BLACKFORT TECHNOLOGY · PRIVILEGED ACCESS MANAGEMENT

Blackfort
Privileged Access Bridge

Privilegierten und externen Fernzugriff sichtbar machen, kontrollieren und nachweisen – agentenlos, souverän, im eigenen Rechenzentrum.

Juni 2026 · Blackfort Technology · blackfort-tec.de · vertraulich

MANAGEMENT SUMMARY

Die Kernbotschaft

Warum privilegierter Zugriff jetzt im Fokus steht

- Privilegierter Zugriff ist das höchste IT-Risiko – und zugleich der am wenigsten kontrollierte Pfad in den meisten Organisationen.
- Externe Dienstleister und Administratoren brauchen Zugang zu kritischen Systemen – heute oft über VPN, Sprungserver und Einzelkonten ohne lückenlosen Nachweis.
- PAB bündelt diesen Zugriff in einem agentenlosen Gateway: jede Sitzung wird aufgezeichnet, beaufsichtigt und fälschungssicher protokolliert.
- Betrieb On-Premises und EU-souverän, auf Wunsch als Managed Service durch Blackfort – die Governance bleibt beim Kunden.

> *Sie können nur verantworten, was Sie sehen und beenden können – PAB macht privilegierten Zugriff kontrollierbar und beweisbar.*

DIE AUSGANGSLAGE

Privilegierter Zugriff ist das größte Risiko

03

Die meisten schweren Vorfälle laufen über privilegierte Konten und Fernzugänge.

RISIKOLAGE

Wo es heute wehtut

Privilegierte und externe Zugriffe – die typischen Schwachstellen

- Privilegierte Konten sind das Hauptziel von Angreifern: ist ein Admin-Zugang kompromittiert, steht die Kerninfrastruktur offen.
- Fernzugriffe externer Dienstleister sind ein Lieferketten-Risiko – fremde Identitäten, fremde Endgeräte, oft ohne durchgängige Aufzeichnung.
- Klassische Wege (VPN mit RDP/SSH, Sprungserver, geteilte Konten) hinterlassen lückenhafte, schwer zuordenbare Spuren.
- Ohne lückenlosen Nachweis fehlt im Ernstfall die forensische Grundlage – und im Audit der Beleg wirksamer Kontrollen.
- Software-Agenten auf den Zielsystemen vergrößern Angriffsfläche und Pflegeaufwand.

> *Der gefährlichste Zugang ist der, den niemand mitschneidet und niemand sofort stoppen kann.*

DIE LÖSUNG

Blackfort Privileged Access Bridge

05

Ein agentenloses Gateway für privilegierten Zugriff – kontrolliert, aufgezeichnet, beweisbar.

ÜBERBLICK

Was PAB ausmacht

Drei Eigenschaften, die zusammenwirken

Agentenlos & browserbasiert

- Zugriff allein über den Browser – keine Software auf Client oder Zielsystem.
- Nur das gerenderte Sitzungsbild erreicht den Arbeitsplatz, kein aktiver Code.
- Unterstützt RDP, SSH, VNC, Telnet und Kubernetes.

Souverän & On-Premises

- Betrieb im eigenen Rechenzentrum, in der EU.
- Keine fremde Cloud-Steuerungsebene im Zugriffspfad.
- Optional als Managed Service durch Blackfort.

Lückenlos auditierbar

- Jede Sitzung wird aufgezeichnet und ist wiedergebbar.
- Fälschungssicherer, akteur-genauer Audit-Trail.
- Live-Aufsicht und sofortiges Beenden laufender Sitzungen.

ARCHITEKTUR

Wie ein Zugriff abläuft

Ein einziger kontrollierter Pfad – ohne Eingriff am Zielsystem

- Der Administrator meldet sich nur am PAB-Portal an – nie mit direktem Netzpfad zum Ziel.
- Das Sitzungs-Token bleibt serverseitig; im Browser liegt nur ein gehärtetes Sitzungscookie.
- Die Plattform baut die Verbindung auf und überträgt ausschließlich Pixel und Eingaben.
- Aufzeichnung, Audit und Aufsicht greifen zentral – für jede Verbindung, agentenlos.

Ein kontrollierter Pfad statt vieler offener Türen.

FUNKTION · NACHWEIS

Lückenlose Aufzeichnung & Wiedergabe

Jede privilegierte Sitzung – vollständig dokumentiert

- Jede privilegierte Sitzung wird vollständig als Video aufgezeichnet – aktiv auf allen Verbindungen, nicht optional.
- Grafische Sitzungen (RDP, VNC) wie Terminal-Sitzungen (SSH, Telnet, Kubernetes) werden gleichermaßen vollständig erfasst.
- Aufzeichnungen sind direkt im Portal auffindbar und abspielbar – kein Export, kein Drittwerkzeug nötig.

- Wer wann auf welchem System war, ist jederzeit nachvollziehbar – Grundlage für Forensik und Auditnachweis.

> *Vollständige Sicht auf jede Sitzung – aufgezeichnet, wiedergebbar, nachweisbar.*

FUNKTION · KONTROLLE

Live-Aufsicht & NOT-AUS

Mitsehen und im Zweifel sofort eingreifen

- Ein Aufseher verfolgt eine laufende privilegierte Sitzung in Echtzeit mit – schreibgeschützt, ohne selbst zu steuern.
- Im Zweifel beendet er die Sitzung sofort (NOT-AUS) – auch mitten in der Aktion.
- Die Aufsicht funktioniert ohne Administratorrechte des Aufsehers und ist vom Operator nicht verhinderbar.
- So wird wirksame Vier-Augen-Aufsicht über besonders kritische Zugriffe technisch durchsetzbar.

> *Mitsehen, wenn es zählt – und eingreifen, bevor Schaden entsteht.*

FUNKTION · NACHWEISBARKEIT

Fälschungssicherer Audit-Trail

Wer – wann – was, eindeutig zugeordnet

- Sicherheitsrelevante Aktionen werden als strukturierte, fälschungssichere Einträge erfasst – mit echtem Akteur, Zeit und Aktion.
- Erfasst werden u. a. das Beenden einer Sitzung (NOT-AUS) sowie Datei-Transfers in und aus der Sitzung.
- Die Zuordnung erfolgt am Zugangs-Broker – der tatsächliche Nutzer ist eindeutig, nicht hinter einem technischen Dienstkonto verborgen.
- Prüffähige Nachweise für interne Revision, Risikokontrolle und externe Audits.

> *Nachweise, die im Audit standhalten – akteur-genau und fälschungssicher.*

FUNKTION · VERWALTUNG

Administration & Governance

Feingranulare Kontrolle im eigenen Portal

- Vollständige Verwaltung im Portal: Verbindungen, Verbindungsgruppen, Benutzer, Benutzergruppen und eine feingranulare Rechte-Matrix.
- Konten lassen sich zeitlich befristen (gültig von / bis) und auf Zugriffsfenster (Wochentage, Uhrzeiten) begrenzen.
- Datei-Transfer und Zwischenablage je Verbindung gezielt freigeben oder sperren.
- Alle unterstützten Verbindungs- und Protokolloptionen sind vollständig abgedeckt – ohne Funktionslücke gegenüber der Plattform.

> *Feingranulare Kontrolle – wer, worauf, wann und wie.*

SICHERHEIT

Sicherheit by Design

Internetfähig – und genau dafür gehärtet

- Das Sitzungs-Token bleibt serverseitig; im Browser liegt nur ein HttpOnly-, Secure- und SameSite-Cookie.
- Schutz gegen Cross-Site-Request-Forgery, strikte Content-Security-Policy, HSTS und Rate-Limiting an der Edge.
- Exakt gepinnte Komponenten, automatisierte Sicherheits-Scans und Software-Stückliste (SBOM) in der Build-Kette.
- Privilegierte Aktionen (Aufsicht, NOT-AUS, Datei-Transfer) laufen rollengebunden über den kontrollierten Broker.

> *Sicherheit ist nicht aufgesetzt, sondern in die Architektur eingebaut.*

REGULATORIK

PAB im regulatorischen Kontext

14

Privilegierter Zugriff ist in nahezu jedem Rahmenwerk eine Kernanforderung.

ANKNÜPFUNGSPUNKTE

Wo PAB auf Anforderungen einzahlt

Implementierte Funktionen, den gängigen Rahmenwerken zugeordnet

Rahmenwerk	Anforderung an privilegierten Zugriff	Erfüllt durch PAB (implementiert)
DORA (EU 2022/2554)	Schutz & Zugriffskontrolle (Art. 9); Steuerung von IKT-Drittparteien inkl. Audit-/Exit-Strategie (Art. 28/30)	Gebündelter, aufgezeichneter Dienstleister-Zugang; Break-Glass-/Exit-Modell; akteur-genauer Audit
NIS2 (EU 2022/2555)	Risikomanagement mit Zugriffskontrolle und Lieferkettensicherheit (Art. 21)	Zentrale Zugriffskontrolle; Aufzeichnung & Protokollierung externer Zugriffe
ISO/IEC 27001:2022	Privilegierte Zugriffsrechte (A.8.2); Protokollierung (A.8.15); Überwachung (A.8.16)	Rechte-Matrix & Befristung; lückenlose Aufzeichnung; Live-Aufsicht
IEC 62443-3-3 (OT)	Authentisierung, Nutzungskontrolle, auditierbare Ereignisse (SR 1.x / 2.x)	Agentenloser, kontrollierter OT-Fernzugriff mit Sitzungsaufzeichnung
BSI IT-Grundschutz	Identitäts-/Berechtigungsmanagement (ORP.4); sichere Fernwartung (OPS)	Zentrales Zugriffsgateway; befristete Konten; Aufzeichnung
DSGVO	Sicherheit der Verarbeitung & Nachvollziehbarkeit (Art. 32)	Nachvollziehbarer Zugriff auf Systeme mit personenbezogenen Daten

PAB liefert die technischen Kontrollen und prüffähigen Nachweise – die Compliance-Bewertung bleibt bei Ihnen.

IKT-Drittparteienrisiko gezielt adressiert

Externer Zugriff – vom Risiko zum kontrollierten Prozess

- Externe Dienstleister erhalten Zugang ausschließlich über PAB – gebündelt, aufgezeichnet und jederzeit entziehbar.
- Die Governance bleibt beim Kunden: Sie entscheiden, wer Zugriff erhält; Blackfort verantwortet den sicheren technischen Ablauf.
- Break-Glass-Notfallzugang und dokumentierte Übergabe adressieren die geforderte Exit- und Kontinuitätsstrategie (DORA Art. 28).
- Kein zusätzlicher unbekannter Drittanbieter im privilegierten Pfad – sondern die Erweiterung einer bestehenden, geprüften Beziehung.

> *Drittparteien-Zugriff wird vom Risiko zum kontrollierten, nachweisbaren Prozess.*

ZIELGRUPPEN

Für jede Rolle der passende Nutzen

Ein Werkzeug, fünf Perspektiven

Rolle	Zentrale Frage	Was PAB liefert
IT-Administration	Wie arbeite ich sicher und ohne Reibung?	Browserzugriff ohne Client-Setup; alle Protokolle; Datei-Transfer & Zwischenablage steuerbar
Leitung IT	Wie behalte ich Betrieb und Kosten im Griff?	Zentrales, agentenloses Gateway; On-Prem oder Managed Service; vollständig automatisiert betrieben
CISO	Sind privilegierte Zugriffe kontrolliert und beweisbar?	Aufzeichnung, Live-Aufsicht, NOT-AUS, fälschungssicherer Audit
IKT- / Risikokontrolle	Halten unsere Kontrollen dem Audit stand?	Akteur-genaue Nachweise; befristete Rechte; Anknüpfung an DORA/NIS2/ISO
Vorstand	Reduziert das unser Risiko – souverän und angemessen?	Geringeres Angriffs- und Drittparteienrisiko; EU-Souveränität; belegte Sicherheit

Ein Werkzeug – fünf Perspektiven, die zusammenpassen.

Betrieb & Souveränität

Wie PAB läuft – und wer es betreibt

Souverän & On-Prem

- Betrieb im eigenen Rechenzentrum (VMware, Hyper-V, Proxmox, KVM).
- Daten und Steuerung in der EU.
- Keine fremde Cloud-Steuerungsebene.

Managed Service

- Blackfort übernimmt Betrieb, Wartung und Updates.
- Optionales Break-Glass-Modell: Kunde ohne Standing-Admin, nur Notfallzugang.
- Ein Ansprechpartner für Betrieb und Sicherheit.

Automatisiert & aktuell

- Vollständig als Code betrieben – versioniert und reproduzierbar.
- Updates per Neuaufbau statt Eingriff im Bestand.
- Sicherheits-Scans fest in der Build-Kette.

POSITIONIERUNG

Warum Blackfort

Souveränität, Compliance und Umsetzung – aus einer Hand

- Deutscher Anbieter, EU-souveräner Betrieb – kein Hyperscaler-Lock-in im privilegierten Pfad.
- Compliance- und Technik-Kompetenz verbunden: Regulatorik (DORA/NIS2/ISO 27001) trifft echte Umsetzung.
- Agentenlos und schlank – Einführung ohne Roll-out auf Endgeräten oder Zielsystemen.
- Managed Service aus einer Hand: ein Ansprechpartner für Betrieb, Sicherheit und Weiterentwicklung.
- Produkt aktiv im Einsatz.

> *Wir setzen um, was wir verkaufen – PAB betreiben wir selbst.*

NÄCHSTER SCHRITT

Privilegierten Zugriff sichtbar und beweisbar machen

Lassen Sie uns einen Pilot auf Ihre kritischsten Zugriffe ansetzen.

- Gemeinsame Identifikation der kritischsten privilegierten und externen Zugriffe.
- Aufbau einer PAB-Instanz in Ihrer Umgebung – On-Prem oder als Managed Service.
- Nachweisbare Kontrolle: Aufzeichnung, Aufsicht und Audit-Trail ab Tag 1.

Blackfort Technology · info@blackfort-tec.de · +49 228 29978061 · blackfort-tec.de