience by minimizing user friction such as CAPTCHA and multi-factor authentication (MFA).

Conclusion

Security controls must deter the theft, monetization, and adaptation stages of credential-based attacks, including client-side exploits, automated attacks leveraging previously compromised credentials, imitation attacks that emulate human behavior, and coordinated human-powered attacks specifically designed to bypass anti-automation defenses.

By continuously securing and monitoring credentials, and removing unwanted automation, machine learning algorithms have a large data set of human traffic. When a data set representing the world's most valuable brands is combined with durable telemetry signals and historical fraud records, the highest real-world security efficacy can be achieved. This solution will effectively deter credential theft, unauthorized use, abuse, and fraud—protecting revenue, brand, and the bottom line.

To learn more, explore F5 Application Security.

[1] Genesis Marketplace, a Digital Fingerprint Darknet Store, found at https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[2] Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies, found at https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal

[3] Juniper Research Online Payment Fraud https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

[4] Shape Security Predictions 2020 https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape Security Predictions 2020 Report - Emerging Threats to Application Security.pdf

©2021 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
OV-300SP | JOB-CODE-605389222