Internal Use Only

Global Leader In
Cybersecurity

Bitdefender®



Bitdefender

Wer kontrolliert wirklich Ihre Cybersicherheit?

**Risiken verringern,
ohne Sicherheit zu beeinträchtigen**



Internal Use Only

Bitdefender

Umfrage 1

Inwiefern spielt digitale Souveränität in Ihrem Unternehmen eine Rolle?

a) Wir planen konkret, so souverän wie möglich zu werden.

b) Wir haben es auf dem Schirm, es ist aber noch nicht konkret.

c) Für uns ist es aktuell nicht wichtig.

Internal Use Only

Bitdefender

Souveränität ist ein Kaufkriterium für Cybersicherheit

DATENSOUVERÄNITÄT

76,1 %

der Organisationen betrachten Datensouveränität als zentrales Kriterium bei der Auswahl einer Cybersecurity-Plattform.*

*Bitdefender Cybersecurity Assessment 2026.



Geopolitische Unsicherheit

Organisationen wollen mehr Kontrolle über kritische digitale Infrastruktur



Steigende Governance-Anforderungen

NIS2, DORA und nationale Initiativen verstärken die Prüfung von Governance und 3rd-Party-Risiken



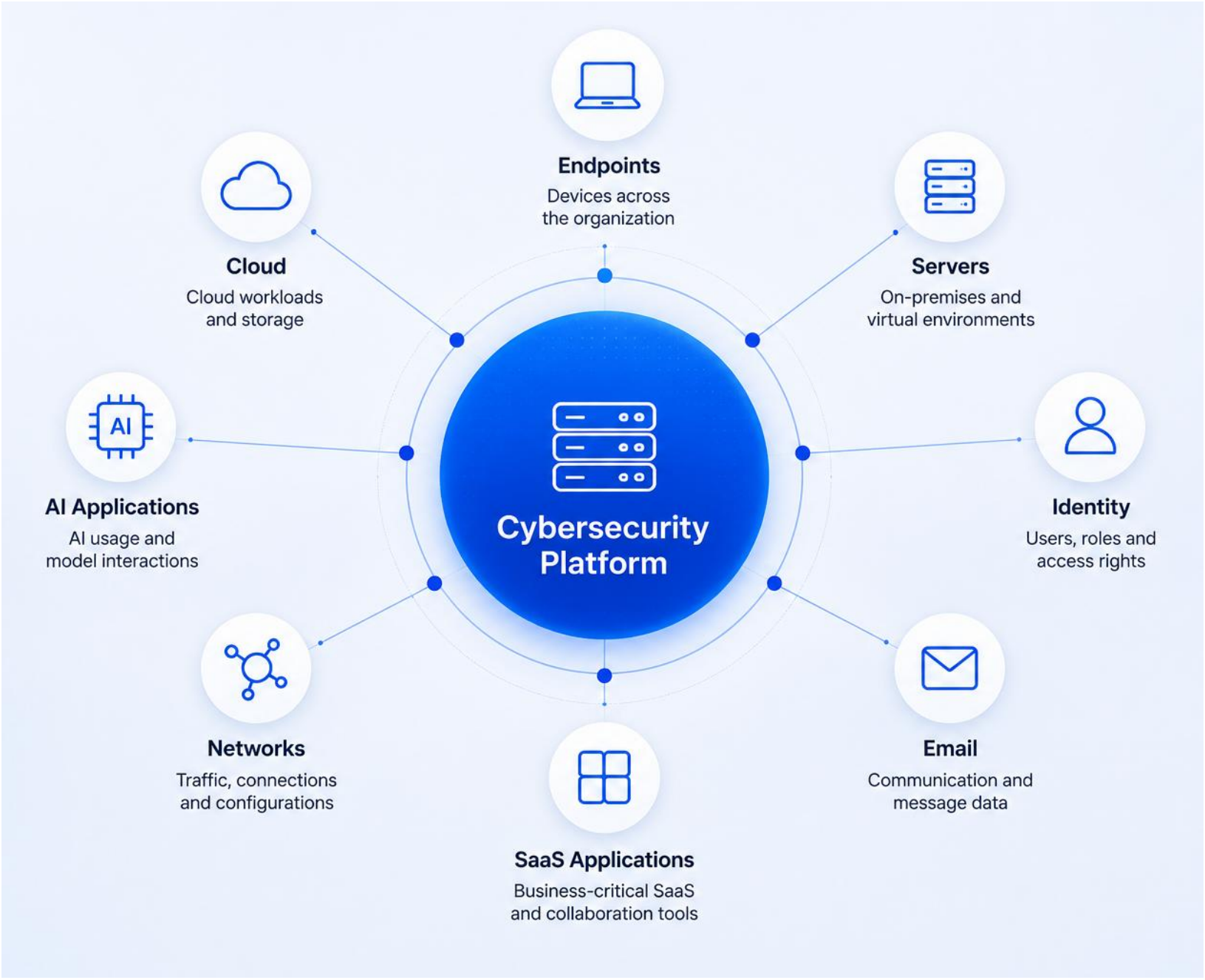
Wachsende Menge an Sicherheitsdaten

Vernetzte Plattformen verarbeiten immer größere Mengen sensibler Betriebsdaten

Bitdefender

Ihre Cybersecurity-Plattform enthält mehr als nur Sicherheitsdaten

… möglicherweise den **umfangreichsten Betriebsdatensatz** Ihrer Organisation.



Internal Use Only

Bitdefender

Umfrage 2

Wenn Sie an digitale Souveränität denken, welche der folgenden Kriterien spielen dabei die wichtigste Rolle?

a) Wo liegen die Daten?

b) Wer hat Zugriff auf die Daten

c) Wer hat die Hoheit über die Anwendung?

d) Alle drei gleich wichtig

Bitdefender

Datenlokalisierung ist nur ein Teil der Souveränität

Datenlokalisierung ≠ Datensouveränität

Datenlokalisierung

Wo liegen meine Daten?

- ☑ Betrifft den physischen Standort
- ☑ Regelt Speicherung und Verarbeitung innerhalb einer geografischen Grenze
- ☑ Wichtig, aber nur ein Teil der Frage

- ☑ Betrifft Rechtsraum, Governance und letztliche Kontrolle
- ☑ Bestimmt, wer auf Ihre Daten zugreifen, sie verarbeiten oder Zugriff erzwingen kann
- ☑ Legt fest, ob Ihre Daten wirklich nach den von Ihnen gewählten Gesetzen geschützt sind

Der Standort ist ein Teil der Souveränität. Governance bestimmt sie.

Bitdefender

Souveränität erfordert drei Kontrolleinstanzen

DATEN-SOUVERÄNITÄT

Kontrolle über Sicherheitsdaten

Stellt sicher, dass Telemetrie, Protokolle und Vorfallsdaten unter europäischer Governance geschützt bleiben.

TECHNISCHE SOUVERÄNITÄT

Kontrolle über die Technologie

Stellt sicher, dass die Cybersecurity-Plattform selbst europäischem Recht unterliegt.

OPERATIVE SOUVERÄNITÄT

Kontrolle über den Betrieb

Stellt sicher, dass Sicherheitsdienste und operative Kontrolle unter europäischer Governance bleiben.

Souveränität entsteht erst, wenn alle drei Formen der Kontrolle zusammenwirken.

Bitdefender

Regulierungen erhöhen die Anforderungen an Governance und Drittparteirisiken



NIS2

Operative Resilienz
- Organisationen müssen kritische IKT-Abhängigkeiten und Lieferkettenrisiken kennen.

DORA

Drittparteirisiken
- Finanzunternehmen müssen IKT-Dienstleister über den gesamten Lebenszyklus steuern.

Nationale Souveränitätsinitiativen

Strategische Kontrolle
- Öffentlicher Sektor und regulierte Branchen berücksichtigen bei der Auswahl von Technologieanbietern zunehmend Rechtsraum und Governance.

Von Organisationen wird erwartet, Technologie-, Governance- und Drittparteirisiken zu verstehen und zu steuern – nicht nur technische Leistung.

Internal Use Only

Bitdefender

Umfrage 3

Wo stehen Sie heute bei der Bewertung des Risikos durch Abhängigkeiten von US-Unternehmen?

a) Wir haben eine umfangreiche Risiko-Bewertung vorgenommen

b) Wir beginnen gerade mit der Risiko-Bewertung

c) Wir haben noch keine Risiko-Bewertung vorgenommen

d) Wir sehen da kein für uns relevantes Risiko

Bitdefender

Eine **ausgereifte Souveränitätsstrategie** erfordert **fortlaufende Governance**

PROPRIETARY AND CONFIDENTIAL

STRATEGIE IN DER PRAXIS

Ein wiederholbarer Bewertungsprozess in fünf Schritten

01 **Pflichten verstehen**
Ergebnis: Anforderungsübersicht

02 **Anbieter bewerten**
Ergebnis: Inventar der Abhängigkeiten und Zugriffe

03 **Rechtsraum- und Betriebsrisiko bewerten**
Ergebnis: Eigentums- und Kontrollrisiken

04 **Technologieentscheidungen steuern**
Ergebnis: dokumentierte Prüfung und Freigabe

05 **Fortlaufend überwachen**
Ergebnis: Nachweise, Status und Neubewertung

Bitdefender

Sovereignty Framework

Hilfsmittel – aber ein Erstversuch!



#	Sovereignty Objectives	Weight in Scoring
SOV-1	Strategic Sovereignty	15%
SOV-2	Legal & Jurisdictional Sovereignty	10%
SOV-3	Data & AI Sovereignty	10%
SOV-4	Operational Sovereignty	15%
SOV-5	Supply Chain Sovereignty	20%
SOV-6	Technology Sovereignty	15%
SOV-7	Security & Compliance Sovereignty	10%
SOV-8	Environmental Sustainability	5%
	Total	100%

Bitdefender

… und etwas lokaler und genauer

„Der Kriterienkatalog C3A **eine Bewertung, ob ein Cloud-Angebot** im jeweiligen Risikokontext **selbstbestimmt genutzt werden kann**.

Die C3A dienen dabei als richtungsweisender Handlungsrahmen und schaffen Transparenz, entfalten jedoch keine regulative Wirkung.



Internal Use Only

Bitdefender

Ein einheitlicher Ansatz für Cybersecurity-Souveränität

DATEN-SOUVERÄNITÄT

Datenlokalisierung und Zugriffskontrolle innerhalb der EU

- Datenspeicherung und -verarbeitung in der EU
- Kontrollierter Zugriff auf Sicherheitsdaten
- Vertrauenswürdige, zertifizierte souveräne europäische Cloud-Infrastruktur

TECHNISCHE SOUVERÄNITÄT

Technologie unter EU-Rechtsraum

- In Europa entwickelte Cybersecurity-Technologie
- Unterliegt dem EU-Rechtsrahmen
- Geringere Exponierung gegenüber Rechtsordnungen außerhalb der EU

OPERATIVE SOUVERÄNITÄT

Europäische Kontrolle über Betrieb und Servicebereitstellung

- Security Operations und Support in der EU
- Monitoring, Analyse und Reaktion innerhalb der EU
- EU Sovereign MDR

Europäisches Ökosystem aus souveräner Infrastruktur und Betrieb.

OVHcloud | secunet

CYBERSECURITY MADE IN EUROPE™

In Europa entwickelt • In Europa betrieben • EU-Governance

European DIGITAL SME Alliance — Issued by the European DIGITAL SME Alliance

EU Sovereign MDR / Managed SOC

KI-gestütztes, menschlich gesteuertes MDR unter EU-Kontrolle

24×7 Managed Detection & Response vollständig im souveränen EU-Betriebsmodell

Was macht es souverän?

- 24×7×365 MDR durch EU-Experten aus einem SOC in der EU
- Monitoring, Untersuchungen und Incident Response bleiben vollständig in der EU
- Keine Follow-the-Sun-Übergaben oder Eskalationen außerhalb der EU
- Threat Research, Malware-Analyse und Detection Engineering bleiben in der EU
- KI-gestützte Untersuchungen nutzen souverän gehostete LLMs; Kundendaten werden nie von öffentlichen KI-Diensten verarbeitet

Menschen, Prozesse, Werkzeuge und Servicebereitstellung bleiben unter EU-Kontrolle – auch während der Incident Response.

Bitdefender

Souveräne Cybersicherheit für Deutschland mit secunet



GravityZone verbindet in Europa entwickelte Cybersicherheit mit zertifizierter souveräner Cloud-Infrastruktur von SysEleven, einem Unternehmen der secunet.

Hosting in Deutschland

Deutsche souveräne Kontrolle

- GravityZone wird in der SysEleven Cloud in Deutschland gehostet und unterstützt Bitdefender-Kunden bei der Einhaltung von EU- und deutschen Vorschriften.

BSI-zertifiziertes Cloud-Hosting

Zertifizierte Infrastruktur

- SysEleven verfügt über ISO 27001 auf Basis von BSI IT-Grundschutz sowie C5-Testat und SCS-Zertifizierung.

EU-Governance

Für anspruchsvolle Umgebungen konzipiert

- Unterstützt Organisationen mit strengen deutschen und EU-Anforderungen an Souveränität und Compliance.

In Europa entwickelte Cybersicherheit • Zertifizierte deutsche Cloud • Hosting in Deutschland

Bitdefender

Cybersecurity-Souveränität bewerten

Ein praxisnahes Fünf-Schritte-Modell zur Bewertung der Souveränitätsreife Ihrer Organisation.

01
Pflichten verstehen

Welche Regulierungen und Governance-Anforderungen gelten für uns?

- NIS2, DORA, DSGVO
- Branchenspezifische Anforderungen
- Nationale und lokale Pflichten

02
Anbieter bewerten

Welche Anbieter verarbeiten unsere Sicherheitsdaten oder haben Zugriff darauf?

- Sicherheitsplattform
- Cloud-Anbieter
- MDR und Partner
- SaaS und Dritte

03
Rechtsraumrisiko bewerten

Welches Recht gilt für den Anbieter?

- Eigentum und Rechtsraum
- Extraterritoriales Risiko
- Daten- und Kontrollrisiken
- Vertragsschutz

04
Governance formalisieren

Sind diese Entscheidungen begründet und dokumentiert?

- Aufsicht der Leitung
- Risikoakzeptanz
- Nachweisbarkeit
- Compliance-Prüfung

05
Fortlaufend überwachen

Können wir dauerhaft nachweisen, steuern und verbessern?

- Durchgehende Transparenz
- Compliance-Überwachung
- Sicherheitsniveau
- Laufende Neubewertung

Internal Use Only

Thank you

