Caep Hub

Static access welcomes risk. SGNL's CAEP Hub closes the gap.

Static access puts your critical business systems at risk during hijacking, token theft, and malware attacks. Continuous Access Evaluation Profile (CAEP) offers a standardized way for systems to continuously share user and access updates for improved security, but enterprise adoption has been challenging as many vendors are just starting to support CAEP.

With SGNL's CAEP Hub, you can now protect your most sensitive data and critical apps with automated, continuous access decisions and easily adapt your existing tech stack to support continuous access evaluation.

Slash risk by integrating CAEP into all critical systems

CAEP Hub drastically reduces the blast radius of session hijacking, token theft, and malware by automatically responding to events happening anywhere in your ecosystem. SGNL CAEP Hub even covers critical systems that don't yet support CAEP natively.

With SGNL at the center, all of your systems can now:

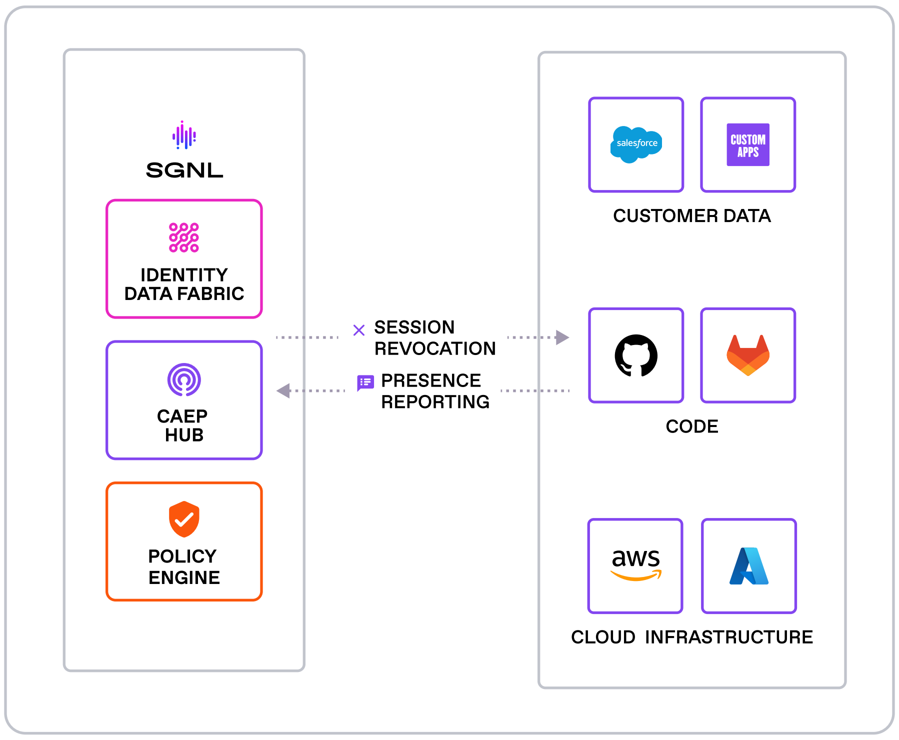
- **Dynamically control and manage** sessions across enterprise services/apps
- **Receive, transmit, and transform** CAEP events
- **Respond to standard CAEP and SSF events,** along with events from proprietary APIs
- **Choose from a catalog of actions** that can be easily adopted to respond to these events
- **Take advantage of centralized policy and auditing** to control actions

How CAEP Hub protects your entire ecosystem

Boost your critical systems protection against common attacks

With triggers based on context changes such as Claim, Device Trust, Session, and Account Changes, you can unleash the power of CAEP Hub features on your most urgent use cases, including:

- Session hijacking
- Credential change
- Malware
- Token theft
- Device compliance change
- Session revocation



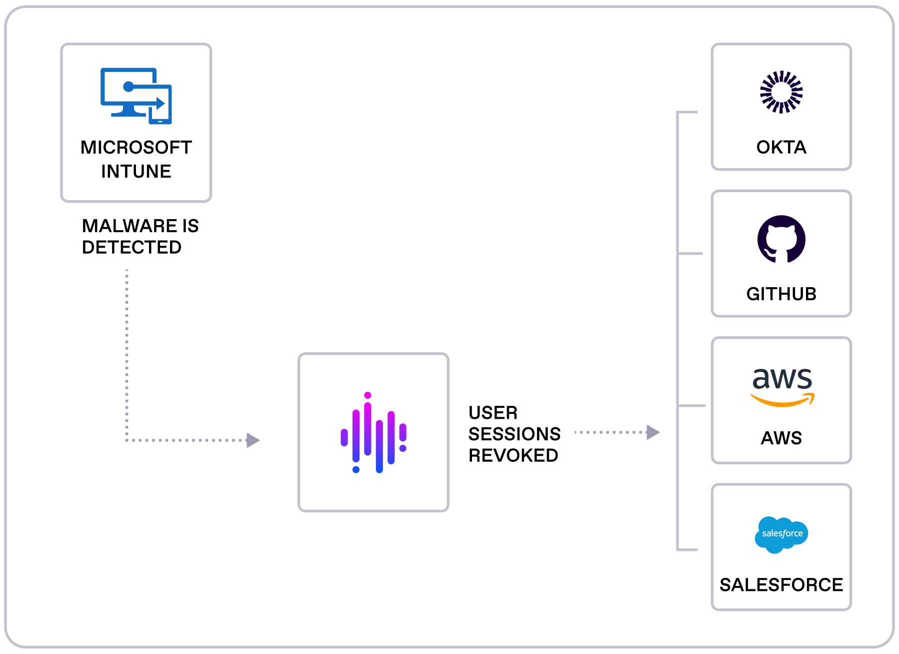
Automatically revoke privileged access when security threats surface

EXAMPLE THREAT SCENARIO

A device management provider (e.g., Intune, Airwatch, etc.) detects malware in a user's device. Organizational policy dictates that privileged access must be revoked until the issue is resolved.

CHAIN OF EVENTS

- The device management provider marks the device as compromised and non-compliant, and SGNL detects this change
- SGNL sends a session revoke event to the IdP
- SGNL revokes all sessions in privileged apps and blocks sign-in



RESULT

Threat actors are automatically stopped before exfiltrating company data and causing further damage.

ABOUT SGNL

SGNL's modern Privileged Identity Management system eliminates standing access to critical systems by granting and revoking contextual access in real time, drastically reducing the potential impact of a breach. By incorporating context-based intelligence, SGNL prevents attackers—leveraging compromised credentials or other means—from freely navigating cloud applications like Azure, AWS, GitHub, and Salesforce, as well as on-prem systems.

SGNL IS BACKED BY LEADING TECH INVESTORS

CISCO investments

M12 MICROSOFT'S VENTURE FUND