Privileged Access Bridge vs. Enterprise-PAM

Vergleich & DORA/NIS2-Checkliste für privilegierte Zugriffe

Privilegierte Zugriffe sind das lohnendste Ziel eines Angreifers und ein Kernpunkt jeder Prüfung nach DORA, NIS2 und ISO 27001. Dieses Dokument stellt die Blackfort Privileged Access Bridge (PAB) einem klassischen Enterprise-PAM gegenüber und liefert eine praktische Checkliste, an der Sie Ihre eigene Lösung messen können.

1. Der Vergleich auf einen Blick

Kriterium	Privileged Access Bridge	Klassisches Enterprise-PAM
Souveränität / EU-Betrieb	**EU-Betrieb.** Betrieb in Ihrer eigenen Umgebung, in der EU. Kein Datenabfluss in Drittstaaten.	US-Jurisdiktion häufig. Anbieter oft unter US-Kontrolle; Cloud-Komponenten und Support-Zugriffe können außerhalb der EU liegen.
Betriebsmodell	**On-Premises, agentenlos.** Auf Ihrem vorhandenen Hypervisor, kein Agent auf Client oder Ziel. Auch als Managed Service durch Blackfort.	Oft an Appliances oder Agenten auf den Zielsystemen gebunden.
Zugriff	**Über den Browser.** RDP, SSH und VNC laufen vollständig im Browser — nichts wird installiert.	Häufig eigene Clients oder Agenten je Protokoll.
Kontrollen	**Marktstandard, EU-souverän.** Session-Recording, Live-Aufsicht mit sofortiger Beendigung, Vier-Augen-Prinzip, MFA, fälschungssicherer Audit-Trail.	Vergleichbarer Funktionsumfang — Unterschied liegt im Betriebsmodell, in der Jurisdiktion und im Preis.
Preis	**Nach realer Admin-Zahl.** Sie zahlen für die Menschen, die tatsächlich administrieren — ohne Enterprise-Sockel.	Appliance-/Lizenzsockel, der bei kleinen und mittleren Admin-Teams überproportional wiegt.
Drittanbieter-Risiko (DORA/NIS2)	**Schlanke Bewertung.** EU-Betrieb, On-Premises und einsehbare Datenflüsse verkürzen Ihr Register- und Ausstiegs-Assessment.	US-Jurisdiktion und Cloud-/Support-Zugriffe außerhalb der EU erschweren die Bewertung von Auslagerung, Datenfluss und Ausstieg.

„Klassisches Enterprise-PAM" steht allgemein für etablierte Plattformen dieser Klasse. Beispiel für die Eigentümer-/Jurisdiktionslage: Balabit gehört seit 2018 zu One Identity (einer Quest-Software-Marke); Quest wurde 2021/22 von der US-Beteiligungsgesellschaft Clearlake Capital übernommen. Quellen: oneidentity.com/balabit-acquisition · blocksandfiles.com (Quest/Clearlake, 2021).

2. Checkliste: Privilegierte Zugriffe nach DORA & NIS2

Prüfen Sie Ihre bestehende oder geplante Lösung an diesen Punkten. DORA (u. a. Art. 9 Schutz & Prävention, Art. 28 f. Drittparteienrisiko) und NIS2 (Art. 21 Risikomanagement, Zugriffskontrolle) verlangen belegbare Kontrollen über privilegierte Zugriffe — nicht nur Richtlinien.

Kontrolle & Nachweis

- ☐ Jede privilegierte Sitzung wird vollständig aufgezeichnet und ist wiedergebbar.
- ☐ Laufende Sitzungen sind live und schreibgeschützt beaufsichtigbar.
- ☐ Eine laufende Sitzung lässt sich bei Bedarf sofort beenden (Not-Aus).
- ☐ Kritische Zugriffe erfordern eine zweite freigebende Person (Vier-Augen-Prinzip).
- ☐ Zugang nur mit Mehrfaktor-Authentifizierung an einem gehärteten Portal.
- ☐ Sicherheitsrelevante Aktionen werden akteur-genau und fälschungssicher protokolliert.
- ☐ Rechte sind rollenbasiert und nach dem Least-Privilege-Prinzip vergeben.

Souveränität & Drittparteienrisiko

- ☐ Aufzeichnungen und Protokolle bleiben in Ihrer Umgebung und in der EU.
- ☐ Kein Datenabfluss in Drittstaaten; Support-Zugriffe sind nachvollziehbar begrenzt.
- ☐ Der Anbieter ist im Auslagerungsregister sauber erfassbar (Sitz, Datenfluss, Zugriff).
- ☐ Es gibt eine dokumentierte Ausstiegs-/Rückgabestrategie (Exit).
- ☐ Das Betriebsmodell (Eigenbetrieb oder Managed) ist vertraglich klar geregelt und kündbar.

> **So deckt die PAB diese Punkte ab:** Session-Recording, Live-Aufsicht mit sofortiger Beendigung, Vier-Augen-Prinzip, MFA und ein fälschungssicherer Audit-Trail — On-Premises in Ihrer EU-Umgebung, agentenlos, über den Browser. Die Nachweise entstehen direkt aus dem System.

3. Nächster Schritt

Sehen Sie die Privileged Access Bridge an Ihrem eigenen Anwendungsfall. In einer kurzen Demo zeigen wir Session-Recording, Live-Aufsicht mit Not-Aus und den Audit-Trail live — an einem Beispiel aus Ihrer Umgebung.

Demo anfragen: www.blackfort-tec.de/pab · Antwort binnen 1 Werktag, unverbindlich.

Blackfort Technology — Security-Beratung und -Produkte aus Deutschland. Gegründet von Christian Gebhardt: zuvor Deputy CISO der Gothaer Solutions (DORA/VAIT) und mehrjähriger Auditleiter in der Internen Revision der Postbank und Deutsche Bank; Erstautor des ACS/BSI-Leitfadens „Penetrationstests von LLM" und Mitglied der KI-Facharbeitsgruppe der Allianz für Cybersicherheit (BSI).