CSURFACE

WHITEPAPER · CREDENTIAL LEAKAGE

Leaked credentials · the gap between exposure and discovery

Credential Leakage Monitor: why continuous monitoring of breach databases, the dark web and public repositories systematically outperforms any point-in-time audit — with active validation to eliminate false positives.

CAPABILITY	AUDIENCE	EDITION
Credential Leakage Monitor	CISO · IAM Lead · SOC	2026

READING	CLASSIFICATION	SOURCE
7 pages	Public	CSURFACE Platform

EXECUTIVE SUMMARY

The reaction window is measured in hours

The thesis of this whitepaper, in one page — what executives need to know before the technical detail.

CREDENTIAL-BASED BREACHES

30%

of incidents begin with a compromised credential

TIME TO DETECTION

94 days

is the average between the leak and its discovery

DETECTION WITH CONTINUOUS MONITORING

< 24h

from the leak to a validated alert

About **30% of data breaches begin with a compromised credential** (Verizon DBIR). The core problem is that credentials leak without being noticed. The average interval between the leak of a credential and its discovery by the affected organization is **94 days**.

Ninety-four days represent a broad operational window for the attacker: enough time to complete reconnaissance, escalate privileges, exfiltrate data and, in many cases, close out the operation without immediate evidence. The leaked credential constitutes the access vector that precedes the incident, available months before any internal detection mechanism is triggered.

This whitepaper presents CSURFACE's **Credential Leakage Monitor**: continuous monitoring of public breach databases, the dark web and public code repositories to detect leaked corporate credentials in hours. The operation is entirely external, with no agent or installation, and includes active validation that confirms the currency of each credential before any alert is issued.

The thesis. Credential defense requires continuous monitoring. Credentials leak continuously and, for that reason, must be monitored continuously. Reducing the discovery window from quarters to hours is what turns a months-long incident into a response contained within a single business day.

What this whitepaper covers

- Why credentials leak — and why traditional detection is slow.
- The three leak sources that truly matter to an organization.
- Why active validation is what separates a useful alert from noise.
- The recommended response workflow and a representative use case.

THE LANDSCAPE · PART 01

Credentials leak continuously — detection does not keep pace

How corporate credentials reach the wrong hands and why traditional controls are slow to notice.

Whitepaper 2026
CSURFACE

THE FIVE PATHS OF CREDENTIAL LEAKAGE

CRITICAL Third-party SaaS breach
The employee reused the corporate password; the service is breached and the credential goes to market.

CRITICAL Successful phishing
The credential is typed into a fake page and sent directly to the attacker.

WARNING Public repositories
Accidental commit of a .env file, a cloud key or a password in a configuration file.

CRITICAL Infostealers
Malware on a personal laptop exfiltrates every password saved in the browser.

WARNING Insider action
A disgruntled employee shares or sells access to third parties.

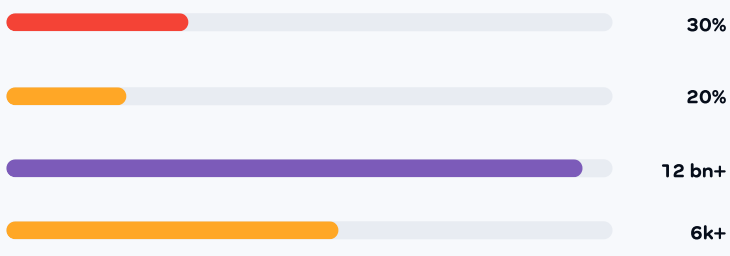
WHAT CSURFACE OBSERVES · THE PLATFORM'S OWN DATA

170
leaked corporate credentials identified across 16 companies analyzed by the platform

37%
of the companies analyzed had at least one corporate credential exposed

The scale of the problem

None of these five paths crosses the perimeter the organization controls — and none triggers an internal alert. The credential becomes available externally, in sources accessible to adversarial actors, without any internal signal being generated.



Sources: Verizon DBIR, SpyCloud, HaveIBeenPwned, GitHub Secret Scanning Trends.

The cost of not detecting. The average cost of a data breach in the United States reached **$10.22M** in 2025 (IBM Cost of a Data Breach 2025), and in the United States breach exposure arises from a 50-state patchwork of notification laws, FTC Act §5 enforcement, and state statutes such as the CCPA, whose private right of action provides statutory damages of $100–$750 per consumer per incident. Every day removed from the discovery window reduces the probability of the leak evolving into an incident — an impact that CSURFACE's risk calculator translates into annual expected loss (ALE).

Why detection is slow. Password audits are point-in-time (annual or semiannual); MFA reduces risk but does not cover service and *legacy* accounts; DLP watches data leaving, not the return of a credential for sale in a forum; and the SIEM only detects anomalous use after the attacker is already inside. None of these controls observes the outside — precisely where the leaked credential is exposed.

THE THREE SOURCES · PART 02

Where to monitor: three sources that matter

Breach databases, the dark web and public repositories — what each source reveals and what CSURFACE does with it.

THE THREE SOURCES MONITORED IN PARALLEL

1 **Breach databases**
Cross-referencing the domain against aggregated databases of public leaks.

2 **Dark web**
Monitoring of markets and forums that trade recently stolen credentials.

3 **Public repositories**
Scanning of new commits in search of secrets from the client's environment.

01. Breach databases

More than **12 billion credentials** have already been exposed in public incidents — from historical leaks to consolidated collections. Public sources such as HaveIBeenPwned maintain aggregated databases of these events.

What CSURFACE does. It continuously cross-references the client's corporate domain against these databases. When a credential linked to the domain appears in any breach — even from a third-party SaaS — the organization is notified.

02. Dark web

Markets, forums and messaging channels trade credentials recently extracted by infostealers, with daily updates of the batches available. Organizations of a relevant profile may have access dossiers available for immediate acquisition.

What CSURFACE does. It monitors known communities through threat intelligence partners and identifies the active sale of credentials associated with the client's domain.

03. Public code repositories

On platforms such as GitHub, GitLab and Bitbucket, developers inadvertently publish **.env** files, cloud access keys and passwords in configuration files — on the order of thousands of secrets exposed per day.

What CSURFACE does. It continuously scans new public commits in search of patterns associated with the client's environment: cloud keys, tokens, internal hostnames and other secrets.

Why three sources, and not one. Each source covers a distinct leak path: the breach database reveals password reuse; the dark web reveals the recently stolen credential for sale; the public repository reveals the secret forgotten in code. Monitoring only one of them leaves two-thirds of the problem invisible.

VALIDATION AND WORKFLOW · PART 03

Active validation: only alert on what still works

Detecting a leaked credential is half the work. The other half is confirming whether it is still a threat.

Why active validation matters

A significant portion of recorded leaks is historically old: the password has already been replaced, the key has already been revoked, the account has already been deactivated. Issuing alerts about these credentials produces operational noise — and the accumulation of noise compromises the team's capacity to respond to the alerts that are genuinely critical.

CSURFACE performs automatic, safe and non-destructive validation to confirm the currency of each detected credential. The result: the organization receives notifications **exclusively** about credentials that remain active, with a marked reduction in false positives.

How the credential is validated, by type

SAML / OAuth
A refresh token request; if accepted, the account is active.

SMTP / email
An authentication attempt without sending a message.

Cloud keys
A read-only identity call, which fails if the key has been revoked.

API tokens
A query to an identity endpoint of the /me or /whoami type.

Non-destructive validation. Every check confirms the credential's currency without altering data, sending messages or triggering blocks on the target account. The objective is to answer a single question — is this credential still active? — before mobilizing the security team for investigation.

RECOMMENDED RESPONSE WORKFLOW · FROM THE ALERT TO THE RECALCULATED RISK

1. **Immediate notification**
Alert via Slack, email or SMS with context: source, leak date, partial credential and validation result.

2. **IdP activation**
Optional integration with Okta, Microsoft Entra ID or JumpCloud forces the password reset and revokes active sessions.

3. **Ticket for the SOC**
Automatic ticket with the collected evidence, including the account's recent access history, for investigation.

4. **Updated dashboard**
The organization's exposure is recalculated and reflected in the dashboard, keeping prioritization aligned with current risk.

IdP integrations are optional — detection and validation operate 100% externally, with no agent.

APPLICATION AND RESULTS · PART 04

From the alert to a response in hours

A representative use case, the outcome indicators and the compliance framing.

TRADITIONAL DETECTION

94 days

average between the leak and its discovery — a window sufficient for the attacker to complete the compromise cycle.

→

WITH CSURFACE'S MONITOR

< 24h

from the leak to a validated alert — typical notification SLA in under 4 hours.

Use case · media, 2,500 employees

A media company placed its root domain and four known SaaS platforms under monitoring. In the **first week**, the cross-reference with breach databases revealed the following funnel:

- WARNING **247 exposed credentials** — of the domain, found in public breaches.
- CRITICAL **38 still valid** — confirmed by the platform's active validation.
- CRITICAL **12 from current employees** — forced into immediate password reset.
- WARNING **26 from former employees** — orphaned SaaS accounts closed; offboarding reviewed.

In **month 2**, a new alert identified an active cloud key published in a public repository. Validation confirmed the key's currency, which held read permission over a bucket containing customer data. The revocation was completed within 4 hours of disclosure — before any recorded exploitation.

Outcome indicators

INDICATOR	BASELINE	CSURFACE
Time to detection	94 days	**< 24 hours**
False positives	High	**Low**
Notification after exposure	Point-in-time	**SLA < 4 hours**
Source coverage	One, if any	**Three sources**

Ranges observed in monitoring conducted by the CSURFACE platform. The result varies according to the dispersion of each organization's surface.

Compliance framing. Rapid detection supports the timely breach notification required under state law and — for public companies — the SEC's Form 8-K Item 1.05 material-incident disclosure, the credential and access controls expected under the GLBA Safeguards Rule and FFIEC guidance, the access management of ISO 27001 (A.9) and the identification and authentication of PCI DSS (Requirement 8).

NEXT STEPS

Credential defense begins with a single domain

The Credential Leakage Monitor is one of the capabilities of the CSURFACE platform — a Continuous Exposure Management platform. In an integrated architecture, it brings together continuous discovery of the external surface with Machine Learning, analysis of the digital supply chain, exploitability validation, threat intelligence with dynamic prioritization and monitoring of leaked credentials. It operates entirely externally — with no agent and no installation — with optional cloud, WAF and CIEM integrations available for organizations that require in-depth coverage.

Receive the preliminary analysis

Provide your corporate domain and receive, free of charge, an assessment of the credentials already exposed in public sources associated with your organization.

Use the risk calculator

Estimate the annual expected loss (ALE) and the VaR of your sector, with a FAIR methodology calibrated by market benchmark.

Read the next whitepaper

Threat Intelligence and Dynamic Prioritization — how compromised credentials feed risk prioritization.

See which credentials have already leaked — monitoring initiated with the root domain

Receive free preliminary analysis

© 2026 CSURFACE · Educational material. Statistics with indicated public sources (Verizon DBIR, HaveIBeenPwned, GitHub Secret Scanning Trends, SpyCloud, IBM Cost of a Data Breach 2025).