

Infinigate Attack Prevention Service

Reseller Sales Playbook

Executive Summary	4
Kundenstory: Der Angriff, der nicht stattfand	5
Das Unternehmen	5
Der Trigger: NIS2-Compliance	5
Die Entdeckung	5
Szenario ohne APS	6
Szenario mit APS	6
Das Ergebnis	6
Featuretexte – kundensprachlich	7
Dashboard	7
Domain Screening	7
Credential Leak Detection	7
Dark Web Monitoring	8
Metadaten-Analyse	8
CSV Export	9
Zeitfilter	9
Infotexte	9
Feature-Benefit-Tabelle	10
Die aktuelle Bedrohungslage	11
Schadensbilanz Deutschland 2025	11
BSI Lagebericht 2025	11
BKA Bundeslagebild Cybercrime 2024	11
Bitkom Cyberkriminalität 2025	12
Verizon DBIR 2025 – Globale Trends	12
ENISA Threat Landscape 2025	12
Deutsche Cyberangriffe	13
Typische Angriffskette – Kill Chain	14
APS in der Defense-in-Depth-Strategie	15
NIS2 & Compliance	16
Wer ist betroffen?	16
Die wichtigsten NIS2-Pflichten	16
Wie APS bei der NIS2-Compliance hilft	17
Für wen ist APS?	18
Ideale Verkaufssituationen	18
Top 10 Verkaufsargumente	19
1. Frühwarnsystem statt Reaktion	19
2. Made in Germany	19
3. Menschlich validiert – kein Daten-Rauschen	19
4. NIS2-Compliance-Baustein	19

5. Ab 250 Euro – weniger als 9 Euro pro Tag	19
6. Kein Security-Team erforderlich	19
7. Credentials + Phishing = 38 % aller Breaches	20
8. Schnelles Onboarding – kein Agent, kein Netzwerkzugang	20
9. Recurring Revenue für Partner	20
10. Bewährte Technologie – 4.000+ Projekte	20
Pricing & Packaging	21
NFR-Lizenzen für Partner	22
SLA-Details	22
ROI-Berechnung für Kundengespräche	22
90-Tage Partner-Aktivierungsplan	23
Phase 1: Foundation (Tag 1-30)	23
Phase 2: Aktivierung (Tag 31-60)	23
Phase 3: Conversion (Tag 61-90)	23
Aktivierungs-Timeline	24
Praxis-Tipps für jede Phase	25
Akquise-Phase	25
Aktivierungs-Phase	25
Abschluss-Phase	25
Erfolgsmetriken nach 90 Tagen	25
Partnerassets	26
30-Sekunden Elevator-Pitch	26
5-Minuten Pitch	26
Phase 1: Bedrohungslage (60 Sekunden)	26
Phase 2: Die Lücke aufzeigen (60 Sekunden)	26
Phase 3: APS vorstellen (90 Sekunden)	26
Phase 4: Konkretes Beispiel (60 Sekunden)	26
9 Discovery-Fragen	27
Einwandbehandlung	28
Case-Templates	29
Case 1: Mittelständischer Maschinenbauer	29
Case 2: Regionalbank	29
Case 3: Klinikverbund	30
Case 4: E-Commerce-Unternehmen	30
Case 5: Stadtwerke (Energieversorger)	30
Case 6: IT-Systemhaus (MSP/MSSP)	30
FAQ – Häufig gestellte Fragen	31
Kontakt & Nächste Schritte	33
Für Partner: So starten Sie sofort	33
Kontaktinformationen	33
Quellenliste	34

Executive Summary

Der Infinigate Attack Prevention Service (APS) ist das Frühwarnsystem für IT-Sicherheit, das bestehende Schutzmaßnahmen um eine entscheidende Dimension erweitert: den Blick nach außen. Während Firewalls und EDR-Lösungen das interne Netzwerk schützen, erkennt APS Bedrohungen außerhalb des Unternehmens, im Darknet, in Leak-Datenbanken, und erkennt Phishing-Webseiten, bevor Angreifer zuschlagen können.

Entwickelt in Kooperation mit antago (ISO 27001/9001/27701 zertifiziert), vereint APS KI-gestützte Analyse, Deep-Dark-Web-Recherche, HUMINT und OSINT, gestützt auf operative Erfahrung aus über 4.000 Spionage- und Cyberwar-Projekten. Der Datalake steht in Deutschland. Die Lösung wurde auf der it-sa 2025 in Nürnberg erstmals vorgestellt.

Warum jetzt? Die Bedrohungslage in Deutschland hat 2025 einen neuen Höchststand erreicht. Laut BSI werden täglich 119 neue Schwachstellen entdeckt¹, der Gesamtschaden durch Cyberkriminalität beträgt 289 Mrd. Euro². Seit Dezember 2025 ist das NIS2-Umsetzungsgesetz in Kraft, über 30.000 Unternehmen sind betroffen, und die Geschäftsleitung haftet persönlich³.

Was Partner davon haben: APS bietet ein sofort vertriebsfähiges Managed-Security-Angebot mit planbarem Recurring Revenue. Drei Pakete ab 250 Euro pro Monat ermöglichen den Einstieg für jedes Kundensegment. NFR-Lizenzen mit 50 % Dauerrabatt sichern den risikofreien Eigenbetrieb. Mit dem 90-Tage-Aktivierungsplan erreichen Partner ihren ersten Abschluss innerhalb von drei Monaten.

Kernzahlen auf einen Blick:

Kennzahl	Wert
Gesamtschaden Cybercrime DE	289,2 Mrd. Euro (2025) Kennzahl
Davon Cyberattacken	202,4 Mrd. Euro (70 %)
NIS2-betroffene Unternehmen	Über 30.000
Ransomware trifft KMU	80 %
Neue Schwachstellen pro Tag	119 (+24 % YoY)
Einstiegspreis APS	ab 250 Euro/Monat
NFR-Rabatt für Partner	50 % dauerhaft (Advanced)

¹BSI Lagebericht 2025: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

²Bitkom Wirtschaftsschutz 2025: <https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz>

³IHK Muenchen NIS2: <https://www.ihk-muenchen.de/ratgeber/digitalisierung/informationssicherheit/nis-2-kritis/>

Kundenstory: Der Angriff, der nicht stattfand

Im Januar 2026 startet Schmitt Bremsen ein NIS2-Compliance-Projekt. Als Zulieferer eines KRITIS-Unternehmens fällt die Firma unter die erweiterten NIS2-Pflichten . Der externe Berater identifiziert eine Lücke: Es gibt keine Lösung für externe Bedrohungserkennung. Weder werden Darknet-Quellen überwacht, noch gibt es ein Credential Monitoring. Der beauftragte Infinigate-Partner empfiehlt den Attack Prevention Service.

Das Unternehmen

Firma: Schmitt Bremsen GmbH (fiktiv), mittelständischer Zulieferer für die Automobilindustrie. 300 Mitarbeitende, Sitz in Baden-Württemberg. Jahresumsatz: 85 Mio. Euro. Kunden: drei große OEMs, darunter ein DAX-Konzern. IT-Abteilung: 8 Personen unter IT-Leiter Dieter Wagner.

Dieter ist stolz auf seine IT-Infrastruktur. Next-Gen-Firewall von einem führenden Hersteller, EDR auf jedem Endpoint, regelmäßige Patches, jährlicher Pentest. Die IT-Abteilung arbeitet professionell. Doch Dieter hat einen blinden Fleck: Er weiß nicht, was außerhalb seines Netzwerks passiert. Er weiß nicht, ob Zugangsdaten seiner Mitarbeiter im Darknet kursieren. Er weiß nicht, ob jemand eine Domain registriert hat, die seiner Firma zum Verwechseln ähnlich sieht.

Der Trigger: NIS2-Compliance

Im Januar 2026 startet Schmitt Bremsen ein NIS2-Compliance-Projekt. Als Zulieferer eines KRITIS-Unternehmens fällt die Firma unter die erweiterten NIS2-Pflichten⁴. Der externe Berater identifiziert eine Lücke: Es gibt keine Lösung für externe Bedrohungserkennung. Weder werden Darknet-Quellen überwacht, noch gibt es ein Credential Monitoring. Der beauftragte Infinigate-Partner empfiehlt den Attack Prevention Service.

Die Entdeckung

Bereits beim Onboarding liefert APS alarmierende Ergebnisse:

- **8 Mitarbeiter-Credentials** aus einem Datenbank-Leak von 2024 tauchen in einer Darknet-Datenbank auf, darunter die E-Mail-Adresse und das Passwort des Geschäftsführers. Zwei der Passwörter sind noch aktiv.
- **Eine registrierte Domain** ‘schmitt-bremsen.de’ (doppeltes i) wird erkannt, offensichtlich für Phishing vorbereitet. Die Domain ist erst 3 Wochen alt.
- **Metadaten-Scan** zeigt: In einer PDF-Stellenausschreibung auf der Unternehmenswebsite sind interne Hostnamen und Active-Directory-Kontennamen sichtbar.

⁴BSI NIS2: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

Szenario ohne APS

Die Angreifer hätten die geleakten Credentials für einen initialen Zugriff genutzt, etwa über das VPN oder Webmail. Laut Verizon DBIR 2025 beginnen 22 % aller Datenverletzungen mit gestohlenen Zugangsdaten⁵. Die Phishing-Domain hätte für gezielte Spear-Phishing-Mails an Mitarbeitende und Kunden gedient. Ein typisches Ransomware-Playbook: Credentials + Phishing = Netzwerkzugang = Lateral Movement = Verschlüsselung. Durchschnittlicher Schaden bei einem Ransomware-Angriff auf ein mittelständisches Unternehmen: 1,82 Mio. Euro. Dazu kämen Produktionsausfall, Reputationsschaden und mögliche Vertragsverluste beim DAX-Kunden.

Szenario mit APS

Dieter erhält am Tag nach dem Onboarding eine Warnung im Dashboard. Sein Partner hilft bei der sofortigen Reaktion:

- Sofort-Maßnahme 1: Passwort-Reset aller 8 betroffenen Accounts, MFA-Aktivierung für alle Mitarbeiter
- Sofort-Maßnahme 2: Der Reseller bewertet die erkannte Phishing-Domain und initiiert anschließend geeignete Gegenmaßnahmen, etwa das Hardening der Firewall-Regeln sowie die Einleitung eines Domain-Takedowns beim zuständigen Registrar oder Hosting-Provider.
- Sofort-Maßnahme 3: Bereinigung der Metadaten in allen öffentlichen Dokumenten

Gesamtkosten: 250 Euro pro Monat für APS Advanced. Vermiedener Schaden: potenziell Millionen.

Das Ergebnis

Schmitt Bremsen nutzt APS heute dauerhaft. Sein Geschäftsführer schläft besser, und die NIS2-Compliance-Dokumentation enthält jetzt einen nachweisbaren Baustein für externe Bedrohungserkennung.

 APS hat uns gezeigt, was wir nicht wussten. und genau das hätte uns das Genick brechen können.”

Dieter Wagner, IT-Leiter, Schmitt Bremsen GmbH (fiktiv)

⁵Verizon DBIR 2025: <https://www.verizon.com/business/resources/reports/dbir/>

Featuretexte – kundensprachlich

Die folgenden Beschreibungen sind für den direkten Einsatz im Kundengespräch formuliert. Jedes Feature wird verständlich erklärt, der konkrete Nutzen dargestellt und mit einem praxisnahen deutschen Beispiel unterlegt.

Dashboard

Das APS Dashboard ist Ihre zentrale Kommandozentrale. Alle Findings, von Credential Leaks über Phishing-Domains (nach Schweregrad priorisiert) bis zu Darknet-Erwähnungen, werden übersichtlich auf einen Blick dargestellt. Flexible Zeitfilter (1 Woche, 2 Wochen, 1 Monat, 3 Monate, Custom) ermöglichen gezielte Analysen.

Kundennutzen: Auf einen Blick sehen, wo Handlungsbedarf besteht, ohne sich durch verschiedene Tools klicken zu müssen. Zeitersparnis für die IT-Abteilung, klare Priorisierung für die Geschäftsführung.

Praxisbeispiel: Der IT-Leiter eines Maschinenbauers öffnet morgens das Dashboard und sieht sofort: 3 neue Findings in der letzten Woche. Er kann sofort handeln, ohne erst lange nach Informationen suchen zu müssen.

Domain Screening

APS überwacht kontinuierlich neue Domain-Registrierungen weltweit und erkennt Typosquatting, Lookalike-Domains und Phishing-Domains, die Ihrem Unternehmen ähnlich sehen. Die Erkennung basiert auf Algorithmen, die Zeichenaustausch, homoglyphe Zeichen und ähnlich klingende Phishing-Webseiten.

Kundennutzen: Schutz vor Phishing-Angriffen auf Kunden und Mitarbeiter. Markenschutz durch Früherkennung von Fake-Domains. Verhinderung von CEO-Fraud und Business-E-Mail-Compromise.

Praxisbeispiel: Ein Angreifer registriert 'infinigate-de.com'. APS erkennt die ähnliche Webseite sofort und warnt. Der Partner kann einen Domain-Takedown einleiten, bevor die Webseite für Phishing genutzt wird.

Credential Leak Detection

APS durchsucht Leak-Datenbanken, Darknet-Marktplätze und Hacker-Foren nach kompromittierten Zugangsdaten Ihrer Mitarbeiter. Das Besondere: Die Pre-Leak-Detection findet Credentials teilweise noch BEVOR sie öffentlich verfügbar sind, in geschlossenen Foren und bei Händlern im Darknet.

Kundennutzen: Account-Übernahmen verhindern, bevor sie passieren. Zeitvorsprung vor den Angreifern. Reduktion des Risikos von Ransomware-Angriffen, die häufig mit gestohlenen Credentials beginnen.

Praxisbeispiel: Laut Bitkom 2025 hatten 27 % der deutschen Unternehmen gestohlene Zugangsdaten. Laut Verizon DBIR 2025 beginnen 22 % aller Breaches mit Credential Abuse. APS hätte diese in vielen Fällen früher erkannt.

Dark Web Monitoring

APS überwacht Darknet-Foren, Telegram-Kanäle, Pastebin und andere Quellen auf Erwähnungen Ihres Unternehmens, Ihrer Domains. Das System nutzen zahlreiche Quellen und hat Zugang zu geschlossenen Foren, die automatisierten Tools verschlossen bleiben.

Kundennutzen: Erfahren, wenn Ransomware-Gruppen über Ihr Unternehmen diskutieren oder Daten zum Verkauf angeboten werden, bevor der Angriff stattfindet. Frühzeitige Warnung bei geplanten Angriffen.

Praxisbeispiel: Eine Ransomware-Gruppe diskutiert in einem Darknet-Forum über einen geplanten Angriff auf ein deutsches Klinikum. APS erkennt die Diskussion und warnt, der Angriff kann verhindert werden. Vergleichbares Szenario: Klinikum Ingolstadt (Dez 2024).

Metadaten-Analyse

APS scannt öffentlich zugängliche Dokumente Ihres Unternehmens (PDFs, Office-Dokumente, Bilder) auf sensible Metadaten wie Benutzernamen und Softwareversionen. Laut BSI hatten 47 % der .de-Domains sensible Informationen öffentlich einsehbar.

Kundennutzen: Angriffsoberfläche reduzieren, indem versteckte Informationen in öffentlichen Dokumenten identifiziert und bereinigt werden. Verhinderung gezielter Angriffe, die auf diesen Informationen basieren.

Praxisbeispiel: Eine PDF-Stellenausschreibung auf der Unternehmenswebsite enthält in den Metadaten den Benutzernamen des HR-Mitarbeiters (j.mueller@intern.firma.de), wertvolle Informationen für Reconnaissance.

API-Schnittstelle

Die APS API stellt alle Findings und zugehörigen Metadaten programmgesteuert bereit. Abfragen können nach Zeitraum und Relevanz gefiltert und in bestehende Systeme integriert werden; die API unterstützt SIEM, Ticketing und Workflow Anbindungen (z. B. Jira, ServiceNow). Die technische Dokumentation ist unter api.insight.antago.de/docs verfügbar.

Kundennutzen: Automatisierte Prozesse ohne Medienbruch, schnelle SOC Integration und skalierbare Weiterverarbeitung der Findings in vorhandenen Tools (SIEM, Ticketing, Reporting).

Praxisbeispiel: Das SOC ruft kritische APS Findings per API ab, korreliert sie im SIEM und erzeugt automatisch Incidents im Ticketing System (z. B. ServiceNow) inklusive empfohlener nächsten Schritte.

CSV Export

Alle Findings können basierend auf dem gewählten Zeitraum als CSV-Datei exportiert werden. Der Export enthält alle relevanten Details.

Kundennutzen: Nahtlose Integration in eigene Reporting-Workflows und Compliance-Nachweise (NIS2, ISO 27001, DORA). Dokumentationspflicht erfüllen.

Praxisbeispiel: Der CISO exportiert monatlich alle Findings als CSV und integriert sie in den Quartals-Security-Report für den Vorstand. Bei der NIS2-Prüfung dient der Export als Nachweis für die kontinuierliche externe Bedrohungserkennung.

Zeitfilter

Flexible Zeitraumauswahl für alle Findings: 1 Woche, 2 Wochen, 1 Monat, 3 Monate oder ein individueller Zeitraum (Custom). Alle Dashboard-Ansichten und Exporte respektieren den gewählten Zeitfilter.

Kundennutzen: Historische Trends erkennen, Fortschritte messen und gezielt auf bestimmte Zeiträume fokussieren. Ideal für Audits und Compliance-Nachweise.

Praxisbeispiel: Vor dem NIS2-Audit filtert der IT-Leiter auf die letzten 3 Monate und kann lückenlos nachweisen, welche Findings erkannt und bearbeitet wurden. Der Auditor sieht: kontinuierliche Überwachung ist aktiv.

Infotexte

Zu den Findings bietet APS erklärende Infotexte, die ein- und ausgeblendet werden können. Diese erklären den Kontext, die Risikobewertung und empfohlene Gegenmaßnahmen in verständlicher Sprache, ohne Security-Fachsprache.

Kundennutzen: Auch ohne dediziertes Security-Team können Findings verstanden, bewertet und priorisiert werden. Enablement für IT-Generalisten und Geschäftsführung.

Praxisbeispiel: Ein IT-Administrator ohne tiefes Security-Know-how entdeckt ein Finding zu geleakten Credentials und erhält eine verständliche Erklärung: Wie hoch ist das Risiko, was sollte jetzt getan werden. Schritt-für-Schritt.

Feature-Benefit-Tabelle

Die folgende Tabelle zeigt den direkten Zusammenhang zwischen APS-Features und dem konkreten Kundennutzen. Nutzen Sie diese Tabelle im Kundengespräch, um gezielt auf die Bedürfnisse Ihres Gegenübers einzugehen:

Feature	Was es erkennt	Kundennutzen	APS-Paket
Domain Screening	Phishing-Domains, Typosquatting, Lookalike-Domains	Markenschutz, Phishing-Prävention, CEO-Fraud-Abwehr	Alle Pakete
Credential Leak Detection	Kompromittierte Zugangsdaten in Leak-DBs und Darknet	Account-Übernahmen verhindern	Alle Pakete
Pre-Leak Detection	Zugangsdaten VOR Veröffentlichung in geschlossenen Quellen	Zeitvorsprung vor Angreifern	Alle Pakete
Dark Web Monitoring	Diskussionen, Datenangebote, Ransomware-Pläne im Darknet	Geplante Angriffe frühzeitig erkennen	Alle Pakete
Metadaten-Scan	Sensible Infos in öffentlichen Dokumenten (PDFs, Office, Bilder)	Angriffsoberfläche reduzieren	Alle Pakete
Threat Forecasting	Branchentrends, Bedrohungs-Scoring, Priorisierung	Schnelle Reaktion, Fokus auf Kritisches	Alle Pakete
Lieferketten-Monitoring	Kompromittierte Partner und Zulieferer	Supply-Chain-Risiken erkennen (NIS2 Art. 21)	Alle Pakete
Reports	Dashboard	Compliance-Nachweis	Alle Pakete
Proactive Alerts	Neue Findings	Benachrichtigung über kritische Findings innerhalb von 24 Stunden nach Validierung	Premium/Ultimate
Active Response	Blockierungen, Mailfilterregeln	Direkte Schadensbeseitigung, aktive Abwehr	Ultimate
API-Zugriff	SIEM-, Ticketing- und Workflow-Integration	Automatisierte Prozesse, SOC-Integration	Alle Pakete

Die aktuelle Bedrohungslage

Die IT-Sicherheitslage in Deutschland ist so angespannt wie nie zuvor. Die Zahlen für 2025 zeigen eine dramatische Entwicklung, die jedes Unternehmen betrifft, unabhängig von Größe oder Branche. Dieser Abschnitt fasst die wichtigsten Statistiken aus verlässlichen deutschen und internationalen Quellen zusammen.

Schadensbilanz Deutschland 2025

Der Gesamtschaden durch Datendiebstahl, Spionage und Sabotage erreichte 2025 mit 289,2 Milliarden Euro einen neuen Rekord (Vorjahr: 266,6 Mrd.)⁶. Davon entfielen 202,4 Milliarden Euro (70 %) allein auf Cyberattacken. 8 von 10 Unternehmen waren betroffen, 73 % registrierten eine Zunahme der Angriffe. 46 % der Angriffe wurden nach Russland, 46 % nach China zurückverfolgt⁷. Jedes dritte Unternehmen zahlte nach einer Ransomware-Attacke Lösegeld. Bei 27 % wurden Zugangsdaten und Passwörter gestohlen⁸.

BSI Lagebericht 2025

Der BSI Lagebericht 2025 dokumentiert die fortschreitende Verschlechterung der Sicherheitslage:

- 119 neue Schwachstellen pro Tag (+24 % gegenüber Vorjahr; 2024: 96, 2023: 78, 2022: 68)⁹
- 950 Ransomware-Angriffe im Berichtszeitraum Juli 2024 – Juni 2025¹⁰
- 80 % der Ransomware traf KMU (kleine und mittlere Unternehmen)¹¹
- Über 800 neue Phishing-Seiten pro Tag weltweit¹²
- KMU erfüllen nur 56 % der IT-Sicherheits-Basisanforderungen¹³
- 47 % der .de-Domains hatten sensible Informationen öffentlich einsehbar¹⁴
- 80 % der KRITIS-Betreiber haben ein ISMS, aber Defizite bei Angriffserkennung¹⁵

BKA Bundeslagebild Cybercrime 2024

- 131.391 Cybercrime-Fälle in Deutschland registriert, dazu 201.877 Auslandstaten¹⁶
- 2-3 schwere Ransomware-Angriffe pro Tag in Deutschland
- Aufklärungsquote bei Cybercrime nur 32 % (vs. 58 % bei Gesamtkriminalität)
- Deutschland: 4. am häufigsten betroffenes Land weltweit
- Lösegeld global: 800 Mio. USD (Rückgang 35 %, aber 90 % der Geschädigten zahlten KEIN Lösegeld)
- KI als Treiber für Cyberstraftaten 2025, automatisierte Phishing-Kampagnen, Deepfakes, KI-generierte Malware

⁷Verfassungsschutz Wirtschaftsschutz 2025: <https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html>

Bitkom Cyberkriminalität 2025

61 % der Internetnutzenden in Deutschland waren in den letzten 12 Monaten direkt von Cyberkriminalität betroffen¹⁷. 70 % sehen ein hohes Risiko für Deutschland insgesamt. Diese Zahlen verdeutlichen: Cyberkriminalität ist kein Nischenthema mehr, sondern betrifft die breite Bevölkerung und jedes Unternehmen.

Verizon DBIR 2025 – Globale Trends

Der Verizon Data Breach Investigations Report 2025 analysiert über 22.000 Sicherheitsvorfälle weltweit und zeigt klare Muster:

- 22 % aller Breaches: Credential Abuse, gestohlene Zugangsdaten sind der häufigste Angriffsvektor
- 88 % der Web-App-Angriffe nutzten gestohlene Credentials
- 60 % aller Breaches: Human Element, Menschen bleiben das schwächste Glied
- 30 % via Drittanbieter (verdoppelt gegenüber Vorjahr), Supply-Chain-Angriffe boomen
- VPN-Exploits: 8-facher Anstieg gegenüber Vorjahr

ENISA Threat Landscape 2025

- 4.875 Incidents analysiert (Juli 2024 – Juni 2025)¹⁸
- 81,1 % Cybercrime = Ransomware¹⁹
- 27,3 % Web-Threats, 18,2 % OT-Threats²⁰
- 10,6 % Supply-Chain-Risiken²¹
- Lumma Infostealer: meistverbreitete Malware seit Anfang 2025, spezialisiert auf den Diebstahl von Credentials und Session-Tokens

¹⁶BKA Bundeslagebild Cybercrime 2024: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
¹⁷Bitkom Cyberkriminalität 2025: <https://www.bitkom.org/Bitkom/Publikationen/Cyberkriminalitaet-Studienbericht>
¹⁸ENISA Threat Landscape 2025: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

Deutsche Cyberangriffe 2024/2025

Diese realen Fälle zeigen: Kein Unternehmen ist zu groß, zu klein oder zu bekannt, um Opfer eines Cyberangriffs zu werden. Besonders auffällig: Viele Angriffe erfolgten über Drittanbieter und Zulieferer, genau dort, wo APS ansetzt.

Unternehmen	Zeitraum	Details
BER Flughafen	Sept 2025	Ransomware über Collins Aerospace (Zulieferer) — Supply-Chain-Angriff
Vodafone	Juli 2025	Angriff über externen IT-Dienstleister — Drittanbieter-Kompromittierung
Volkswagen	Mai 2025	Stormous/V4 Ransomware-Gruppe — Darknet-Ankündigung vor Angriff
Adidas	Mai 2025	Datenleck über Kundendienstanbieter — Kundendaten betroffen
Vorwerk	Jan/Feb 2025	3,3 Mio. Nutzerdaten im Darknet aufgetaucht
Stadtwerke Schwerte	März 2025	Cyberangriff auf kommunalen KRITIS-Versorger
Klinikum Ingolstadt	Dez 2024	Ransomware-Angriff auf Krankenhaus-IT
TeamViewer	Juni 2024	APT-Angriff auf interne IT (Göppingen)
Schalke 04	Sept 2024	Cyberangriff auf den Fußballverein
CDU	Mai 2024	Cyberangriff auf die Partei-IT



Im Q2 2025 wurden durchschnittlich 1.286 wöchentliche Attacken pro Organisation in Deutschland registriert, ein Anstieg von 22 % gegenüber dem Vorjahr.

Fazit für das Kundengespräch:

Die Bedrohungslage ist real, messbar und betrifft jede Branche. Besonders relevant für APS: 38 % aller Breaches beginnen mit Credentials (22 %) oder Phishing (16 %), genau die Bereiche, die APS abdeckt. Und 30 % der Angriffe kommen über Drittanbieter, APS überwacht auch die Lieferkette.

Typische Angriffskette – Kill Chain

Jeder Cyberangriff folgt einem typischen Muster. Die sogenannte Kill Chain²² beschreibt die Phasen eines Angriffs von der Aufklärung bis zur finalen Aktion. APS setzt bewusst in den Phasen 1 und 2 an – dort, wo Angriffe erkannt und verhindert werden können, BEVOR sie das Netzwerk erreichen.

Präventions-Logik: Wenn ein Angriff in Phase 1 oder 2 erkannt wird, finden Phase 3–6 nicht statt. APS verhindert damit nicht nur einzelne Angriffe, sondern die gesamte Kill Chain. Zusätzlich kann APS, einen bereits durchgeführten Angriff anhand verschiedener Findings, im Nachhinein aufdecken.

Phase	Was passiert	APS-Abdeckung
Phase 1: Aufklärung (Reconnaissance)	Angreifer sammeln Informationen: Domains, E-Mails, öffentliche Dokumente, Metadaten, Organigramme, LinkedIn-Profil	Domain Screening, Metadaten-Analyse, OSINT
Phase 2: Bewaffnung & Vorbereitung	Phishing-Domains registrieren, Credentials kaufen/beschaffen, Exploit-Kits vorbereiten, Zugänge identifizieren	Credential Leak, Pre-Leak Detection, Dark Web Monitoring
Phase 3: Zustellung (Delivery)	Phishing-Mail versenden, kompromittierte Website, Exploit-Kit ausliefern, Watering-Hole-Angriff	Außerhalb APS-Scope (Firewall, E-Mail-Security, Web-Gateway)
Phase 4: Ausnutzung (Exploitation)	Malware wird ausgeführt, initialer Zugang erlangt, Schwachstelle ausgenutzt	Außerhalb APS-Scope (EDR, Endpoint Protection)
Phase 5: Installation & C2	Persistence etablieren, Lateral Movement, Command & Control aufbauen	Außerhalb APS-Scope (SIEM, NDR, XDR)
Phase 6: Aktion (Impact)	Datenexfiltration, Verschlüsselung, Erpressung, Sabotage	Außerhalb APS-Scope (Incident Response, BCM)

Kernaussage für das Kundengespräch:

APS deckt die Phasen 1 und 2 ab — dort, wo 38 % aller Breaches ihren Ursprung haben (22 % Credentials + 16 % Phishing)

Wer hier erkennt, verhindert den gesamten Rest der Kill Chain.

²²MITRE ATT&CK Framework: <https://attack.mitre.org>

APS in der Defense-in-Depth-Strategie

APS ergänzt bestehende Sicherheitsmaßnahmen und schließt die Lücke zwischen interner und externer Sicherheit:

Außen (APS)	Perimeter	Innen
Credential Monitoring Darknet Monitoring Domain Screening Metadaten-Analyse Pre-Leak Detection	Firewall E-Mail-Security Web Application Firewall VPN DDoS-Schutz	EDR/XDR SIEM NDR Patch Management Access Management



NIS2 & Compliance

Seit dem 6. Dezember 2025 ist das NIS2-Umsetzungsgesetz in Deutschland in Kraft²⁵. Es betrifft über 30.000 Unternehmen — eine Verzehnfachung gegenüber den bisherigen ca. 2.000 KRITIS-Betreibern²⁴. Für Partner bedeutet dies: Ein riesiger Markt an Unternehmen, die jetzt handeln müssen.



Wer ist betroffen?

NIS2 betrifft Unternehmen in 18 Sektoren, die bestimmte Schwellenwerte überschreiten:

- **Wesentliche Einrichtungen:** Energie, Transport, Bankwesen, Gesundheit, Wasser, Digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt
- **Wichtige Einrichtungen:** Post, Abfall, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung
- **Schwellenwerte:** Ab 50 Mitarbeitende ODER 10 Mio. Euro Umsatz. Zulieferer von KRITIS-Betreibern unabhängig von der Größe.

Die wichtigsten NIS2-Pflichten

- **Registrierungspflicht** beim BSI innerhalb von 3 Monaten
- **Meldepflicht** für Sicherheitsvorfälle: 24h Erstmeldung, 72h Zwischenmeldung, 1 Monat Abschlussbericht
- **Risikomanagement** inkl. Business Continuity, Lieferkettensicherheit und Angriffserkennung
- **Geschäftsleitung haftet persönlich** für die Umsetzung, Delegation an IT-Leiter reicht NICHT
- **Nachweispflicht** alle 3 Jahre für Betreiber kritischer Anlagen
- **Multi-Faktor-Authentifizierung** verpflichtend
- **Bußgelder:** bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes

Wie APS bei der NIS2-Compliance hilft

NIS2 betrifft Unternehmen in 18 Sektoren, die bestimmte Schwellenwerte überschreiten:

NIS2-Anforderung	APS-Beitrag	APS-Modul
Risikomanagement (Art. 21 Abs. 2a)	Externe Bedrohungserkennung als Teil des Risikomanagements	Dashboard, Threat Forecasting
Bewältigung von Sicherheitsvorfällen	Frühwarnung ermöglicht schnellere Erkennung und Reaktion	Proactive Alerts (Premium/Ultimate), Active Response Service (Ultimate)
Sicherheit der Lieferkette (Art. 21 Abs. 2d)	Überwachung von Zulieferern und Partnern auf Kompromittierung	Lieferketten-Monitoring
Nachweispflicht (alle 3 Jahre)	Dokumentierte Findings als Compliance-Nachweis	CSV Export, Zeitfilter
Cyberhygiene und Schulung	Verständliche Infotexte für Mitarbeiter-Awareness	Infotexte, Dashboard
Kryptografie und Verschlüsselung	Erkennung wenn Credentials trotz Verschlüsselung geleakt werden	Credential Leak, Pre-Leak Detection

Wichtig:

APS ist ein Baustein der NIS2-Compliance, kein Allheilmittel. Es deckt den Bereich externe Bedrohungserkennung ab und ergänzt damit Firewall, EDR, SIEM und organisatorische Maßnahmen. Für Partner ist dies ein starkes Verkaufsargument: APS adressiert eine konkrete NIS2-Anforderung, die die meisten Unternehmen noch nicht erfüllen.

²⁵OpenKRITIS NIS2: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>

Für wen ist APS?

APS adressiert ein breites Spektrum von Unternehmen. Die Gemeinsamkeit: Alle haben eine externe Angriffsfläche, die sie derzeit nicht überwachen. Die folgende Tabelle zeigt die primären Zielgruppen:

Segment	Beispiele	Treiber
KRITIS-Betreiber	Energie, Wasser, Gesundheit, Transport	NIS2-Pflicht, BSI-Meldepflicht, 24h-Monitoring
KRITIS-Zulieferer	Maschinenbau, Automotive, Elektrotechnik	NIS2 über Lieferkette, OEM-Anforderungen
Finanzdienstleister	Banken, Versicherungen, Vermögensverwalter	BaFin, DORA, DSGVO, Markenschutz
E-Commerce	Online-Shops, Marktplätze, SaaS-Anbieter	Fake-Shop-Erkennung, Markenschutz
Öffentliche Einrichtungen	Kommunen, Stadtwerke, Behörden	BSI-Grundschutz, NIS2
KMU > 50 MA	Alle Branchen	NIS2-Schwelle, fehlende Security-Teams

Ideale Verkaufssituationen

APS lässt sich besonders gut in folgenden Situationen positionieren:

- **NIS2-Compliance-Projekte** — APS adressiert die Anforderung ‘externe Bedrohungserkennung’
- **Security Assessments und Pentests** — APS als kontinuierliche Ergänzung zur punktuellen Prüfung
- **SOC-Aufbau oder MSSP-Erweiterung** — APS als Threat-Intelligence-Baustein
- **DORA-Compliance (Finanzsektor)** — Anforderungen an Drittanbieter-Überwachung
- **Nach einem Sicherheitsvorfall** — ‘Nie wieder überrascht werden’ und wissen welche Informationen abhanden gekommen sind.
- **Branchen mit starkem Markenschutz-Bedarf** — E-Commerce, Finanzdienstleister, Consumer Brands

Top 10 Verkaufsargumente

Die folgenden zehn Argumente sind für den direkten Einsatz im Kundengespräch formuliert. Jedes Argument ist endkundenverständlich und kann sofort verwendet werden:

- 1

Frühwarnsystem statt Reaktion

APS erkennt Bedrohungen, BEVOR sie Ihr Netzwerk erreichen. Während Firewalls und EDR reagieren, wenn der Angreifer bereits da ist, warnt APS in Phase 1 und 2 der Kill Chain bei der Aufklärung und Vorbereitung.
- 2

Made in Germany

Datalake in Deutschland, entwickelt mit antago (ISO 27001/9001/27701 zertifiziert, Sitz Bensheim). Keine Datenübertragung in Drittländer. DSGVO-konform. Besonders relevant für regulierte Branchen und öffentliche Auftraggeber.²⁶
- 3

Menschlich validiert – kein Daten-Rauschen

Jedes Finding wird durch erfahrene Analysten geprüft — mit Expertise aus über 4.000 Spionage- und Cyberwar-Projekten. Sie erhalten keine Alert-Flut, sondern priorisierte, validierte Warnungen mit Handlungsempfehlungen.²⁷
- 4

NIS2-Compliance-Baustein

APS adressiert direkt mehrere NIS2-Anforderungen: externe Bedrohungserkennung und Lieferkettensicherheit. Über 30.000 Unternehmen sind betroffen, die Geschäftsleitung haftet persönlich.²⁸
- 5

Ab 250 Euro – weniger als 9 Euro pro Tag

Der durchschnittliche Ransomware-Schaden liegt bei 1,82 Mio. Euro. APS kostet ab 250 Euro pro Monat. Das Verhältnis Kosten zu potenziellem Schaden ist überwältigend. Keine versteckten Kosten, keine Paketlimits.
- 6

Kein Security-Team erforderlich

APS ist ein Managed Service. Verständliche Infotexte, validierte Findings und monatliche Review-Meetings (Premium/Ultimate), auch Unternehmen ohne dediziertes Security-Team können APS effektiv nutzen. Ideal für KMU mit generalistischer IT.

7 Credentials + Phishing = 38 % aller Breaches

Laut Verizon DBIR 2025 beginnen 38 % aller Datenverletzungen mit gestohlenen Zugangsdaten. APS deckt genau diese beiden Angriffsvektoren ab — und verhindert damit den Rest der Kill Chain.

8 Schnelles Onboarding – kein Agent, kein Netzwerkzugang

APS arbeitet vollständig extern. Kein Agent zu installieren, kein Netzwerkzugang nötig. Das Onboarding dauert wenige Tage. Sie benötigen nur die zu überwachenden Domains. Erste Findings innerhalb zwei Wochen.

9 Recurring Revenue für Partner

Monatliche Lizenzgebühren bedeuten planbaren, wiederkehrenden Umsatz. NFR-Lizenzen mit 50 % Dauerrabatt (Advanced) ermöglichen risikofreien Eigenbetrieb. Die eigene Firma als erstes APS-Projekt liefert echte Findings für überzeugende Demos.

10 Bewährte Technologie – 4.000+ Projekte

APS basiert auf der operativen Erfahrung von antago aus über 4.000 Spionage- und Cyberwar-Projekten.

Tipp für das Gespräch:
Wählen Sie 3-4 Argumente, die zum konkreten Kunden passen.

Bei KRITIS-Betreibern:
#4 (NIS2), #1 (Frühwarnsystem), #2 (Made in Germany).

Bei KMU:
#5 (Preis), #6 (kein Security-Team), #3 (validiert).

Pricing & Packaging

APS wird in drei Paketen angeboten, alle mit vollem Feature-Umfang bei Monitoring und Erkennung. Der Unterschied liegt im Active Response Service (ab Premium) und der Reaktionszeit bei kritischen Findings.

Feature	Advanced	Premium	Ultimate
Monatspreis (HEK)	250 €	500 €	800 €
NFR-Preis (not for Resale) (Partner, -50 %)	125 €	-	-
Onboarding	✓	✓	✓
Dashboard-Zugriff	✓	✓	✓
Domain Screening	✓	✓	✓
Credential & Pre-Leak Detection	✓	✓	✓
Dark Web Monitoring	✓	✓	✓
Metainformation Scanning	✓	✓	✓
Triage & Threat Forecasting	✓	✓	✓
Proactive Alerts	-	✓	✓
Service Review Meetings	-	1x/Monat	1x/Monat
API-Zugriff	✓	✓	✓
Active Response Service	-	-	✓

NFR-Lizenzen für Partner (not for Resale)

- 50 % Rabatt dauerhaft auf Advanced Paket (125 Euro pro Monat)
- Bestellung über techservices@infinigate.de
- Partner erhält zusätzliche Zugänge zum Demo-Dashboard.
- Empfehlung: Eigene Firma als erstes APS-Projekt aufsetzen, so entstehen echte Findings für überzeugende Kundendemos

SLA-Details

- Review Meeting: 1x pro Monat (Premium/Ultimate), Besprechung aller Findings, Trend-Analyse, nächste Schritte
- Kritische Findings: Zeitnahe Benachrichtigung per E-Mail, proaktiv innerhalb 24h nach Validierung (Premium/Ultimate)
- API-Zugriff: immer inkludiert, Integration in SIEM, Ticketing und eigene Workflows möglich
- Paketlimits: Keine — alle Pakete gleicher Umfang bei Monitoring und Erkennung

ROI-Berechnung für Kundengespräche

Stellen Sie dem Kunden folgende Rechnung auf:

Position	Betrag
APS Advanced (12 Monate)	z.B. 4.800 Euro/Jahr (Beispielpreis)
APS Premium (12 Monate)	z.B. 9.000 Euro/Jahr (Beispielpreis)
Durchschn. Ransomware-Schaden (Bitkom)	1.820.000 Euro
Bußgeld NIS2-Verstoß (bis zu)	10.000.000 Euro
Produktionsausfall (1 Woche, KMU 300 MA)	ca. 500.000 Euro

Fazit:
APS kostet weniger als 14 Euro pro Tag (Advanced), ein Bruchteil der potenziellen Schäden.

90-Tage Partner-Aktivierungsplan

Der folgende Plan führt Partner systematisch vom NFR-Start bis zum ersten Abschluss in 90 Tagen. Jede Phase hat klare KPIs und konkrete Aktionen.

Phase 1:
Foundation (Tag 1-30)

Ziel: Eigenes Dashboard aufsetzen, Produkt verstehen, Zielkunden identifizieren, Pitch vorbereiten.

- KPI 1: NFR-Lizenz bestellt und Dashboard eingerichtet
- KPI 2: 10 Zielkunden identifiziert (NIS2-pflichtig, KRITIS, KMU > 50 MA)
- KPI 3: Eigenes Dashboard kennengelernt, erste eigene Findings analysiert
- Aktion: Playbook studieren, 30-Sekunden- und 5-Minuten-Pitch üben, erste informelle Gespräche

Phase 2:
Aktivierung (Tag 31-60)

Ziel: Aktiv Gespräche führen, Demos zeigen, erste Interessenten qualifizieren.

- KPI 1: 5 Discovery-Gespräche geführt (Fragebogen aus Partnerassets nutzen)
- KPI 2: 3 Live-Demos gezeigt (eigenes NFR-Dashboard mit echten Findings, wahlweise Demo-Dashboard)
- Aktion: Gesprächsleitfaden und Einwandbehandlung aus diesem Playbook nutzen

Phase 3:
Conversion (Tag 61-90)

Ziel: Angebote erstellen, ersten Abschluss erzielen, Pipeline aufbauen.

- KPI 1: 2 Angebote erstellt und versendet
- KPI 2: 1 Abschluss (erster zahlender Endkunde)
- KPI 3: 3 weitere Pipeline-Opportunities dokumentiert



Aktivierungs-Timeline

Zeitraum	Aktivität	KPI / Meilenstein	Phase
Tag 1-7	NFR-Lizenz bestellen und Dashboard einrichten	NFR bestellt, Dashboard-Zugang aktiv	Akquise
Tag 8-14	10 Zielkunden identifizieren (NIS2, KRITIS, KMU > 50 MA)	Zielkundenliste dokumentiert	Akquise
Tag 8-21	Eigenes Dashboard kennenlernen, erste Findings analysieren	Eigene Findings dokumentiert	Akquise
Tag 15-21	Playbook studieren, 30s- und 5min-Pitch üben	Pitch-Übung absolviert	Akquise
Tag 22-30	Erste informelle Gespräche mit Bestandskunden	Mind. 3 Erstgespräche	Akquise
Tag 31-44	5 Discovery-Gespräche führen (mit Fragebogen)	5 Gespräche dokumentiert	Aktivierung
Tag 45-58	3 Live-Demos zeigen (eigenes NFR-Dashboard)	3 Demos durchgeführt	Aktivierung
Tag 31-60	Domain-Checks für Interessenten durchführen	Mind. 1 Domain-Check	Aktivierung
Tag 61-74	2 Angebote erstellen	2 Angebote versendet	Abschluss
Tag 75-88	Erster Abschluss (zahlender Endkunde)	1 Abschluss	Abschluss
Tag 89-90	Review Meeting mit Infinigate Account Manager	Pipeline-Review abgeschlossen	Abschluss



Praxis-Tipps für jede Phase

Akquise-Phase:

- **NFR sofort bestellen**, nicht warten, bis der erste Kunde fragt. Die eigene Firma als erstes Projekt aufsetzen.
- **Dashboard täglich öffnen**, nur wer das Produkt kennt, kann es überzeugend präsentieren. Eigene Findings analysieren und dokumentieren.
- **Zielkundenliste priorisieren**: NIS2-pflichtige Unternehmen > 50 MA zuerst, dann KRITIS-Zulieferer, dann Finanzdienstleister.
- **Pitch üben**, 30-Sekunden- sowie 5-Minuten-Pitch üben.

Aktivierungs-Phase:

- **Eigenes Dashboard zeigen**, echte Findings Ihrer eigenen Firma sind überzeugender als jede Powerpoint-Präsentation.
- **Discovery-Fragen nutzen**, die 10 Fragen aus dem Partnerassets-Abschnitt öffnen das Gespräch und decken Wissenslücken auf.
- **NIS2-Argument einsetzen**, persönliche Haftung der Geschäftsleitung ist der stärkste Beschleuniger für Kaufentscheidungen.

Abschluss-Phase:

- **Angebot zeitnah senden**, idealerweise innerhalb von 24h nach dem Gespräch. Momentum nicht verlieren.
- **Paket-Empfehlung aussprechen**, statt drei Optionen eine klare Empfehlung geben.
- **Infinigate Account Manager** einbinden, bei Bedarf technische Vertiefung anbieten.

Erfolgsmetriken nach 90 Tagen

Metrik	Zielwert
NFR-Lizenz aktiv	Ja
Zielkunden identifiziert	10+
Discovery-Gespräche	5+
Live-Demos	3+
Angebote erstellt	2+
Abschlüsse	1+
Pipeline-Opportunities	3+

Partnerassets

Dieser Abschnitt enthält sofort einsetzbare Werkzeuge für den Vertriebsalltag: Pitch-Vorlagen, Discovery-Fragen und Einwandbehandlungen.

30-Sekunden Elevator Pitch

Good Design. Wissen Sie, welche Informationen über Ihr Unternehmen im Web verfügbar sind? Der Infinigate Attack Prevention Service ist Ihr Frühwarnsystem: Er erkennt Cyberbedrohungen außerhalb Ihres Netzwerks, geleakte Zugangsdaten, Phishing-Webseiten, Darknet-Diskussionen, bevor Angreifer zuschlagen. Ab 250 Euro im Monat. Made in Germany.”

Tipp: Dieser Pitch funktioniert, weil er mit einer Frage beginnt (erzeugt Neugier), einen konkreten Nutzen nennt (Frühwarnsystem) und mit einem klaren Preis und Qualitätsmerkmal endet (250 Euro, Made in Germany).

5-Minuten Pitch

Der 5-Minuten-Pitch folgt einer bewährten Struktur in 5 Phasen. Üben Sie jede Phase einzeln, bevor Sie den kompletten Pitch vor einem Kunden halten.

Phase 1: Bedrohungslage (60 Sekunden):

“Die Zahlen sind alarmierend: 289 Milliarden Euro Schaden durch Cyberkriminalität in Deutschland . 80 % der Ransomware trifft KMU . Und seit Dezember 2025 haftet die Geschäftsleitung persönlich für IT-Sicherheit, NIS2 ist in Kraft.”

Phase 3: APS vorstellen (90 Sekunden):

“Der Infinigate Attack Prevention Service schließt genau diese Lücke. APS ist ein Frühwarnsystem, das Bedrohungen außerhalb Ihres Netzwerks erkennt, mit einer einzigartigen Kombination aus KI-Analyse, Darknet-Recherche und menschlicher Expertise aus über 4.000 Projekten . Alle Daten werden in Deutschland gespeichert und verarbeitet.”

Phase 2: Die Lücke aufzeigen (60 Sekunden):

“Die meisten Unternehmen haben in Firewalls und EDR investiert, und das ist gut so. Aber diese Tools schützen das Netzwerk von innen. Wer schaut nach außen? Wer sagt Ihnen, dass Ihre Mitarbeiter-Credentials im Darknet verkauft werden? Oder dass eine Phishing-Domain registriert wurde, die Ihrer zum Verwechseln ähnlich sieht?”

Phase 4: Konkretes Beispiel (60 Sekunden):

“Stellen Sie sich vor: Ein Mitarbeiter nutzt sein Firmen-Passwort auch für einen privaten Online-Shop. Dieser Shop wird gehackt. Ohne APS erfahren Sie das nie, bis der Angreifer mit diesen Credentials in Ihr VPN kommt. Mit APS erhalten Sie eine validierte Warnung, bevor der Angreifer zuschlägt. Sie setzen das Passwort zurück, aktivieren MFA, und der Angriff läuft ins Leere.”



9 Discovery-Fragen

Diese Fragen öffnen das Gespräch und decken Wissenslücken beim Kunden auf. Jede Frage zielt auf einen APS-Nutzen ab:

1. “Wissen Sie, ob Zugangsdaten Ihrer Mitarbeiter in Leak-Datenbanken aufgetaucht sind?”
→ [Credential Leak Detection](#)
2. “Wie würden Sie erfahren, wenn jemand eine Phishing-Domain registriert, die Ihrer ähnlich sieht?”
→ [Domain Screening](#)
3. “Was wissen Sie über Diskussionen zu Ihrem Unternehmen im Darknet?”
→ [Dark Web Monitoring](#)
4. “Wie stellen Sie sicher, dass Ihre NIS2-Anforderungen an externe Bedrohungserkennung erfüllt sind?”
→ [NIS2 Compliance](#)
5. “Wann haben Sie zuletzt Ihre öffentlich zugänglichen Dokumente auf sensible Metadaten geprüft?”
→ [Metadaten-Analyse](#)
6. “Wie schnell würden Sie es merken, wenn ein Zulieferer kompromittiert wird?”
→ [Lieferketten-Monitoring](#)
7. “Haben Sie einen Plan für den Fall, dass morgen 500 Ihrer Mitarbeiterdaten im Darknet auftauchen?”
→ [Incident Preparedness](#)
8. “Wie viel Prozent Ihres Security-Budgets investieren Sie in Prävention vs. Reaktion?”
→ [Präventions-Argument](#)
9. “Wer in Ihrem Unternehmen haftet persönlich, wenn NIS2-Pflichten nicht erfüllt werden?”
→ [Persönliche Haftung](#)

Einwandbehandlung

Die häufigsten Einwände und professionelle Antworten für das Kundengespräch:

Einwand	Antwort
“Wir haben bereits eine Firewall und EDR.”	APS schaut nach außen, nicht nach innen. Firewall und EDR schützen Ihr Netzwerk, aber wer sagt Ihnen, dass Ihre Credentials im Darknet verkauft werden oder eine Phishing-Webseite registriert wurde? APS ergänzt Ihre bestehende Infrastruktur um den fehlenden Blick nach außen.
“Das ist zu teuer.”	Ab 250 Euro pro Monat, das sind weniger als 9 Euro pro Tag. Der durchschnittliche Ransomware-Schaden in Deutschland liegt bei 1,82 Mio. Euro. APS ist keine Ausgabe, sondern eine Frühwarnfunktion.
“Wir sind zu klein, uns greift niemand an.”	80 % der Ransomware-Angriffe treffen KMU (BSI 2025). Gerade kleinere Unternehmen haben oft weniger Schutz und sind damit leichtere Ziele. Angreifer nutzen automatisierte Tools, die nicht nach Unternehmensgröße unterscheiden.
“Wir haben kein Security-Team.”	Genau deshalb ist APS als Managed Service konzipiert. Sie erhalten validierte Warnungen und verständliche Handlungsempfehlungen, kein Datenmeer aus unsortierten Alerts. Die Infotexte erklären Findings verständlich.
“Können wir das nicht selbst?”	Darknet-Zugänge, HUMINT-Quellen, Pre-Leak-Detection und die Analyse-Erfahrung aus 4.000+ Projekten, das ist nicht mit internen Bordmitteln abbildbar. APS bringt die Infrastruktur und Expertise mit, die Sie bräuchten.
“Wir haben andere Prioritäten.”	NIS2 ist seit Dezember 2025 in Kraft. Die Geschäftsleitung haftet persönlich. Externe Bedrohungserkennung ist eine NIS2-Pflicht, nicht ein Nice-to-have. Bußgelder bis 10 Mio. Euro.
“Was unterscheidet APS von Threat-Intelligence-Feeds?”	APS ist kein reiner Feed. Feeds überwachen allgemeine Strömungen, APS konkrete Unternehmen. Jedes Finding wird durch Analysten validiert, mit Erfahrung aus über 4.000 Projekten. Der Datalake steht in Deutschland. Sie erhalten Handlungsempfehlungen, nicht nur Rohdaten.
“Wir haben bereits einen Pentest gemacht.”	Ein Pentest hat einen technischen Scope, APS einen “intelligence” Scope. APS ist ein kontinuierliches Monitoring.
“Wie lange dauert das Onboarding?”	Wenige Tage. Sie benötigen lediglich die zu überwachenden Domains. Kein Agent zu installieren, kein Netzwerkzugang nötig. APS arbeitet vollständig extern.

Case-Templates

Die folgenden sechs Cases decken die wichtigsten Branchen und Verkaufssituationen ab. Nutzen Sie diese als Vorlage und Inspiration für Kundengespräche, passen Sie die Details an Ihren konkreten Interessenten an:

Case 1:
Mittelständischer
Maschinenbauer

Branche: Maschinenbau / Automotive-Zulieferer, 400 MA, KRITIS-Zulieferer, Jahresumsatz 120 Mio. Euro

Trigger: NIS2-Projekt: Als Zulieferer eines KRITIS-Unternehmens muss die Firma Lieferketten-Compliance nachweisen. Der OEM-Kunde verlangt einen Nachweis für externe Bedrohungserkennung als Teil der Lieferantenqualifizierung.

APS-Wert: Credential Monitoring + Lieferketten-Überwachung + NIS2-Dokumentation via Executive Reports und CSV Export

Ergebnis: 12 geleakte Credentials gefunden (davon 3 noch aktiv), 2 Phishing-Webseiten entdeckt und vom Netz genommen. NIS2-Nachweis für externe Bedrohungserkennung dokumentiert. OEM-Kunde zufrieden.

Case 2:
Regionalbank

Branche: Finanzdienstleistung, 120.000 Kunden, BaFin-reguliert, 250 MA

Trigger: BaFin-Prüfung steht an, DORA-Compliance erforderlich. Die Bank sucht nach einer Lösung für kontinuierliches Threat Monitoring ihrer Online-Banking-Domain und Mitarbeiter-Credentials.

APS-Wert: Phishing-Domain-Überwachung + Credential Leak Detection + Reports als BaFin/DORA-Nachweis.

Ergebnis: 3 Phishing-Domains identifiziert. 7 Mitarbeiter-Credentials in Leak-Datenbanken gefunden. Quartals-Reports dienen als DORA-Compliance-Nachweis



Case 3:

Klinikverbund

Branche: Gesundheitswesen, 3 Häuser, KRITIS-Betreiber, 1.200 MA

Trigger: BSI-Meldepflicht für KRITIS, zunehmende Darknet-Diskussionen über Angriffe auf deutsche Krankenhäuser (vgl. Klinikum Ingolstadt Dez 2024). Der CISO will proaktiv werden.

APS-Wert: Dark Web Monitoring + Pre-Leak Detection.

Ergebnis: Ransomware-Vorbereitung in einem Darknet-Forum erkannt, eine Gruppe diskutierte gezielt über Zugangsdaten zum RIS/PACS-System. Sofortige Warnung, Passwort-Reset aller betroffenen Accounts, Angriff verhindert.

Case 4:

E-Commerce-Unternehmen

Branche: Online-Handel, 200 Mio. Euro Umsatz, 150 MA, B2C

Trigger: Markenschutz-Problem: Kunden beschwerten sich über Fake-Shops, die den echten Shop imitieren. DSGVO-Compliance für Kundendaten erforderlich. Reputationsschaden durch Fake-Produkte.

APS-Wert: Domain Screening + Metadaten-Scan + Credential Monitoring.

Ergebnis: 7 Fake-Shops identifiziert und per Takedown vom Netz genommen. Metadaten in 23 Produktkatalogen (PDFs) bereinigt, enthielten Mitarbeiterdaten. Kundenbeschwerden über Fake-Shops um 80 % reduziert.

Case 5:

Stadtwerke (Energieversorger)

Branche: Energieversorgung, KRITIS, 600 MA, kommunaler Versorger

Trigger: NIS2 + BSI-Meldepflicht + OT-Sicherheit. Der CISO benötigt eine Lösung, die auch OT-relevante Bedrohungen im Darknet erkennt. Stadtwerke Schwerte (März 2025) als warnendes Beispiel.

APS-Wert: Lieferketten-Monitoring für OT-Zulieferer

Ergebnis: Credentials des SCADA-Administrators im Darknet entdeckt, sofortige Sperrung, Passwort-Reset, Zugangsaudit. Zusätzlich: 2 OT-Zulieferer mit kompromittierten Systemen identifiziert und informiert.

Case 6:

IT-Systemhaus (MSP/MSSP)

Branche: IT-Dienstleistung, 50 MA, 200 Endkunden, MSSP-Ambitionen

Trigger: Erweiterung des MSSP-Portfolios um ein differenzierendes Security-Angebot. Wunsch nach Recurring Revenue und stärkerer Kundenbindung. Wettbewerber bieten bereits Threat Intelligence an.

APS-Wert: NFR-Eigenbetrieb als Showcase + Resale an Endkunden + White-Label-fähige Executive Reports

Ergebnis: 5 Endkunden in 3 Monaten gewonnen (3x Advanced, 1x Premium). Monatlicher Recurring Revenue von min. 1.250 Euro aufgebaut. Eigene Firma als lebende Demo, echte Findings überzeugen Interessenten.

FAQ – Häufig gestellte Fragen

Die folgenden Fragen und Antworten können Sie direkt im Kundengespräch nutzen:

1. Was genau ist APS?

APS steht für Attack Prevention Service. Es ist ein Managed-Security-Service von Infinigate, der Cyberbedrohungen außerhalb Ihres Netzwerks erkennt, im Darknet, in Leak-Datenbanken, bei Domain-Registrierungen. APS ist Ihr Frühwarnsystem, entwickelt in Kooperation mit antago (ISO 27001/9001/27701 zertifiziert), mit einem Datalake in Deutschland. Die Lösung vereint KI-gestützte Analyse mit menschlicher Expertise aus über 4.000 Projekten.

2. Wie unterscheidet sich APS von einer Firewall oder EDR?

Firewall und EDR schützen Ihr Netzwerk von innen. APS schaut nach außen: Welche Ihrer Credentials sind geleakt? Gibt es Phishing-Domains? Wird Ihr Unternehmen im Darknet diskutiert? APS ergänzt Ihre bestehende Infrastruktur um die entscheidende externe Perspektive. Zusammen bilden Firewall, EDR und APS eine lückenlose Defense-in-Depth-Strategie.

3. Wer betreibt APS?

APS wird von Infinigate Deutschland GmbH in Kooperation mit antago (Bensheim) betrieben. antago bringt über 10 Jahre Erfahrung in Penetration Testing, IT-Forensik, Incident Response und Dark Web Monitoring mit, aus mehr als 4.000 Spionage- und Cyberwar-Projekten. Das Dashboard läuft unter insight.antago.de, der Datalake steht in Deutschland.

4. Wo werden die Daten gespeichert?

Alle Daten werden in einem dedizierten Datalake in Deutschland gespeichert und verarbeitet. Es gibt keine Datenübertragung in Drittländer. Dies ist besonders relevant für DSGVO-, NIS2- und DORA-Compliance.

5. Wie schnell bekomme ich Ergebnisse nach dem Onboarding?

Das Onboarding dauert wenige Tage. Sie benötigen lediglich die zu überwachenden Domains. Erste Finding, insbesondere Credential Leaks und Domain-Screenings, liegen in der Regel innerhalb der ersten Woche vor. Darknet-Monitoring liefert kontinuierlich neue Ergebnisse. Kein Agent zu installieren, kein Netzwerkzugang nötig.

6. Brauche ich ein eigenes Security-Team?

Nein. APS ist als Managed Service konzipiert. Alle Findings werden durch Analysten validiert und mit verständlichen Handlungsempfehlungen versehen. Die Infotexte im Dashboard erklären jedes Finding auch für Nicht-Experten. Monatliche Review-Meetings (ab Premium Lizenz) mit dem APS-Team stellen sicher, dass keine Findings übersehen werden.

7. Hilft APS bei NIS2-Compliance?

Ja. APS adressiert mehrere NIS2-Anforderungen: externe Bedrohungserkennung (Risikomanagement Art. 21), Lieferketten-Sicherheit (Art. 21 Abs. 2d), Meldepflicht-Unterstützung, und dokumentierte Executive Reports als Compliance-Nachweis. APS ist ein wichtiger Baustein der NIS2-Umsetzung, in Kombination mit Firewall, EDR und organisatorischen Maßnahmen.

8. Gibt es eine API?

Ja. Ein API-Zugriff ist immer inkludiert, bei allen drei Paketen. Sie können APS-Findings in Ihr SIEM, Ticketing-System (z.B. Jira, ServiceNow) oder eigene Workflows integrieren. Die API-Dokumentation finden Sie unter: <https://api.insight.antago.de/docs>

9. Was passiert bei einem kritischen Finding?

Bei allen Paketen stellen wir in einem Dashboard alle Findings zur Verfügung. Bei den Paketen Premium und Ultimate erfolgt die Benachrichtigung proaktiv innerhalb von 24 Stunden nach Validierung durch das Analysten-Team. Zusätzlich stehen bei dem Paket Ultimate, Active-Response-Maßnahmen zur Verfügung wie Blockierungen und Mailfilterregeln.

10. Wie starte ich als Partner?

Drei einfache Schritte: (1) Bestellen Sie Ihre NFR-Advanced-Lizenz (50 % Dauerrabatt) über techservices@infinigate.de. (2) Richten Sie Ihre eigene Firma als erstes APS-Projekt ein, so haben Sie echte Findings für Demos. (3) Nutzen Sie den 90-Tage-Aktivierungsplan in diesem Playbook und starten Sie mit dem 30-Sekunden-Pitch bei Ihren ersten 10 Zielkunden.



Kontakt & Nächste Schritte

Sie haben das Playbook gelesen und sind bereit, mit APS zu starten? Die folgenden Schritte führen Sie vom Playbook zum ersten Kunden:

Für Partner: So starten Sie sofort

- 1. **NFR-Lizenz bestellen:** Kontaktieren Sie techservices@infinigate.de oder Ihren Infinigate Ansprechpartner und bestellen Sie Ihre NFR-Advanced-Lizenz (50 % Dauerrabatt).
- 2. **Eigene Firma aufsetzen:** Richten Sie Ihre eigene Firma als erstes APS-Projekt ein. Geben Sie ihre Domain an. Innerhalb einer Woche haben Sie erste Findings.
- 3. **Dashboard kennenlernen:** Öffnen Sie das Dashboard täglich. Analysieren Sie Ihre eigenen Findings.
- 4. **10 Zielkunden identifizieren:** Nutzen Sie die Zielkunden-Tabelle aus diesem Playbook. Priorisieren Sie NIS2-pflichtige Unternehmen, KRITIS-Zulieferer und Bestandskunden mit Security-Bedarf.
- 5. **Erste Gespräche führen:** Nutzen Sie den 30-Sekunden-Pitch als Gesprächseinstieg und die Discovery-Fragen, um den Bedarf zu ermitteln.
- 6. **90-Tage-Plan befolgen:** Halten Sie sich an die KPIs und Meilensteine. Nach 90 Tagen haben Sie Ihren ersten zahlenden Kunden und eine gefüllte Pipeline.

Kontaktinformationen

Thema	Kontakt
NFR-Bestellung	Ihr Infinigate Account Manager oder direkt unter techservices@infinigate.de
APS Produktseite	https://www.infinigate.com/de/services/aps/
Technische Fragen	Infinigate APS Team unter support@infinigate.de
Vertriebsunterstützung	Gemeinsame Produktvorstellungen unter techservices@infinigate.de
Dashboard	insight.antago.de (nach Onboarding)



Starten Sie jetzt! Ihre Kunden werden nicht warten. NIS2 ist in Kraft, die Bedrohungslage eskaliert, und 30.000+ Unternehmen suchen nach Lösungen. Mit APS haben Sie die Antwort.

Quellenliste

Alle in diesem Playbook verwendeten Statistiken stammen aus den folgenden öffentlich verfügbaren Quellen:

1. BSI Lagebericht 2025:

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

2. Bitkom Wirtschaftsschutz 2025: <https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz>

3. Bitkom Cyberkriminalität 2025:

<https://www.bitkom.org/Bitkom/Publikationen/Cyberkriminalitaet-Studienbericht>

4. BKA Bundeslagebild Cybercrime 2024:

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html

5. IHK München NIS2: <https://www.ihk-muenchen.de/ratgeber/digitalisierung/informationssicherheit/nis-2-kritis/>

6. BSI NIS2-regulierte Unternehmen:

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

7. OpenKRITIS NIS2-Umsetzung:

<https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>

8. Infinigate APS Produktseite: <https://www.infinigate.com/de/services/aps/>

9. Infinigate it-sa 2025:

<https://www.infinigate.com/news/infinigate-at-it-sa-2025-strong-focus-on-ot-security-new-services-and-partner-enablement/>

10. Verizon DBIR 2025: <https://www.verizon.com/business/resources/reports/dbir/>

11. ENISA Threat Landscape 2025: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

12. MITRE ATT&CK Framework: <https://attack.mitre.org>

13. Verfassungsschutz Wirtschaftsschutz 2025:

<https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html>

Über die Infinigate Group

Die Infinigate Group, die führende Technologieplattform und der Trusted Advisor in den Bereichen Cybersecurity, Cloud und Netzwerkinfrastruktur, ist in über 100 Ländern in der EMEA-Region, Australien und Neuseeland vertreten. Im Geschäftsjahr 2023-2024 erreichte die Gruppe einen Umsatz von 2,3 Mrd. Euro. Der Fokus und das tiefe technische Know-how in den Bereichen Cybersicherheit, sichere Netzwerke und sichere Cloud für KMUs und Unternehmen zeichnen Infinigate aus. 1.250 Mitarbeiter bieten lokal zugeschnittene Dienstleistungen an, die eine robuste zentrale Lieferkette ergänzen und das Wachstum der Partner, MSSPs und Hersteller unterstützen.



Visit:
infinigate.de/techservices

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

+49 89 89048 403
techservices@infinigate.de
www.infinigate.com/de

