

Infinigate Security Awareness Service

Reseller Sales Playbook

powered by



Executive Summary	4	Top 10 Verkaufsargumente	16
Kennzahlen auf einen Blick	4	Ergänzende Leistungsbausteine	18
Das Angebot: Eine Lizenz, zwei Modelle	5	90-Tage Partner-Aktivierungsplan	19
Die Modellfrage: In zwei Fragen zur Empfehlung	5	Phase 1: Foundation (Tag 1-30)	19
Der Upsell-Pfad nach dem Abschluss	5	Phase 2: Aktivierung (Tag 31-60).....	19
Vom Erstgespräch zum Abschluss	6	Phase 3: Conversion (Tag 61-90).....	19
Kundenstory: Der Klick, der nicht passierte	7	Erfolgsmetriken nach 90 Tagen	19
Das Unternehmen.....	7	Partnerassets	20
Der Trigger: DSGVO-Prüfung eines Mandanten	7	30-Sekunden Elevator Pitch	20
Der Start: Schulung zuerst	7	Positionierung: Souveränität statt Angst	20
Die erste Simulation	8	5-Minuten Pitch	21
Szenario ohne Security Awareness.....	8	12 Discovery-Fragen	22
Szenario mit Security Awareness	8	Einwandbehandlung	23
Das Ergebnis	8	Case-Templates	24
Featuretexte: kundensprachlich	9	Case 1: Mittelständischer Industriebetrieb (150 Mitarbeitende)	24
Multi-Channel Phishing-Simulation.....	9	Case 2: Regionalbank (280 Mitarbeitende, DORA-Pflicht)	24
Trainingsbibliothek mit über 7.000 Inhalten	9	Case 3: IT-Systemhaus als MSP (200 Endkunden).....	24
KI-adaptive Lernpfade	9	Case 4: Klinikverbund (5 Häuser, 800 Mitarbeitende)	24
Phishing Reporter	10	Case 5: Steuerberatungskanzlei (85 Mitarbeitende).....	25
Human Risk Dashboard.....	10	Case 6: Stadtwerke (KRITIS, 600 Mitarbeitende)	25
Compliance Reporting und Audit-Trails	10	12 Mottos für Security Awareness	26
Live-Trainings und Workshops (kostenpflichtige Zusatzbausteine)	11	Top-3 Begründung	26
Feature-Benefit-Tabelle	12	FAQ: Häufig gestellte Fragen	28
Die aktuelle Bedrohungslage	13	Kontakt & Nächste Schritte	29
Schadensbilanz Deutschland 2025	13	Für Partner: So starten Sie sofort	29
Der menschliche Faktor in den Zahlen.....	13	Kontaktinformationen.....	29
Neue Angriffsvektoren 2026.....	13	Quellen	30
NIS2 & Compliance	14		
Wer ist betroffen?	14		
Die wichtigsten NIS2-Anforderungen für Awareness	14		
Wie der Service bei der NIS2-Compliance hilft	14		
Für wen ist der Service?	15		
Ideale Zielgruppe	15		
Ideale Verkaufssituationen	15		

Executive Summary

Im Zentrum dieses Playbooks steht die Lizenz der Infinigate Awareness Plattform: ein Abonnement pro User, erhältlich in zwei Modellen. Self-Serviced für Kunden, die selbst steuern möchten, und Managed für Kunden, bei denen Infinigate den kompletten Betrieb übernimmt. Für Sie als Partner entsteht daraus wiederkehrender Umsatz und eine langfristige Kundenbindung.

Dieser Service macht die Mitarbeitenden Ihrer Kunden zur stärksten Verteidigungslinie des Unternehmens. Das Prinzip: Kompetenz statt Kontrolle. Mitarbeitende lernen zuerst in kompakten Einheiten, danach folgen realistische Simulationen. Sie erkennen Angriffe automatisch und arbeiten souveräner und freier. Margenstarke Live-Trainings und Workshops der zertifizierten Security Awareness Koordinatoren sind kostenpflichtig zubuchbar und eignen sich als Erweiterung nach dem Lizenzabschluss.

Warum jetzt? Die Bedrohungslage in Deutschland hat 2025 einen neuen Höchststand erreicht. Der Gesamtschaden durch Cyberkriminalität beträgt 289,2 Milliarden Euro, und 60 % aller Sicherheitsvorfälle haben eine menschliche Komponente. Seit Dezember 2025 ist das NIS2-Umsetzungsgesetz in Kraft: Über 30.000 Unternehmen müssen nachweisbare Awareness-Maßnahmen umsetzen, die Geschäftsleitung haftet persönlich.

Was Partner davon haben: Das Abonnementmodell liefert planbaren Recurring Revenue mit rund 35 % Gesamtmarge bei kurzem Abschlusszyklus, und die Zielgruppe ist breit: Praktisch jedes Unternehmen mit E-Mail-Arbeitsplätzen kommt infrage. Nach dem Abschluss lässt sich jedes Konto über Managed Customization, Premium Content und Live-Elemente weiter ausbauen. Das Infinigate TechServices Team unterstützt im Presales und Co-Selling.

Kernzahlen auf einen Blick

2 Modelle
Lizenz mit oder ohne Management

60 %
der Vorfälle mit menschlicher Komponente

24-48 h
bis die Plattform beim Kunden läuft

ca. 35 %
Gesamtmarge für Partner

289 Mrd. €
Schaden durch Cybercrime in DE (2025)

30.000+
NIS2-pflichtige Unternehmen in DE

7.000+
Trainingsinhalte in der Lizenz enthalten

90 Tage
bis zu messbaren Ergebnissen

Das Angebot: Eine Lizenz, zwei Modelle

Grundlage des Angebots ist eine Lizenz pro User im Abonnement der Infinigate Awareness Plattform. In der Lizenz enthalten sind alle Plattform-Features: die Trainingsbibliothek mit über 7.000 Inhalten, Multi-Channel-Simulationen, KI-adaptive Lernpfade, Phishing Reporter, Human Risk Dashboard und Compliance Reporting. Die Staffelnung erfolgt nach Useranzahl, je größer der Kunde, desto attraktiver der Preis pro User. Die einzige Entscheidung, die der Kunde treffen muss: mit oder ohne Management.

Self-Serviced (ohne Management)	Managed (mit Management durch Infinigate)
Kunde verwaltet die Plattform selbst	Infinigate übernimmt den vollständigen Betrieb
Bereitstellung des Tenants durch Infinigate	Bereitstellung plus Kickoff-Meeting durch Infinigate
Nutzerverwaltung und Kampagnen durch den Kunden	Nutzerverwaltung und monatliche Kampagnen durch Infinigate
Standard-Reporting	Monatliches Reporting durch Infinigate
Für Kunden mit eigener IT und eigenem Anspruch an Steuerung	Für alle anderen: der Standardfall im Mittelstand

Die Modellfrage: In zwei Fragen zur Empfehlung

1.

“Haben Sie ein Team, das Kampagnen und Nutzerverwaltung dauerhaft selbst betreiben will?”
Wenn ja: Self-Serviced, idealerweise mit Onboarding Workshop.
2.

“Oder soll das Programm einfach laufen, ohne dass sich bei Ihnen jemand kümmern muss?”
Dann Managed, der Standardfall für die meisten Kunden.

Faustregel für das Gespräch:
Ob ein Awareness-Programm sinnvoll ist, beantworten Bedrohungslage und NIS2 meist von selbst. Die eigentlich spannende Frage ist die nach dem passenden Modell. Ist der Kunde unsicher, passt in den meisten Fällen Managed: der größte Nutzen ohne eigenen Betriebsaufwand, mit einer engen laufenden Zusammenarbeit.

Der Upsell-Pfad nach dem Abschluss

Mit der Lizenz beginnt die Kundenbeziehung erst. Stockt beim Self-Serviced-Kunden die interne Betreuung, ist der Wechsel zu Managed der natürliche nächste Schritt. Managed-Kunden erweitern ihr Programm über die Customization-Option um individuelle Kampagnen und monatliche Reviews. Premium Content bringt exklusive Videoinhalte mit hohem Wiedererkennungswert auf die Plattform. Wer sein Team persönlich weiterentwickeln möchte, bucht die kostenpflichtigen Live-Elemente dazu, vom Workshop bis zum Vertiefungsmodul.

Vom Erstgespräch zum Abschluss

Der Weg zum Abschluss ist kurz, wenn die Grundlagen stimmen. Die Plattform ist in 24 bis 48 Stunden einsatzbereit, und die nötigen Eckdaten für ein Angebot sind schnell erhoben. Fünf Schritte haben sich bewährt:

Schritt 1:

Zielkunden aus dem Bestand ziehen

Fast jeder Kunde mit E-Mail-Arbeitsplätzen kommt infrage. Erstellen Sie eine Liste Ihrer Top-Bestandskunden mit geschätzter Useranzahl. Priorisieren Sie Kunden mit NIS2-Bezug und Kunden, bei denen Sie bereits Firewall oder EDR betreiben.

Schritt 2:

Das Gespräch eröffnen

Nutzen Sie den 30-Sekunden-Pitch aus den Partnerassets. Klären Sie im Gespräch nebenbei zwei Dinge: die ungefähre Anzahl der Mitarbeitenden mit Postfach und die Frage, ob ein eigenes Team den Betrieb übernehmen würde.

Schritt 3:

Demo zeigen, Angebot anfordern

Eine kurze Dashboard-Demo (TechServices unterstützt auf Wunsch) plus die Useranzahl reichen für ein konkretes Angebot: Anfrage an techservices@infinigate.de, Modell und Useranzahl nennen, Angebot kommt kundenindividuell.

Schritt 4:

Ohne Umwege starten

Lange Pilotphasen sind selten nötig. Die Einstiegshürde ist niedrig, im Managed-Modell gehört der Kickoff dazu, und die ersten 90 Tage liefern ohnehin belastbare Ergebnisse.

Schritt 5:

Abschließen und Upsell-Termin setzen

Nach dem Abschluss direkt den Review-Termin nach 90 Tagen vereinbaren. Dort präsentieren Sie die Ergebnisse und platzieren Customization, Premium Content oder Live-Elemente.

Bewährter Gesprächsabschluss

“Wenn Sie mögen, rechne ich Ihnen beide Modelle für Ihre Unternehmensgröße durch.”

Kundenstory: Der Klick, der nicht passierte

Die folgende Geschichte ist fiktiv, basiert aber auf typischen Abläufen aus Awareness-Projekten. Sie zeigt, wie der Service in der Praxis funktioniert und welchen konkreten Wert er für mittelständische Unternehmen bietet.

Das Unternehmen

Firma: Bauer & Söhne Steuerberatung GmbH (fiktiv), mittelständische Steuerberatungskanzlei mit vier Standorten in Bayern. 85 Mitarbeitende. Mandanten: über 200 kleine und mittlere Unternehmen. IT: zwei Personen unter IT-Leiter Markus Huber.

Markus ist stolz auf seine IT-Infrastruktur, vom E-Mail-Filter bis zum Backup-Konzept. Einen blinden Fleck hat er trotzdem: Wie seine Kolleginnen und Kollegen auf einen professionell gemachten Phishing-Angriff reagieren würden, weiß er schlicht nicht. Geschult wurde nie.

Der Trigger: DSGVO-Prüfung eines Mandaten

Im März 2026 kündigt ein großer Mandant eine erweiterte Datenschutz-Due-Diligence an. Der externe Prüfer stellt fest: Es gibt keine nachweisbaren Maßnahmen zur Mitarbeitersensibilisierung, und dokumentiert ist entsprechend nichts. Der betreuende Infinigate-Partner empfiehlt die Security Awareness Services.

Der Start: Schulung zuerst

Das Programm beginnt bewusst mit Wissen. Alle Mitarbeitenden absolvieren kompakte Lerneinheiten von 5 bis 10 Minuten: Wie erkenne ich eine gefälschte E-Mail? Was mache ich mit einer verdächtigen Nachricht? Erst danach folgt die erste Simulation, und niemand geht unvorbereitet hinein. Diese Reihenfolge schafft Akzeptanz und vermeidet Frust.

Die erste Simulation

Nach der Grundschulung folgt die erste Phishing-Simulation. 31 % der Mitarbeitenden klicken auf den simulierten Link, und nur 3 von 85 melden die verdächtige E-Mail. Die Auswertung erfolgt wertfrei und ohne namentliche Bloßstellung. Ein typischer Ausgangswert: Das Wissen ist noch frisch, der geschulte Blick wird erst durch Übung zur Routine.

Szenario ohne Security Awareness

Ein gezielter Spear-Phishing-Angriff auf einen Steuerberater führt zu kompromittierten Mandantendaten. Nach DSGVO drohen Bußgelder von bis zu 4 % des Jahresumsatzes. Der Reputationsschaden gegenüber den Mandanten wiegt mindestens ebenso schwer. Der durchschnittliche Schaden eines Datenschutzvorfalls im Mittelstand liegt im siebenstelligen Bereich.

Szenario mit Security Awareness

Nach 90 Tagen mit monatlichen Lerneinheiten und zwei weiteren Simulationen zeigt sich ein deutliches Bild. Die Klickrate sinkt von 31 % auf 8 %, und 47 Mitarbeitende melden die verdächtige Mail aktiv über den Phishing Reporter. Die Compliance-Dokumentation liegt automatisch vor. Markus legt dem Prüfer lückenlose Nachweise vor und besteht das Audit.

Das Ergebnis

“Unsere Leute sind heute spürbar souveräner. Sie erkennen die Signale und wissen genau, was zu tun ist. Viele sagen mir: Das hilft mir auch privat.” (Markus Huber, IT-Leiter, fiktiv)



Featuretexte – kundensprachlich

Die folgenden Beschreibungen sind für den direkten Einsatz im Kundengespräch formuliert. Wichtig für Ihre Argumentation: Alle Plattform-Features sind Bestandteil der Lizenz. Nur die Live-Formate und der Premium Content am Ende des Kapitels sind kostenpflichtige Zusatzbausteine.

Multi-Channel Phishing-Simulation

Die Plattform simuliert Angriffe über alle Kanäle, die echte Angreifer nutzen: E-Mail-Phishing, SMS (Smishing), Telefonanrufe mit KI-Stimmen (Vishing), QR-Codes (Quishing), MFA-Fatigue und Callback-Phishing. Jede Simulation findet in sicherer Umgebung statt, ohne echte Konsequenzen.

Kundennutzen: Mitarbeitende üben an realistischen Szenarien und entwickeln Erkennungsroutine über alle Angriffswege. Wer auf eine Simulation reagiert, erhält sofort eine kurze Lerneinheit, ohne Bloßstellung.

Praxisbeispiel: Ein Maschinenbauer startet nach der Grundschulung die erste Simulationswelle mit 200 Mitarbeitenden. Das Dashboard zeigt binnen 48 Stunden, welche Themen bereits sitzen und wo Vertiefung sinnvoll ist.

Trainingsbibliothek mit über 7.000 Inhalten

Die Plattform stellt über 7.000 Trainingsmaterialien von 11 internationalen Content-Providern bereit: Videos, interaktive Module, Quizze und Infografiken in über 30 Sprachen. Die Lerneinheiten dauern 5 bis 10 Minuten pro Monat.

Kundennutzen: Mitarbeitende lernen im eigenen Tempo, ohne Ganztagesseminare und ohne Produktionsausfall. Alle Lernfortschritte werden automatisch für Compliance-Nachweise dokumentiert.

Praxisbeispiel: Eine Regionalbank integriert die Pflichtmodule zu Phishing und Datenschutz in ihr Onboarding. Neue Mitarbeitende starten vom ersten Tag an mit dem nötigen Wissen.

KI-adaptive Lernpfade

Die Plattform passt Schulungsinhalte automatisch an den individuellen Wissensstand an. Wer bei einem Thema unsicher ist, erhält gezielt vertiefende Module. Wer sicher ist, wird nicht mit Bekanntem aufgehalten.

Kundennutzen: Jeder lernt genau das, was für ihn relevant ist. Das Programm fügt sich in den Arbeitsalltag ein und wird als Bereicherung wahrgenommen. Diese Wertschätzung ist ein zentraler Faktor für die Akzeptanz.

Praxisbeispiel: Ein Vertriebsmitarbeiter, der QR-Code-Phishing noch nicht kennt, erhält automatisch ein kurzes Modul genau dazu. Seine Kollegin, die das Thema beherrscht, sieht es gar nicht erst.

Phishing Reporter

Mit einem Klick melden Mitarbeitende verdächtige E-Mails direkt aus Outlook oder Google Workspace an die IT. Die Plattform analysiert die Meldung automatisch und gibt Rückmeldung.

Kundennutzen: Aus passiven Empfängern werden aktive Mitgestalter der Unternehmenssicherheit. Die IT erhält strukturierte Meldungen statt unkoordinierter Anrufe, und Mitarbeitende erleben, dass ihre Wachsamkeit zählt.

Praxisbeispiel: Eine Mitarbeiterin erkennt eine verdächtige Rechnung im Posteingang, meldet sie mit einem Klick und arbeitet weiter. Die IT blockiert den Absender unternehmensweit, bevor weitere Kollegen die Mail öffnen.

Human Risk Dashboard

Das zentrale Dashboard zeigt den Awareness-Stand des gesamten Unternehmens auf einen Blick: Erkennungsraten, Meldequoten, Entwicklung pro Abteilung, Compliance-Status.

Kundennutzen: Geschäftsleitung und IT sehen jederzeit, wie sich die Sicherheitskompetenz entwickelt. Die ideale Grundlage für Management-Reporting und NIS2-Nachweise.

Praxisbeispiel: Der IT-Leiter präsentiert der Geschäftsführung quartalsweise die Entwicklung: Klickraten sinken, Meldequoten steigen. Der Wert des Programms wird sichtbar, ohne dass eine einzelne Person bewertet wird.

Compliance Reporting und Audit-Trails

Die Plattform erstellt automatische Compliance-Reports für NIS2, DSGVO, ISO 27001 und DORA. Lückenlose Audit-Trails dokumentieren alle Schulungen und Simulationen.

Kundennutzen: Auditoren erhalten alle Nachweise auf Knopfdruck. Das Risiko von Beanstandungen wegen fehlender Dokumentation entfällt.

Praxisbeispiel: Vor dem NIS2-Audit exportiert der Compliance-Beauftragte den vollständigen Schulungsnachweis für alle 300 Mitarbeitenden. Aufwand: wenige Minuten.

Live-Trainings und Workshops (kostenpflichtige Zusatzbausteine)

Ergänzend zur Plattform bieten die zertifizierten Infinigate Security-Awareness-Koordinatoren Live-Formate an: halbtägige Workshops für Management und IT, Grundlagentrainings, Vertiefungsmodule mit Live-Demos (Phishing, Passwörter knacken, Social Engineering) sowie eine offene Sprechstunde. Diese Bausteine sind optional zubuchbar und werden separat berechnet.

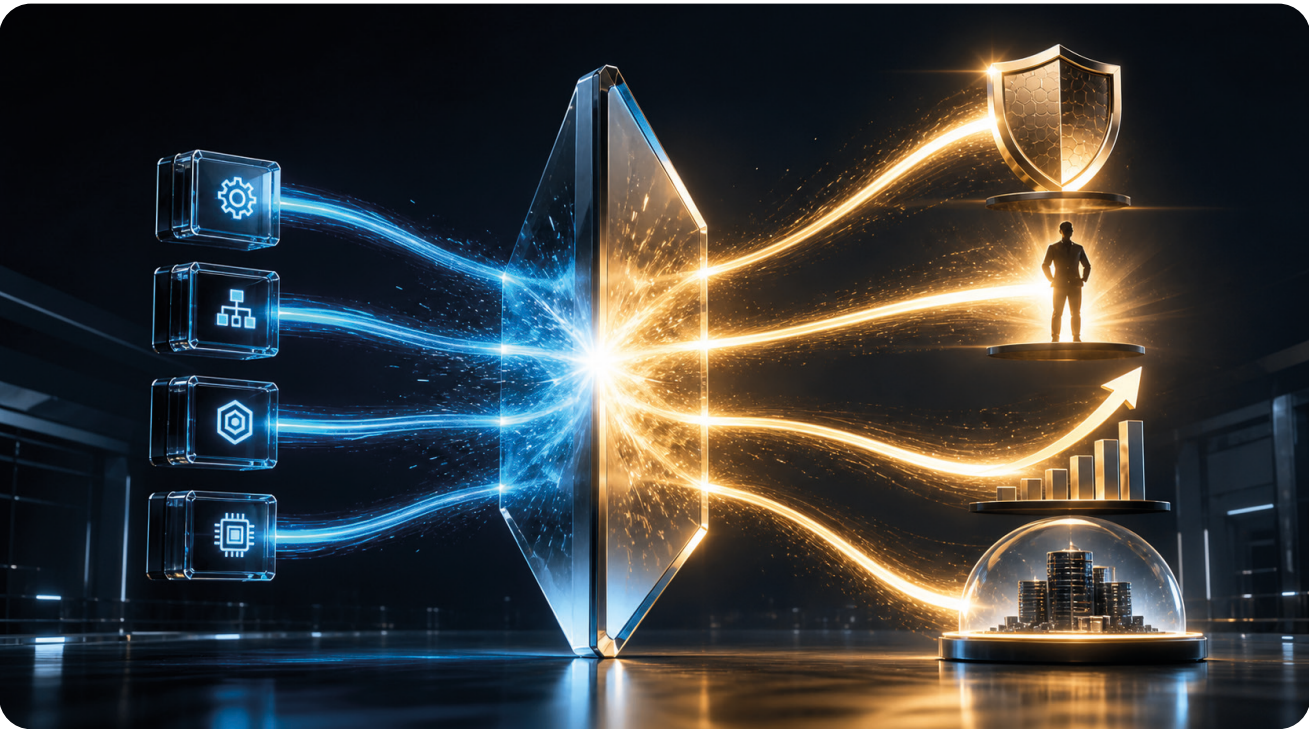
Kundennutzen: Der persönliche Kontakt mit echten Experten verankert das Wissen tiefer als jedes Video. Live-Demos erzeugen Aha-Momente, die im Gedächtnis bleiben.

Praxisbeispiel: Im Vertiefungsmodul Identitäten & Passwörter zeigt der Trainer in einer Live-Demonstration, wie schnell sich unsichere Passwörter knacken lassen. Danach diskutiert niemand mehr über den Sinn von Passwort-Managern und MFA.



Feature-Benefit-Tabelle

Feature	Kundennutzen
Alle Features in einer Lizenz (Self-Serviced oder Managed)	Einfache Entscheidung, transparentes Abo, kein Modul-Dschungel
Multi-Channel Simulation (E-Mail, SMS, Voice, QR, MFA, Callback)	Erkennungsroutine über alle realen Angriffswege
Trainingsbibliothek: 7.000+ Inhalte, 11 Provider, 30+ Sprachen	Nachweisbares Lernen ohne Belastung des Arbeitsalltags
KI-adaptive Lernpfade	Jeder lernt genau das, was er braucht
Phishing Reporter (Outlook / Google Workspace)	Mitarbeitende werden zu aktiven Mitgestaltern der Sicherheit
Human Risk Dashboard	Management-Reporting und Fortschrittsmessung auf einen Blick
Compliance Reports (NIS2, DSGVO, ISO 27001, DORA)	Audit-Sicherheit ohne manuellen Aufwand
Schulung vor erster Simulation	Akzeptanz im Team statt Frust und Widerstand
Wertfreie Auswertung ohne Bloßstellung	Lernkultur statt Kontrollkultur, hohe Beteiligung
Live-Trainings und Workshops (zubuchbar)	Persönliche Expertenvermittlung mit bleibenden Aha-Momenten
Zertifizierte Awareness Koordinatoren	Persönliche Begleitung, die kein reines Tool bietet



Die aktuelle Bedrohungslage

Die IT-Sicherheitslage in Deutschland ist so angespannt wie nie. Dieser Abschnitt fasst die wichtigsten Statistiken aus verlässlichen Quellen zusammen, als Faktenbasis für Ihre Kundengespräche.

Schadensbilanz Deutschland 2025

Der Gesamtschaden durch Datendiebstahl, Spionage und Sabotage erreichte 2025 laut Bitkom 289,2 Milliarden Euro, davon entfielen 70 % auf Cyberattacken. 8 von 10 Unternehmen waren betroffen, 73 % registrierten eine Zunahme der Angriffe. Der BSI-Lagebericht 2025 ergänzt das Bild: 80 % der Ransomware-Angriffe treffen kleine und mittlere Unternehmen, pro Tag werden 119 neue Schwachstellen entdeckt (plus 24 % gegenüber dem Vorjahr), und weltweit entstehen täglich über 800 neue Phishing-Seiten.

Der menschliche Faktor in den Zahlen

Der Verizon DBIR 2025 beziffert den menschlichen Anteil genau: 60 % aller Sicherheitsvorfälle haben eine menschliche Komponente, 22 % aller Datenverletzungen beginnen mit gestohlenen Zugangsdaten und 16 % mit Phishing. Das BKA benennt KI als Treiber der Cyberkriminalität 2025, von automatisierten Phishing-Kampagnen bis zu täuschend echten Deepfakes.

Wichtig für Ihre Gesprächsführung:
Die Zahlen zeigen, dass Angreifer gezielt dort ansetzen, wo Wissen fehlt. Genau dieses Wissen liefert der Service. Wer Mitarbeitende dagegen als Problem darstellt, verliert die Akzeptanz im Unternehmen und meist auch den Abschluss.

Neue Angriffsvektoren 2026

- Quishing: QR-Code-Phishing umgeht klassische E-Mail-Filter und wächst rasant
- KI-generiertes Spear-Phishing: hochpersonalisierte, fehlerfreie Angriffe in Sekunden erstellt
- Deepfake-Vishing: KI-Stimmen imitieren Vorgesetzte und Kollegen am Telefon
- MFA-Fatigue: gezielte Überflutung mit Authentifizierungsanfragen bis zur Bestätigung
- Callback-Phishing: E-Mails verweisen auf Telefonnummern statt Links und umgehen so URL-Filter vollständig

Für das Kundengespräch:
Die Bedrohungslage ist real und messbar. Technische Schutzmaßnahmen bleiben unverzichtbar, doch die Angriffe zielen zunehmend auf Menschen. Unternehmen, die ihre Mitarbeitenden trainieren, schließen genau die Lücke, die Angreifer 2026 am häufigsten nutzen.

NIS2 & Compliance

Wer ist betroffen?

Seit Dezember 2025 ist das NIS2-Umsetzungsgesetz in Deutschland in Kraft. Über 30.000 Unternehmen fallen unter die erweiterten Pflichten: Betreiber wesentlicher und wichtiger Einrichtungen ab 50 Mitarbeitenden oder 10 Millionen Euro Umsatz, dazu Zulieferer über die Lieferkette. Die Geschäftsleitung haftet persönlich für die Umsetzung.

Die wichtigsten NIS2-Anforderungen für Awareness

- Nachweisbare Sicherheitsschulungen für alle Mitarbeitenden (Art. 21 NIS2)
- Dokumentierte Awareness-Maßnahmen als Teil des Risikomanagements
- Regelmäßige Wirksamkeitsüberprüfung, Phishing-Simulationen gelten als Best Practice
- Die Geschäftsleitung muss die Maßnahmen kennen, billigen und überwachen

Wie der Service bei der NIS2-Compliance hilft

NIS2-Anforderung	Lösung durch den Service
Schulungsnachweise für Prüfer	Automatische Compliance-Reports und lückenlose Audit-Trails
Risikobasiertes Management	Human Risk Dashboard mit Entwicklung pro Abteilung
Regelmäßige Überprüfung	Kontinuierliche Simulationen mit dokumentierten Ergebnissen
Verantwortung der Geschäftsleitung	Management-Workshops (zubuchbar) und Executive-Reporting

Wichtig:

Security Awareness deckt einen zentralen Teil der NIS2-Pflichten ab. Positionieren Sie den Service als nachweisbaren Baustein des Risikomanagements und kombinieren Sie ihn mit technischen Maßnahmen aus Ihrem übrigen Portfolio.



Für wen ist der Service?

Ideale Zielgruppe

Zielgruppe	Warum ideal
KMU mit NIS2-Pflicht (50 bis 500 Mitarbeitende)	Compliance-Druck, kein eigenes Awareness-Team
Kanzleien, Steuerberater, Notare	Hochsensible Mandantendaten, DSGVO-Prüfungen im Alltag
Gesundheitswesen (Kliniken, Praxen, Pflege)	Viel Personal ohne IT-Hintergrund, hoher Schutzbedarf
Finanzdienstleister und Banken	DORA-Pflicht, MFA-Fatigue und Vishing besonders relevant
Kommunen und öffentliche Verwaltung	Häufige Angriffsziele, selten ein Awareness-Programm
MSPs und Systemhäuser	White-Label-Option, Recurring Revenue, Portfolioerweiterung
Bestandskunden mit Firewall/EDR	Technik vorhanden, die menschliche Komponente fehlt noch

Ideale Verkaufssituationen

- Der Kunde fragt nach NIS2 oder DSGVO und benötigt nachweisbare Schulungsmaßnahmen
- Nach einem Phishing-Vorfall oder Beinahe-Vorfall im Unternehmen
- Ein Audit oder eine Kundenprüfung steht bevor, Nachweise fehlen
- Ein neuer IT-Leiter oder CISO will den Sicherheitsreifegrad heben
- Ein Sicherheitsvorfall bei einem Wettbewerber sorgt für Aufmerksamkeit in der Branche
- Laufendes Firewall- oder EDR-Projekt: Awareness als komplementärer Baustein

Top 10 Verkaufsargumente

1 Wissen ist die wirksamste Verteidigung

60 % aller Sicherheitsvorfälle haben eine menschliche Komponente. Kein technisches System kann die Entscheidung ersetzen, die ein Mensch in zwei Sekunden trifft: klicken oder melden. Das Programm vermittelt genau dieses Entscheidungswissen, dauerhaft.

2 Kompetenz statt Kontrolle

Der Ansatz befähigt Mitarbeitende: Geschult wird vor der ersten Simulation, ausgewertet wird wertfrei und ohne Sanktionen. Das überzeugt Geschäftsführung und Betriebsrat und sichert die Akzeptanz im Programm.

3 NIS2- und DSGVO-Nachweise inklusive

Automatische Compliance-Reports und lückenlose Audit-Trails sind Bestandteil der Lizenz. Über 30.000 Unternehmen brauchen genau diesen Nachweis, die Geschäftsleitung haftet persönlich.

4 Messbare Ergebnisse in 90 Tagen

Typische Entwicklung: Die Klickrate sinkt von rund 30 % auf unter 10 %, die Meldequote vervielfacht sich. Der 90-Tage-Review bietet zugleich den natürlichen Anlass für das Gespräch über Erweiterungen.

5 Eine Lizenz, alles drin

Trainingsbibliothek, Simulationen über sechs Kanäle, KI-adaptive Lernpfade, Phishing Reporter, Dashboard und Compliance-Reports: Alle Plattform-Features sind in der Lizenz enthalten. Die Basisdiskussion bleibt damit angenehm einfach, ganz ohne Modulrechnung.

6 Nur eine Entscheidung: mit oder ohne Management

Der Kunde wählt lediglich zwischen Self-Serviced und Managed. Diese Einfachheit macht die Entscheidung leicht und verkürzt den Weg zum Start.

7 Schneller Start ohne Projektrisiko

Die Plattform läuft in der Cloud und ist in 24 bis 48 Stunden einsatzbereit; installiert wird beim Kunden nichts. Lange Pilotphasen sind dadurch selten nötig.

8 Einfache Kalkulation

Ein User entspricht einem Postfach. Das Mengengerüst für ein Angebot ist damit schnell erhoben, und die Staffelung nach Unternehmensgröße macht die Kalkulation transparent.

9 Recurring Revenue mit Ausbaupfad

Jede Lizenz läuft im Abonnement weiter und bringt rund 35 % Gesamtmenge. Darauf bauen Customization, Premium Content und kostenpflichtige Live-Elemente als planbare Zusatzumsätze auf.

10 White-Label für eigene Managed Services

Partner können den Service unter eigener Marke anbieten. Endkunden sehen die Marke des Partners. Eine gute Basis für MSPs, die ihr Security-Portfolio erweitern.



Ergänzende Leistungsbausteine

Die folgenden Bausteine ergänzen die Lizenz. Sie sind kostenpflichtig zubuchbar und eignen sich als Upsell nach dem Lizenzabschluss:

Baustein	Beschreibung
Onboarding Workshop	Halbtägige Einführung für bis zu vier Personen, einmalig. Empfohlen zum Self-Serviced-Modell.
Managed Customization	Individuell zugeschnittene Kampagnen, monatliche Review-Termine, auf Wunsch jährliche Smishing- und Vishing-Kampagnen.
Premium Content	Exklusive Videoinhalte mit den Infinigate-Koordinatoren für hohen Wiedererkennungswert.
Live-Workshops Management und Technik	Halbtägige Workshops für Führungsebene bzw. IT-Abteilung, pro Termin.
Awareness Basic und Kompakt	Grundagentrainings als Halbtags- oder 90-Minuten-Format, privat oder als offener Termin.
Vertiefungsmodule	Je 1,5 Stunden mit Live-Demos: Phishing, Identitäten & Passwörter, Mobiles Arbeiten, Social Engineering.
Awareness Sprechstunde	Offene Fragerunde mit einem Koordinator, bis zu einer Stunde pro Termin.
KI-Awareness Training	Halbtägiger Online-Workshop zum sicheren, verantwortungsvollen KI-Einsatz, über die Infinigate Akademie.

Preise und Konditionen:

Alle aktuellen Einkaufspreise finden Sie in der separaten Preisliste. Fordern Sie für jedes Kundenprojekt ein individuelles Angebot an.

Anfragen an: techservices@infinigate.de

90-Tage Partner-Aktivierungsplan

Phase 1:
Foundation (Tag 1-30)

Ziel: Eigene Plattform-Erfahrung aufbauen und das Lizenzpotenzial im Kundenbestand beziffern.

- Zugang zur Plattform über techservices@infinigate.de anfordern
- Onboarding-Schulung absolvieren
- Programm im eigenen Team durchlaufen: erst Lerneinheiten, dann die erste Simulation
- Lizenzpotenzial-Liste erstellen: Top 10 Bestandskunden mit geschätzter Useranzahl und wahrscheinlichem Modell (Self-Serviced oder Managed)
- Kunden mit NIS2-Bezug und bestehendem Firewall- oder EDR-Vertrag priorisieren

Praxis-Tipp: Die Lizenzpotenzial-Liste ist Ihr wichtigstes Werkzeug. Sie zeigt auf einen Blick, wo sich Gespräche zuerst lohnen.

Phase 2:
Aktivierung (Tag 31-60)

Ziel: Gespräche führen und für interessierte Kunden Angebote anfordern.

- Die priorisierten Kunden ansprechen, mit dem 30-Sekunden-Pitch aus diesem Playbook
- Im Gespräch die Useranzahl und die Modellpräferenz klären
- Demo-Termine mit Human Risk Dashboard vereinbaren; TechServices unterstützt auf Wunsch
- Für jeden qualifizierten Kunden ein Lizenzangebot über techservices@infinigate.de anfordern

Praxis-Tipp: Führen Sie das Gespräch über Souveränität statt über Angst, und bieten Sie am Ende an, beide Modelle für die konkrete Unternehmensgröße durchzurechnen.

Phase 3:
Conversion (Tag 61-90)

Ziel: Erste Abschlüsse erzielen und die Pipeline weiter füllen.

- Angebote nachfassen und abschließen; bei Unentschlossenen hilft die Managed-Empfehlung
- Für jeden Abschluss direkt den 90-Tage-Review vereinbaren
- Referenz-Story aus dem ersten Abschluss dokumentieren
- Zwei weitere Kunden in die Pipeline aufnehmen; White-Label-Option für das eigene Portfolio prüfen

Praxis-Tipp: Lassen Sie die Zahlen sprechen. Eine Klickrate, die von 30 % auf unter 10 % fällt, überzeugt jede Geschäftsführung und trägt die Fortführung des Programms gleich mit.

Entwicklungsmetriken
nach 90 Tagen

Metrik	Ziel
Eigenes Programm durchlaufen	Ja, mit dokumentiertem Ergebnis
Lizenzpotenzial-Liste erstellt	Top 10 Kunden mit Useranzahl und Modell
Kundengespräche geführt	Mindestens 5
Lizenzangebote angefordert	Mindestens 3
Erste Lizenzverträge	Mindestens 1

Partnerassets

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

30-Sekunden Elevator Pitch

Wissen Ihre Mitarbeitenden, woran man eine KI-generierte Phishing-Mail erkennt? Mit der Infinigate Awareness Plattform trainieren sie genau das: kompakte Lerneinheiten, dann realistische Simulationen in sicherer Umgebung. Die NIS2- und DSGVO-Nachweise entstehen automatisch. Das Ganze ist eine Lizenz pro Mitarbeitendem, wahlweise komplett durch uns betrieben. Darf ich Ihnen das Konzept einmal zeigen?"

Tipp: Der Pitch funktioniert, weil er mit einer Frage beginnt (erzeugt Neugier), einen positiven Zielzustand beschreibt (Souveränität statt Angst) und mit einer kleinen, konkreten Bitte endet.

Positionierung: Souveränität statt Angst

Verkaufen Sie Souveränität. Der Unterschied im Wortlaut ist klein, die Wirkung im Gespräch erheblich:

Vermeiden Sie	Formulieren Sie stattdessen
"Ihre Mitarbeiter sind Ihr größtes Risiko."	"Ihre Mitarbeitenden können Ihre stärkste Verteidigung sein, wenn man ihnen das Wissen dazu gibt."
"Ein Klick kann Ihre Firma ruinieren."	"Mit dem richtigen Training wird aus dem unsicheren Moment ein souveräner Handgriff: erkennen, melden, weiterarbeiten."
"Wir testen, wer bei Ihnen hereinfällt."	"Wir schulen zuerst und üben dann in sicherer Umgebung. Niemand wird bloßgestellt, jeder lernt dazu."
"Ohne Schulung drohen Bußgelder."	"Die Compliance-Nachweise bekommen Sie automatisch dazu, ein Audit-Thema weniger."



5-Minuten Pitch

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

Phase 1: Die neue Realität (60 Sekunden)

“Cyberangriffe funktionieren heute anders als vor fünf Jahren. KI schreibt Phishing-Mails ohne einen einzigen Rechtschreibfehler und imitiert am Telefon die Stimme des Chefs. 60 % aller Vorfälle haben eine menschliche Komponente, und der Schaden in Deutschland liegt bei 289 Milliarden Euro im Jahr.”

Phase 2: Das Wissens-Gap (60 Sekunden)

“Ihre Firewall schützt die Infrastruktur, und das ist wichtig. Aber die Entscheidung, ob ein Link angeklickt wird, trifft ein Mensch, in zwei Sekunden, hundertfach am Tag. Kein technisches System nimmt ihm diese Entscheidung ab. Und mit NIS2 müssen Sie nachweisen, dass Ihr Team darauf vorbereitet ist.”

Phase 3: Lösung vorstellen (90 Sekunden)

“Die Infinigate Security Awareness Services geben Ihren Mitarbeitenden genau dieses Wissen, und zwar so, dass es bleibt. Zuerst kompakte Lerneinheiten von wenigen Minuten pro Monat, dann realistische Simulationen in sicherer Umgebung, über alle Kanäle: E-Mail, SMS, Telefon, QR-Code. Wer reagiert, bekommt sofort eine kurze Lerneinheit, ohne Bloßstellung. Das Human Risk Dashboard zeigt Ihnen den Fortschritt, und die NIS2-Nachweise entstehen automatisch.”

Phase 4: Konkretes Beispiel (60 Sekunden)

“Stellen Sie sich vor: Eine Mitarbeiterin erhält eine täuschend echte Rechnung per Mail. Ohne Training klickt sie vielleicht, aus reiner Routine. Mit Training erkennt sie die Signale, meldet die Mail mit einem Klick und arbeitet weiter. Die IT blockiert den Absender für das ganze Unternehmen. Aus dem potenziellen Vorfall wird ein Beleg dafür, dass Ihr Team funktioniert.”

Phase 5: Nächster Schritt (30 Sekunden)

“Das Modell ist einfach: eine Lizenz pro Mitarbeitenden, wahlweise Self-Serviced oder komplett durch Infinigate betrieben. Wenn Sie mir Ihre ungefähre Unternehmensgröße nennen, bereite ich einen Vorschlag für beide Varianten vor. Dann können Sie in Ruhe entscheiden, welches Modell besser zu Ihnen passt.”

12 Discovery-Fragen

Diese Fragen öffnen das Gespräch und decken Handlungsbedarf auf. Die Fragen 10 und 11 helfen Ihnen einzuschätzen, welches Modell und welche Größenordnung für ein Angebot passen:

- 1. "Wissen Ihre Mitarbeitenden, woran man eine gefälschte E-Mail erkennt, und was sie dann tun sollen?"
→ Grundsicherung und Phishing Reporter
- 2. "Wie bereiten Sie neue Mitarbeitende auf aktuelle Angriffsmethoden vor?"
→ Onboarding-Integration des LMS
- 3. "Haben Sie schon von QR-Code-Phishing oder Deepfake-Anrufen gehört? Kennt Ihr Team das?"
→ Multi-Channel Simulation
- 4. "Haben Sie nachweisbare Schulungsmaßnahmen, falls morgen ein NIS2- oder DSGVO-Prüfer fragt?"
→ Compliance Reporting
- 5. "Wie würden Sie heute erfahren, ob eine Phishing-Welle gerade Ihr Unternehmen erreicht?"
→ Phishing Reporter und Dashboard
- 6. "Wie messen Sie aktuell die Sicherheitskompetenz Ihres Teams?"
→ Human Risk Dashboard
- 7. "Was passiert bei Ihnen, wenn jemand versehentlich auf einen schädlichen Link klickt? Gibt es einen definierten, angstfreien Meldeweg?"
→ Lernkultur und Reporter
- 8. "Wie viel Arbeitszeit können Ihre Mitarbeitenden realistisch für Schulungen aufbringen?"
→ Micro-Learning, 5 bis 10 Minuten pro Monat
- 9. "Wer in Ihrem Unternehmen haftet persönlich, wenn NIS2-Pflichten nicht erfüllt werden?"
→ Persönliche Haftung der Geschäftsleitung
- 10. "Wie viele Mitarbeitende mit E-Mail-Postfach haben Sie?"
→ Mengengerüst für das Lizenzangebot
- 11. "Haben Sie ein Team, das ein solches Programm selbst betreiben würde, oder soll es einfach laufen?"
→ Modellwahl Self-Serviced oder Managed
- 12. "Was müsste ein Awareness-Programm leisten, damit Sie nach 90 Tagen sagen: Das hat sich gelohnt?"
→ Erfolgskriterien und Abschluss



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

Einwandbehandlung

Einwand	Antwort
"Wir haben bereits Firewall und EDR."	"Sehr gut, die Basis steht. Aber die Entscheidung, ob ein Link angeklickt wird, trifft ein Mensch, nicht die Firewall. Der Service ergänzt Ihre Technik um genau diese Komponente."
"Zu teuer."	"Die monatliche Investition liegt weit unter dem, was ein einziger erfolgreicher Angriff kostet. Gern erstelle ich Ihnen ein konkretes Angebot für Ihre Unternehmensgröße."
"Unsere Leute sind doch fit."	"Umso besser. Dann bestätigt die erste Auswertung das, und Ihr Team bleibt mit minimalem Aufwand auf diesem Niveau. Die Angriffe von 2026 sehen anders aus als die von 2023."
"Keine Zeit für Schulungen."	"Genau dafür ist das Programm gemacht: 5 bis 10 Minuten pro Monat, wann es passt. Keine Ganztagesseminare, kein Produktionsausfall."
"Wir wollen unsere Mitarbeiter nicht kontrollieren."	"Das wollen wir auch nicht. Das Programm schult zuerst, übt dann in sicherer Umgebung und wertet ohne namentliche Bloßstellung aus. Es geht um Kompetenzaufbau, und genau deshalb funktioniert das Programm."
"Wir haben schon KnowBe4."	"Dann kennen Sie den Wert bereits. Wir bieten vergleichbaren Umfang plus persönliche Betreuung durch zertifizierte Koordinatoren und zubuchbare Live-Trainings. Das hat ein reiner Plattform-Anbieter nicht."
"NIS2 betrifft uns nicht."	"Möglich. Aber sind Sie Zulieferer eines größeren Unternehmens? Dann kommt die Anforderung über die Lieferkette. Und unabhängig davon: Die Angriffe treffen Sie so oder so."
"Phishing-Tests frustrieren nur."	"Wenn man mit Tests startet, ja. Deshalb beginnt unser Programm mit der Schulung. Die erste Simulation kommt erst, wenn alle vorbereitet sind. Das ist der entscheidende Unterschied."
"Reicht nicht ein einmaliges Training?"	"Ein Training wirkt punktuell, aber Angriffe entwickeln sich ständig weiter. Das Learn-Management-System macht daraus einen dauerhaften Prozess: monatliche Lerneinheiten, aktuelle Simulationen, fortlaufende Nachweise. Genau das verlangt auch NIS2."
"Ich möchte das intern besprechen."	"Sehr gerne. Darf ich Ihnen dafür eine kurze Zusammenfassung mit dem Konzept und einem Beispiel-Reporting mitgeben? Das macht die interne Diskussion konkreter."
"Wie lange dauert das Onboarding?"	"24 bis 48 Stunden. Die Plattform ist cloudbasiert, es wird nichts installiert, kein Eingriff ins Netzwerk."

Case-Templates

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

Case 1: Mittelständischer Industriebetrieb (150 Mitarbeitende)

Trigger: NIS2-Projekt. Firewall und EDR vorhanden, aber keine nachweisbaren Awareness-Maßnahmen. Der IT-Leiter hat keine Kapazität für Schulungsorganisation.

Lösung: Managed Awareness Service mit Kickoff-Workshop. Grundschulung für alle, danach quartalsweise Simulationen über wechselnde Kanäle.

Ergebnis: Klickrate von 34 % auf 9 % in 90 Tagen. NIS2-Schulungsnachweis vollständig. Managed-Lizenz abgeschlossen.

Case 2: Regionalbank (280 Mitarbeitende, DORA-Pflicht)

Trigger: DORA-Compliance erforderlich, das bisherige Schulungssystem ist veraltet und wird vom Team als lästige Pflicht empfunden.

Lösung: Managed Service mit Customization: individuell zugeschnittene Kampagnen, KI-adaptive Lernpfade, monatliches Management-Reporting für den Vorstand.

Ergebnis: DORA-konforme Dokumentation, Beteiligungsquote der Mitarbeitenden deutlich gestiegen, Erkennungsrate nach sechs Monaten um 88 % verbessert.

Case 3: IT-Systemhaus als MSP (200 Endkunden)

Trigger: Das Systemhaus will sein Managed-Services-Portfolio um Security Awareness erweitern, ohne eigene Plattform-Entwicklung.

Lösung: White-Label-Betrieb auf Basis des Managed Service. Eigene Marke gegenüber den Endkunden, Betrieb durch Infinigate, Eigenbetrieb als Showcase.

Ergebnis: Zwölf Endkunden in vier Monaten gewonnen, Security Awareness als fester Bestandteil jedes neuen Managed-Service-Vertrags etabliert.

Case 4: Klinikverbund (5 Häuser, 800 Mitarbeitende)

Trigger: KRITIS-nahe Anforderungen, hohe Fluktuation in der Pflege, viele Mitarbeitende ohne festen PC-Arbeitsplatz.

Lösung: Managed Service mit Customization, jährliche Smishing-Kampagne (Pflegepersonal nutzt primär Smartphones), zubuchbare Live-Trainings vor Ort.

Ergebnis: Smishing-Klickrate von 41 % auf 11 %, alle Häuser mit einheitlicher Dokumentation, interner Awareness-Beauftragter aufgebaut.

Case 5: Steuerberatungskanzlei (85 Mitarbeitende)

Trigger: DSGVO-Due-Diligence eines Mandanten steht bevor, keine nachweisbaren Schulungsmaßnahmen vorhanden.

Lösung: Self-Serviced-Modell mit Onboarding Workshop. Grundschulung, danach zwei Simulationen, automatische DSGVO-Reports.

Ergebnis: Prüfung bestanden, Klickrate von 31 % auf 8 %, Geschäftsführung führt das Programm dauerhaft fort.

Case 6: Stadtwerke (KRITIS, 600 Mitarbeitende)

Trigger: Ein Angriff auf ein vergleichbares Stadtwerk sorgt für Handlungsdruck im Vorstand. Sofort nachweisbare Maßnahmen gefordert.

Lösung: Managed Service mit Onboarding, zubuchbarer Management-Workshop für die Führungsebene, jährliche Vishing-Kampagne.

Ergebnis: Vollständige Dokumentation in sechs Wochen, Vishing-Erkennungsrate auf 94 % gesteigert, jährlicher Awareness-Tag etabliert.



12 Mottos für Security Awareness

Die folgenden zwölf Mottos eignen sich für unterschiedliche Kommunikationsanlässe, von Präsentationen über E-Mails bis zu Social-Media-Posts und Veranstaltungen:

1. "Sicher erkennen. Souverän handeln. Frei arbeiten." TOP 1
2. "Wissen ist die beste Verteidigung." TOP 2
3. "Menschen stärken. Unternehmen schützen." TOP 3
4. "Kompetenz statt Kontrolle."
5. "Sicherheit, die im Kopf beginnt."
6. "Souverän im Posteingang."
7. "Lernen in sicherer Umgebung."
8. "Erkennen statt erschrecken."
9. "Das Wissen, das auch privat schützt."
10. "Security Awareness ohne erhobenen Zeigefinger."
11. "Aus Routine wird Erkennungskompetenz."
12. "Ihr Team. Ihre stärkste Verteidigungslinie."

Top-3 Begründung

#1

"Sicher erkennen. Souverän handeln. Frei arbeiten."

Am stärksten, weil es den kompletten Nutzenbogen in drei Schritten erzählt und mit dem emotionalen Ziel endet: Freiheit statt Angst. Funktioniert als Headline, Claim und Gesprächseinstieg.

#2

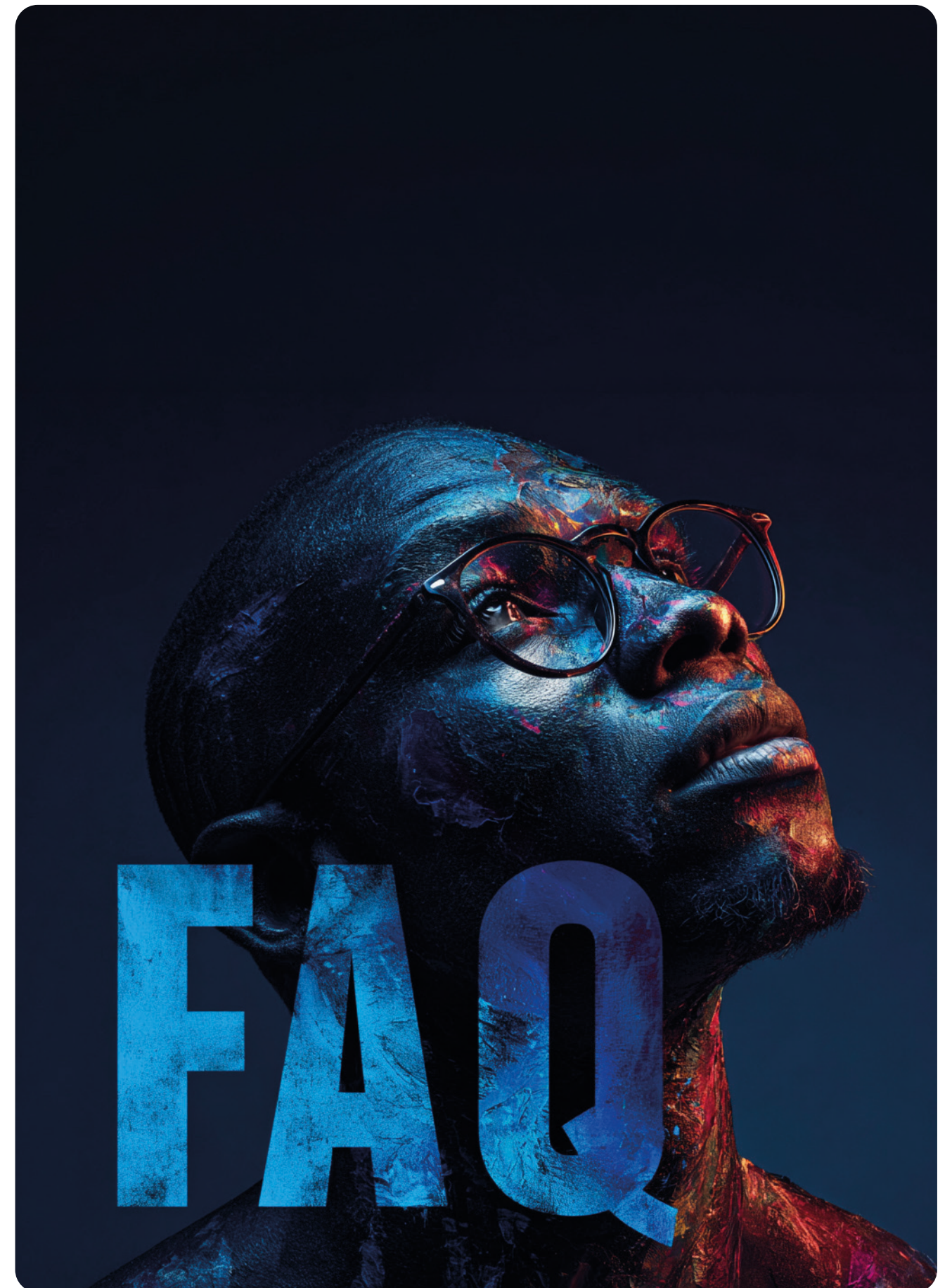
"Wissen ist die beste Verteidigung."

Klare, universelle Nutzensaussage, die den Kompetenzansatz auf den Punkt bringt. Eignet sich besonders für Präsentationen und Angebotstexte.

#3

"Menschen stärken. Unternehmen schützen."

Verbindet die Mitarbeiterperspektive mit dem Unternehmensnutzen in einer Zeile. Ideal für Management-Gespräche und Executive Summaries.



FAQ – Häufig gestellte Fragen

- 1. Was ist das Kernangebot?**

Eine Lizenz pro User der Infinigate Awareness Plattform, abgerechnet im Abonnement, in zwei Modellen: Self-Serviced (der Kunde betreibt selbst) oder Managed (Infinigate übernimmt den kompletten Betrieb). Alle Plattform-Features sind in der Lizenz enthalten. Live-Trainings und Workshops sind kostenpflichtige Zusatzbausteine.
- 2. Wie unterscheidet sich der Service von Firewall oder EDR?**

Firewall und EDR schützen die technische Infrastruktur. Der Service adressiert die Entscheidungen, die Menschen täglich treffen: klicken oder melden. Beide Ebenen ergänzen sich.
- 3. Warum beginnt das Programm mit Schulung statt mit einem Test?**

Weil unvorbereitete Tests Frust erzeugen und die Akzeptanz zerstören. Die Grundschulung kommt zuerst, die erste Simulation folgt danach. So erleben Mitarbeitende das Programm als Unterstützung.
- 4. Werden Mitarbeitende bloßgestellt, die auf Simulationen reagieren?**

Nein. Wer reagiert, erhält unmittelbar eine kurze Lerneinheit, ohne namentliche Bloßstellung und ohne Sanktionen. Das Ziel ist Kompetenzaufbau. Diese Haltung ist ein wesentlicher Erfolgsfaktor für die Akzeptanz.
- 5. Wie schnell ist die Plattform einsatzbereit?**

In der Regel innerhalb von 24 bis 48 Stunden. Cloudbasiert, ohne Agent und ohne Eingriffe ins Netzwerk des Kunden.
- 6. Braucht der Kunde ein eigenes Security-Team?**

Nein. Im Managed-Modell übernimmt Infinigate den vollständigen Betrieb: Nutzerverwaltung, monatliche Lerninhalte, Simulationen und Reporting.
- 7. Hilft der Service bei NIS2 und DSGVO?**

Ja. Automatische Compliance-Reports und lückenlose Audit-Trails dokumentieren alle Maßnahmen. Der Service ist ein zentraler Baustein der Compliance, ersetzt aber kein vollständiges Risikomanagement.
- 8. Welche Sprachen werden unterstützt?**

Die Trainingsbibliothek umfasst Inhalte in über 30 Sprachen, geeignet für internationale Teams.
- 9. Kann der Service als White-Label angeboten werden?**

Ja. Partner können den Service unter eigener Marke anbieten. Endkunden sehen ausschließlich die Marke des Partners.
- 10. Wie starte ich als Partner?**

Zugang über techservices@infinigate.de anfordern, das Programm im eigenen Team durchlaufen und mit dem 90-Tage-Aktivierungsplan starten. Das TechServices-Team unterstützt im Presales und begleitet auf Wunsch Ihre Kundengespräche.

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. Zugang anfordern: techservices@infinigate.de

2. Demo buchen und die Plattform live erleben

3. Das Programm im eigenen Team durchlaufen: erst Schulung, dann Simulation

4. Lizenzpotenzial-Liste erstellen und erste Kundengespräche terminieren.
Das TechServices-Team begleitet Sie auf Wunsch

Kontaktinformationen

Bereich	Kontakt
Service Sales & Awareness-Anfragen	techservices@infinigate.de +49 89 89048-403
Presales & technische Beratung	techservices@infinigate.de +49 89 89048-403
Postsales Support	support@infinigate.de +49 89 89048-400
Akademie & Trainings	akademie@infinigate.de +49 89 89048-401

Quellen

- **BSI:** Die Lage der IT-Sicherheit in Deutschland 2025
- **Bitkom:** Wirtschaftsschutz 2025
- **BKA:** Bundeslagebild Cybercrime 2024
- **Verizon:** Data Breach Investigations Report 2025

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

