Cribl | //O Push

>SOLUTION BRIEF_

Monitor and defend your identity attack surface with Push Security and Cribl

Get real-time visibility across your SaaS environment and all workforce identities with Push Security and Cribl.

THE CHALLENGE

Compromised identities are the #1 cause of breaches and organizations lack comprehensive visibility into their identity attack surface.

THE SOLUTION

Together, Push Security and Cribl enable you to monitor your identity attack surface and stop identity attacks before your employees' user accounts can be compromised.

THE BENEFITS

- Get complete visibility across your SaaS environment and identity attack surface
- Detect and stop identity attacks at the earliest opportunity in the attack chain
- Proactively improve your overall identity security posture
- Route identity security data to the most cost-effective destinations
- Create Search queries for monitoring against identity attack surface data
- Use Cribl Search Dashboards to enrich data from Push Security events with other event sources and APIs to create powerful and unique views of identity activity and posture

The challenge

Compromised identities are the leading cause of breaches, with cloud-based work leaving organizations with thousands of unmanaged identities and an expanded attack surface. Identities have become the new perimeter, making them a prime target. According to CrowdStrike's 2025 Threat Insight Report, initial access attacks surged, accounting for 52% of vulnerabilities in 2024.

Attackers exploit weak credentials and shared accounts in third-party SaaS apps to bypass security, steal data, deploy ransomware, and disrupt critical systems. Traditional security controls are failing to prevent these breaches, leaving organizations struggling to detect and respond to identity threats. This highlights the urgent need for stronger identity threat detection and response (ITDR).

The solution

Push Security maps your full identity attack surface, detects attacks against it in real time, and improves your organization's overall identity security posture.

Push Security uses an easy-to-deploy browser extension to generate unique identity security events and alerts. This gives you visibility of:

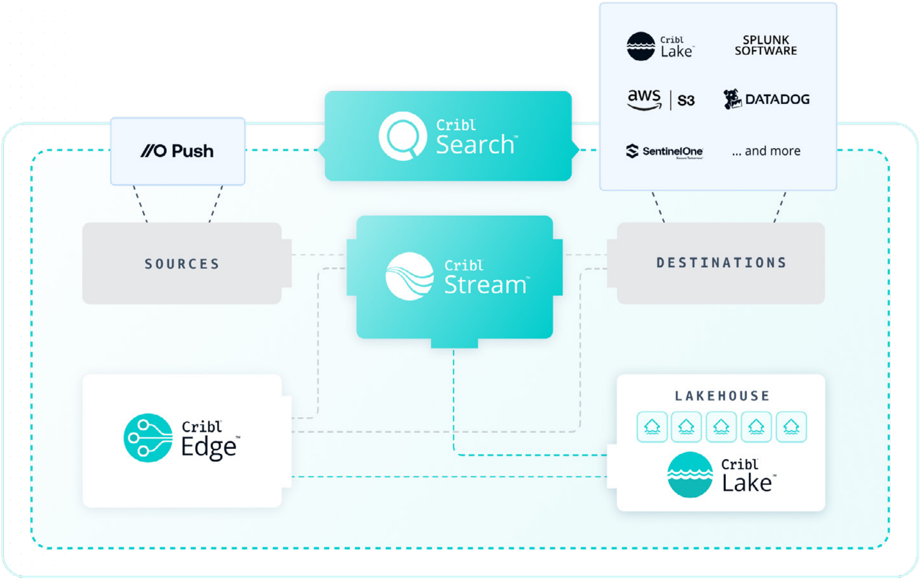
1. Employees logging into all SaaS applications using workforce identities, including all logins to unmanaged (shadow) apps and accounts.
2. The authentication methods being used, such as SAML/OIDC SSO, username and password, MFA, passkeys and password managers.
3. Vulnerable workforce identities using stolen, leaked, weak and reused passwords, missing MFA, ghost logins etc.
4. Real-time detections for attack techniques targeting workforce identities such as phishing, AitM toolkits, credential stuffing and session hijacking.

> “Push Security both significantly reduces our SaaS identity attack surface and helps us better understand where our data is being used.”
>
> Myke Lyons
> CISO at Cribl

As well as generating unique security telemetry, Push Security gives you the ability to enforce controls directly in the browser to block attacks in real time and ensure your users adhere to your security policies.

The integration of Push Security and Cribl provides a solution that allows long-term, cost-effective storage of Push’s data. Furthermore, threat hunting/threat operations/SOC teams can leverage Cribl Search and Cribl Search Dashboarding to conduct threat hunting activities against Push identity data.

This integration enables the selective forwarding of specific Push events and alerts to various security and compliance platforms, including SIEM, XDR, SOAR, and GRC platforms. This capability allows organizations to optimize their security operations by concentrating on the most relevant and critical Push data, thereby improving threat detection and response while managing costs associated with data storage and analysis.



The Benefits of using Push Security with Cribl’s Observability Solution

Push Security Integration for quick set-up.

Push Security and Cribl worked together to develop an easy REST API collector that enables Security teams to quickly collect “Finding” data from their Push Security deployment. This integration allows security teams to quickly collect and route this data to their desired destinations. You can find the collector template here.

Native Push Security and Cribl Stream and Search Packs for a quick start

Push Security and Cribl worked together to develop Push Stream and Search packs to enable customers of Push and Cribl to get up and running even quicker with their deployments. These packs allow for quick routing as well as out-of-the-box identity profile dashboarding for threat hunting, deployment monitoring, and more.

Total visibility across your SaaS environment and identity attack surface

Push Security gives security teams real-time visibility across their entire identity attack surface, including unmanaged identities on shadow SaaS apps. Cribl’s observability solution gives users a cockpit view of their overall identity security posture and the tools to improve it.

Get real-time identity attack detections sent to your SIEM and XDR platform

When Push Security detects attacks against your workforce identities, the high-fidelity alerts can be sent directly to the platforms your SIEM and XDR platform. These alerts can be enriched further using Cribl's enrichment capabilities to leverage correlating data from additional telemetry sources.

Route identity security events and alerts to the most cost-effective destinations

You can easily route Push Security alerts and events through Cribl instead of funneling all your data into an expensive SIEM. Cribl gives you the power to choose where to quickly send alerts and where to send events allowing you to retain and utilize the Push Security data you need while saving money. Optimize the treatment of your Push data to save time and reduce costs.

Summary

Identities are the new perimeter. Push Security and Cribl give you the capability to map your identity perimeter, harden it and monitor for indicators of attack. Use Cribl to harness Push Security's unique identity security telemetry, without skyrocketing your SIEM costs.

With Cribl, Push Security customers can:

- **Get complete visibility across their SaaS environment and identity attack surface**
- **Detect and stop identity attacks at the earliest opportunity in the attack chain**
- **Proactively improve their overall identity security posture**
- **Hunt for identity threats with their push data and other identity datasets**
- **Save money by routing selected data to their SIEM**

Together, Cribl observability solutions give Push Security customers the capability to monitor and defend their identity attack surface without incurring increased SIEM costs.

To get started with Push Security and Cribl today, **click here**. The **Cribl Slack Communityis** also a great place to connect with leaders from other teams leveraging both Push Security and Cribl.

ABOUT PUSH SECURITY

Push Security is the industry's first browser-native Identity Threat Detection & Response (ITDR) platform. Founded in 2021 by offensive security experts, Push Security was the first to recognise the shift in attacker TTPs away from the traditional network and endpoint perimeters, and towards the decentralized identity perimeter. To combat this, Push Security has developed an end-to-end ITDR solution that maps out your full identity attack surface across your entire SaaS environment and establishes defense-in-depth across it by augmenting preventative controls and real-time detection and response capabilities. Push is backed by GV (Google Ventures) and was recently named a "Rising Star for ITDR" by KuppingerCole.

Learn more at www.pushsecurity.com

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, and Cribl Search, the industry's first search-in-place solution. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

SB-0032-EN-3-0425