PreCrime™ by BforeAI

www.bfore.ai

Stop Credential Abuse Before It Becomes a Breach

PreCrime™ | Credentials

PreCrime™ Credentials is a fully managed "Honeypot-as-a-Service" that deceives threat actors by deploying decoy login portals to silently intercept and validate stolen credentials against your actual identity provider. By the time attackers realize the credentials do not work, your systems have automatically neutralized the threat before it can ever be weaponized or sold.

1 click
easy setup and fully managed deception

deception
fully automated and integrated into the identity stack

full coverage
extensible beyond SSO to protect unmanaged applications

The Critical Challenge: Security teams are flooded with credential exposure feed but lack proof of active risk.

Active leaked credentials are the #1 exploit vector today. Most credential exposure programs generate large volumes of stale, unvalidated data that require costly manual investigation and remediation. How do you know which ones are being actively weaponized by attackers? **This is what PreCrime™ Credentials was built for.**

The Shift: From Credential Monitoring to Breach Preemption

Deploy a HoneyPortal Under 5 Minutes:

PreCrime spins up fully managed, non-finger-printable HoneyPortals (VPNs, email, and OWA pages) on secondary domains.

Attract and Deceive Attackers:

Threat actors discover these decoy endpoints and attempt to validate credentials against them.

Automatically Remediate:

The decoy portal always returns a failure to the attacker. In the background, PreCrime securely validates credentials against your Identity Provider.

Deny, Investigate, and Improve:

If credentials are valid, a webhook instantly triggers a SOAR/SIEM playbook to rotate passwords and lock out the attacker before they can exploit them.

Key Product Capabilities

Zero Setup SaaS Delivery

A 100% managed and hosted deception surface. Integration requires zero software, agents, or on-prem hardware. The customer simply configures a DNS record, allowing PreCrime to handle SSL certificates and decoy maintenance.

AI-Native Anti-Fingerprinting

To prevent threat actors from realizing they are interacting with a decoy, BforeAI leverages AI to dynamically rotate certificates, CSS structures, layouts, and login content so decoys look identical to real portals.

Non-SSO Application Coverage

Through a dedicated integration, PreCrime Credentials automates password rotation across hundreds of non-SSO corporate applications (e.g., social ads, third-party portals) where users recycle credentials.

Active Threat Intelligence and Schema Feeds

PreCrime Credentials exposes source IPs, user agents, and MITRE ATT&CK techniques. Confirmed compromised passwords can be instantly blacklisted in Entra and Okta to prevent future user reuse.

MENTIONED BY GARTNER® IN

Predictive Threat Intelligence

Preemptive Cyber Defense

Preemptive Fraud Detection

LEARN MORE ABOUT PRECRIME™

go.bfore.ai/welcome

PreCrime™ | Credentials