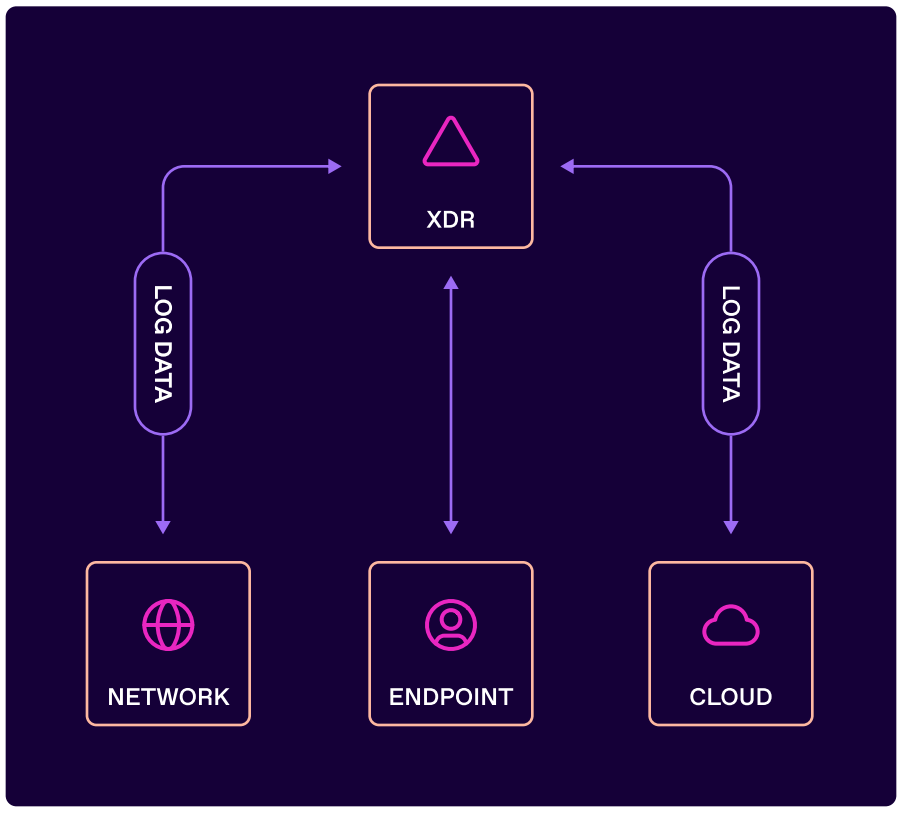
Integrating CAEP with XDR: precision meets power in security management

Introduction

In the world of cybersecurity, having the right tools is crucial for defending against threats. Extended Detection and Response (XDR) and the Continuous Access Evaluation Profile (CAEP) within the Shared Signals Framework (SSF) represent two critical approaches in modern security management. XDR acts as a broad-spectrum hammer, powerful in its ability to neutralize threats across various environments, while CAEP functions as a precise scalpel, finely tuning access controls in real-time. Together, these tools offer a robust and nuanced defense strategy.

Understanding XDR—the hammer

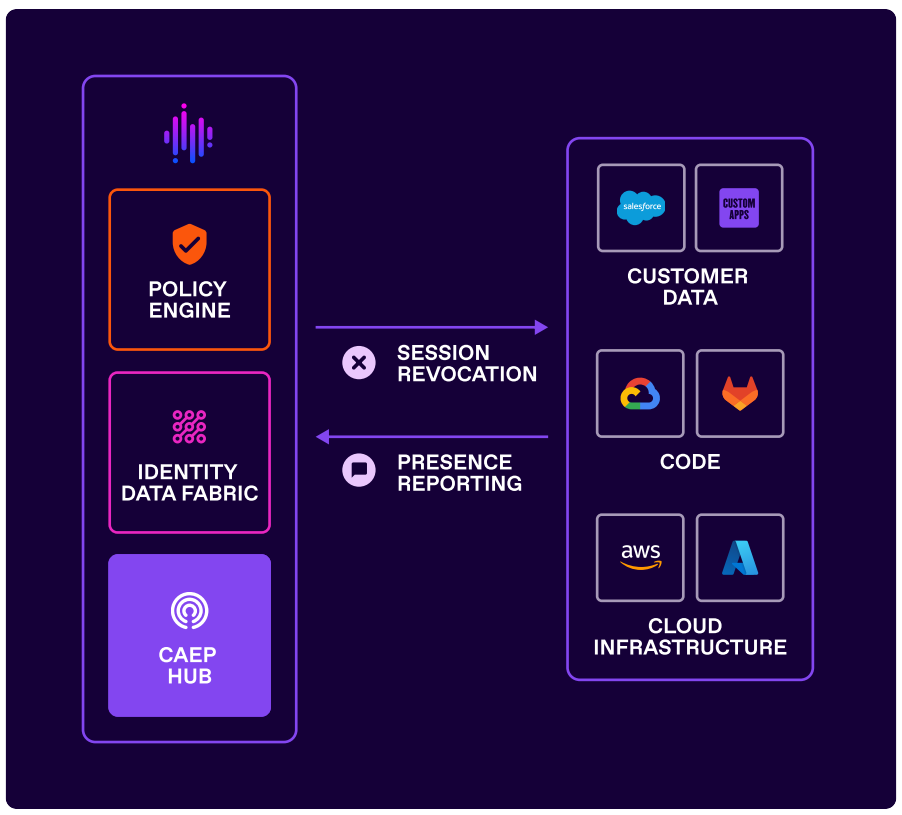
XDR (Extended Detection and Response) unifies data from multiple security tools to provide broad visibility across different environments. It is particularly powerful in detecting and responding to a wide array of threats, such as phishing attempts or network intrusions. XDR's strength lies in its ability to take decisive, broad actions like isolating compromised devices or wiping data to prevent further damage.



- **Key point:** XDR provides comprehensive detection and response capabilities, acting as the first line of defense against cyber threats.
- **Use case-protect cloud infrastructure:** Integrating XDR with context-aware policies eliminates standing access to cloud production environments like Azure and AWS, significantly reducing credential compromise risks. XDR ensures privileged access is granted only when needed, aligning with organizational policies.

The precision of CAEP—the scalpel

CAEP provides the precision needed for real-time access management. Unlike XDR's broad approach, CAEP focuses on continuously evaluating and adjusting access controls based on contextual factors, ensuring that access rights are dynamic and responsive to potential threats.

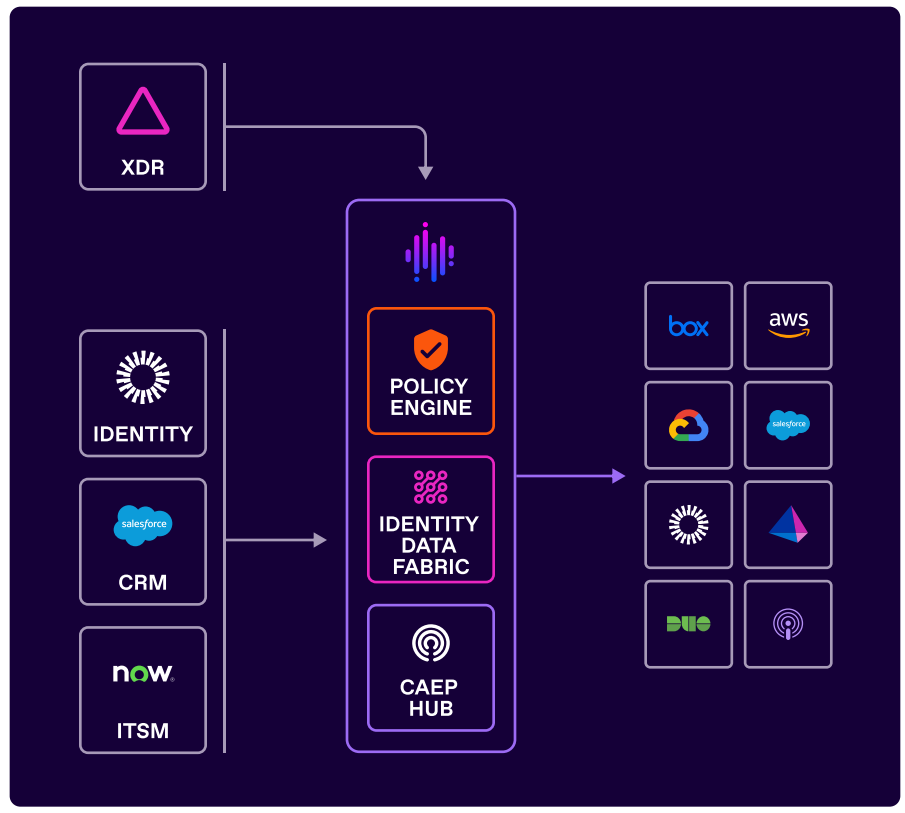


- **Key point:** CAEP provides granular, real-time control over access management, enabling precise adjustments that enhance security without overreaching.
- **Use case-manage user sessions with contextual access:** Static access risks include hijacking, token theft, and malware. CAEP closes this gap by offering a standardized method for systems to continuously share user and access updates, ensuring that access is always contextually appropriate.

The power of integration: XDR and CAEP working together

While XDR and CAEP excel individually, integrating these tools allows organizations to harness both broad and precise security capabilities. XDR's ability to detect and neutralize threats complements CAEP's focus on continuous, granular access management. This combination leads to a more resilient security posture.

- **Key point:** Integrating XDR with CAEP enables organizations to respond swiftly to threats while maintaining precise control over access, reducing the risk of overreach or unnecessary disruption.
- **Use case-eliminate standing access:** SGNL's integration of XDR and CAEP enables organizations to eliminate standing access with high-performance, context-aware policies. This approach is crucial given that over 80% of organizations have suffered identity-related breaches in the last year. By removing unnecessary standing access, the severity of breaches can be significantly reduced.
- **Use case-protect developer platforms:** By integrating CAEP-informed policies with XDR, organizations can control access and actions in code repositories like GitHub. This integration ensures that standing access is removed, reducing the risk of credential compromise. Access decisions are consistently applied across developer platforms using business context, ensuring that the right user has the right access at the right time.



SGNL's integration of XDR and CAEP enables organizations to eliminate standing access with high-performance, context-aware policies. This approach is crucial given that over 80% of organizations have suffered identity-related breaches in the last year.

FAQ

Q What are the differences between XDR and CAEP?

A XDR provides broad-spectrum threat detection and response, while CAEP offers precise, real-time access management based on contextual factors.

Q How does integrating XDR with CAEP improve security?

A The integration allows organizations to leverage the strengths of both tools—XDR's broad threat detection and CAEP's precise access management—creating a comprehensive security solution that is both powerful and agile.

Q How do these tools help eliminate standing access?

A By using context-aware policies, XDR and CAEP work together to ensure that standing access is eliminated, reducing the risk of credential compromise and enhancing overall security.

Conclusion

Organizations today need both broad and precise tools to effectively manage and respond to threats. By integrating XDR and CAEP, organizations can build a comprehensive security strategy that addresses threats at every stage, from detection to response. SGNL's platform enhances these capabilities by providing real-time, context-aware identity management, ensuring that access is always secure and appropriate.

For more information on how SGNL's solutions can help you integrate XDR and CAEP into your security strategy, request a demo at sgnl.ai/demo

By integrating XDR and CAEP, organizations can build a comprehensive security strategy that addresses threats at every stage, from detection to response.