britive

>_ SOLUTION BRIEF

Britive & The Shared Signals Framework (SSF)

Enable continuous Zero Trust. Revoke privilege the precise moment risk is detected.

Traditionally, Zero Trust implementations have relied heavily on verifying identities and access once, usually only at the moment of authentication. But what happens if an identity or device is compromised by malware 30 minutes into an active cloud session?

Waiting for a session to naturally time out, or relying on a human analyst to review an ITSM ticket to sever the connection, leaves your cloud infrastructure exposed.

Security posture is dynamic, and access enforcement should be too.

WHAT IS THE SHARED SIGNALS FRAMEWORK? (SSF)

Ratified by the OpenID Foundation, the Shared Signals Framework (SSF) establishes a standard language for security tools to communicate in real-time. It solves the post-authentication problem by allowing your security stack to instantly share context about identity risk and device posture using two standard event types:

CAEP (Continuous Access Evaluation Profile)
Communicates state changes. For example, an Endpoint Detection and Response (EDR) agent detects that a developer's antivirus was disabled mid-session and broadcasts a CAEP event.

RISC (Risk Incident Sharing and Coordination)
Communicates specific, point-in-time risk events. For example, an Identity Provider detects a credential compromise and broadcasts a RISC event to indicate the account is disabled.

KEY INTEGRATION FEATURES

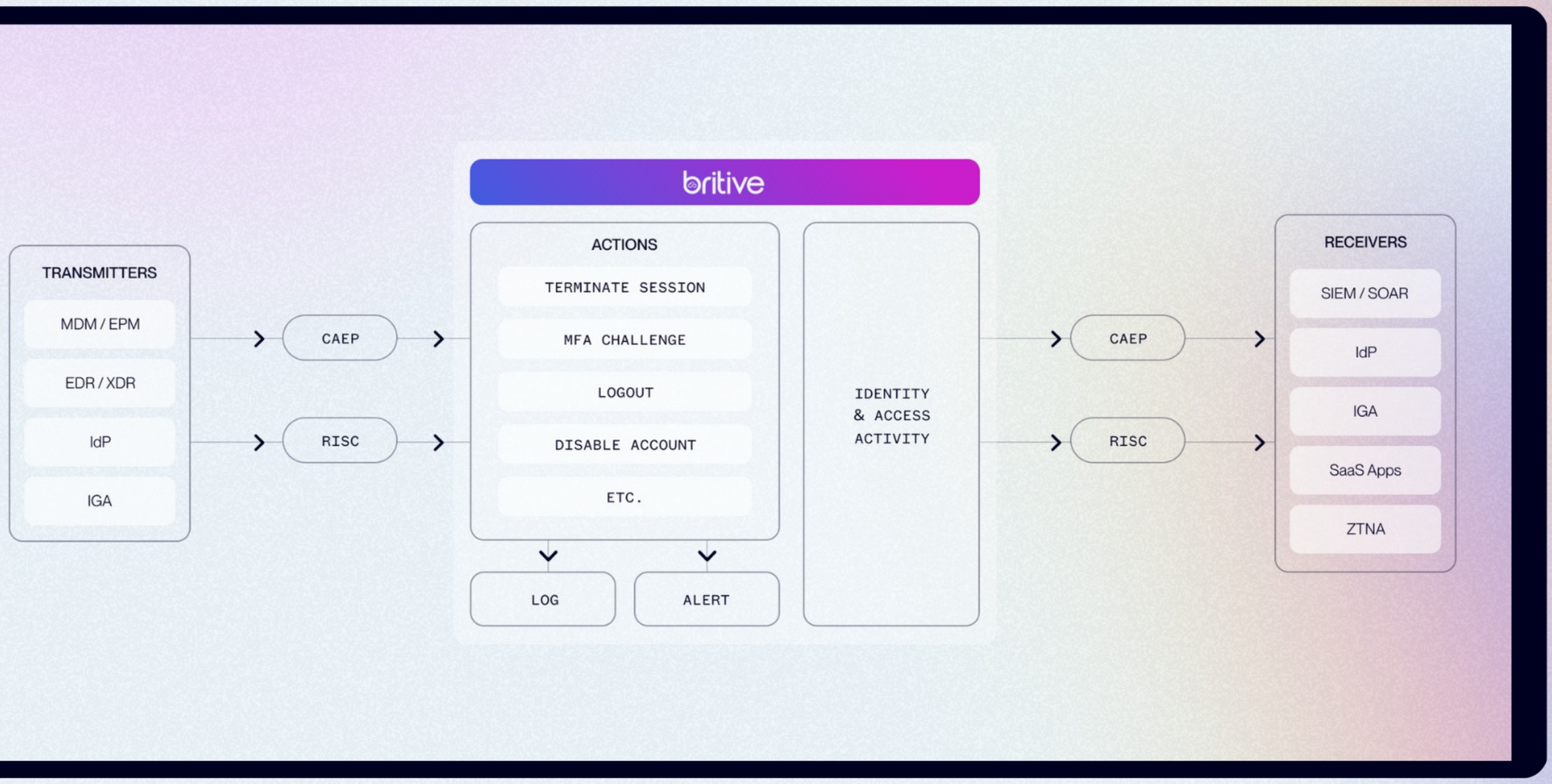
Real-Time Automated Response	Automatically terminate sessions, disable accounts, or enforce step-up authentication the millisecond an inbound CAEP/RISC event triggers a policy violation.
Open Standards, No Lock-In	Built natively on the OpenID Foundation's ratified standard. Integrates directly with any SSF-compatible tool (IdPs, EDRs, MDMs) without requiring proprietary connectors.
Bidirectional Intelligence	Britive acts as both a Receiver and a Transmitter. It emits its own CAEP/RISC events based on privileged access activity to enrich your downstream SOAR or SIEM.
Comprehensive Audit Logging	Every inbound signal, outbound event, and automated action is recorded with named-identity attribution to support strict compliance forensics and incident investigation.

How Britive Delivers Continous Zero Trust

Britive is the first comprehensive PAM platform to natively support SSF for human, AI, and machine identities. Britive consumes these standard CAEP and RISC events from your existing security tools.

Instead of just logging the alert, Britive immediately maps the signal to an automated action. If an endpoint becomes non-compliant mid-session, Britive can instantly terminate the active cloud session, force a logout, or demand step-up MFA.

JIT access ensures privilege only exists when needed. SSF ensures that privilege is held only as long as the security posture justifies it.



BUILT FOR SECURITY, CHOSEN FOR AGILITY

Continuous Zero Trust
Instantly revoke privilege the moment an identity or device falls out of compliance mid-session.

Contain Threats at Machine Speeds
Automate session termination the millisecond a risk signal is received to stop lateral movement.

Unify Your Security Stack
Seamlessly turn isolated EDR and IdP alerts into automated, cross-platform access controls without proprietary connectors or complex custom integrations.

Eliminate Manual Bottlenecks
Sever compromised connections immediately via policy instead of waiting for a human analyst to review a ticket.

Bidirectional Signals & Intelligence
Broadcast real-time privileged access context to your SIEM and SOAR platforms to sharpen downstream risk decisions.

Audit-Ready Evidence
Prove exactly how your security stack responded to real-time threats with a complete, timestamped forensic log.

SECURING ACCESS FOR INDUSTRY LEADERS

fiserv. TOYOTA Forbes ThermoFisher SCIENTIFIC GAP