

# MANAGED SECURITY

# 2025

## Effektiver Schutz vor modernen Cyberangriffen

Ein Whitepaper für Unternehmen, die ihre IT-Sicherheit durch moderne Endpoint-Detection & Response (XDR) auf das nächste Level heben wollen.

## Automatisierte Resilienz

Selbstheilende Endpunkte dank KI-gestützter Erkennung, Isolation und Rollback.

## Prävention statt Reaktion

Angriffe werden nicht nur erkannt, sondern aktiv verhindert, bevor ein Schaden entstehen kann.

# Inhalt

Executive Summary	03
Die neue Bedrohungslandschaft	04
Entwicklung der Cyberangriffe	05
Relevanz für KMU & Grossunternehmen	06
Typische Schwachstellen	08
Herausforderungen	09
Managed Security	10
Ihre Vorteile	12
Integration	14
Kompatibilität mit Windows, macOS, Linux	14
Zusammenspiel mit weiteren Technologien	14
Roadmap zur Einführung	15

Cyberangriffe werden immer komplexer und professioneller. Für die meisten Unternehmen ist es kaum mehr möglich, mit herkömmlichen Strategien und Produkten Schritt zu halten.

Managed Security verbindet moderne Technologien mit kontinuierlicher Überwachung durch ausgewiesene Experten und sorgt so für Sicherheit, bevor ein Schaden entsteht.

Dieses Whitepaper zeigt auf, wie Unternehmen aktuelle Risiken gezielt minimieren, ihre IT-Infrastruktur nachhaltig schützen und gleichzeitig mehr Freiraum für ihr Kerngeschäft gewinnen.

Kontaktieren Sie uns online:  
[galaxyweb.ch/support](https://galaxyweb.ch/support)

Galaxyweb AG

# Executive Summary

## Der entscheidende Faktor für digitale Resilienz.



### Unsere Lösung für Ihre Sicherheit

Die digitale Welt ist zum zentralen Fundament unserer Wirtschaft geworden. Heutige Geschäftsmodelle, Wertschöpfungsketten und sogar kritische Infrastrukturen hängen vollständig von vernetzten Systemen ab. Diese Abhängigkeit bietet Chancen für Innovation und Effizienz, öffnet aber zugleich die Tür für eine neue Qualität von Bedrohungen.

Cyberangriffe sind längst keine Einzelfälle mehr, sondern ein ständiger Begleiter des digitalen Alltags: automatisiert, hochprofessionell und in einem Ausmass, das Unternehmen aller Branchen betrifft.

**Besonders kleine und mittlere Unternehmen**, die oft nicht über eine eigene Security-Abteilung verfügen, geraten zunehmend ins Visier. Klassische Schutzmechanismen wie Firewalls oder signaturbasierte Antivirus-Lösungen reichen hier nicht mehr aus. Sie erkennen bekannte Muster, doch Angreifer entwickeln täglich neue Methoden, die genau jene Hürden umgehen. Zero-Day-Exploits, Ransomware-as-a-Service oder gezielte Phishing-Kampagnen

sind Beispiele für Angriffstypen, die innerhalb von Sekunden verheerende Schäden anrichten können. Finanziell, organisatorisch und nicht zuletzt im Bereich Reputation und Vertrauen.

Statt Unternehmen mit der komplexen Aufgabe der permanenten Bedrohungsanalyse und Abwehr alleine zu lassen, verbindet Managed Security modernste Technologie mit kontinuierlicher Expertise. Galaxyweb stellt mit seiner Security-Plattform eine Lösung bereit, die Bedrohungen in Echtzeit erkennt, automatisch isoliert und im Ernstfall sogar Systeme eigenständig in einen fehlerfreien Zustand zurückversetzt.

**Managed Security geht über reine Technologie hinaus.** Ein entscheidendes Element ist das Zusammenspiel von 24/7 Monitoring durch ein Security Operations Center (SOC), klar definierten Reaktionsprozessen und der engen Zusammenarbeit mit den Kunden. So profitieren Unternehmen nicht nur von der Plattform selbst, sondern auch von einem Expertenteam, das Alarme

bewertet, Angriffe priorisiert und gezielt Massnahmen einleitet. Für die internen IT-Teams bedeutet dies eine deutliche Entlastung: Ressourcen können sich auf das Kerngeschäft konzentrieren.

**Die Vorteile liegen auf der Hand:** Höchster Schutzstandard, kalkulierbare Kosten, schnelle Reaktionszeiten und eine signifikante Reduktion des Geschäftsrisikos. Hinzu kommt die wachsende Bedeutung regulatorischer Anforderungen – sei es das neue Schweizer Datenschutzgesetz (nDSG), die DSGVO oder branchenspezifische Normen wie ISO 27001 oder FINMA-Vorgaben. Managed Security unterstützt Unternehmen dabei, diese Standards einzuhalten und Nachweispflichten zu erfüllen. Managed Security ist nicht nur eine Option für gefährdete Branchen oder Grossunternehmen. Es ist eine zentrale Voraussetzung für die digitale Resilienz aller Organisationen.

*Reger Siess*  
Geschäftsführer

# Die neue Bedrohungslandschaft

**Cyberangriffe** haben sich von vereinzelt Störaktionen zu einem hochlukrativen Geschäftsmodell entwickelt. Ransomware-as-a-Service, Phishing oder Angriffe auf Lieferketten sind heute so professionell organisiert, dass Unternehmen jeder Grösse betroffen sein können. Angreifer nutzen dabei nicht nur technische Schwachstellen, sondern gezielt auch menschliche Faktoren wie Unachtsamkeit oder fehlende Sensibilisierung.

Besonders kritisch ist die zunehmende Automatisierung von Angriffen. KI-gestützte Werkzeuge scannen Netzwerke, identifizieren Schwachstellen und führen Exploits in Sekunden aus. So geraten auch kleinere Unternehmen in den Fokus – nicht, weil sie gezielt ausgesucht wurden, sondern weil ein Bot eine Lücke entdeckt hat.

Hinzu kommt die Hybridität der Arbeitswelt: Homeoffice, mobile Endgeräte und Cloud-Dienste erweitern die Angriffsfläche erheblich. Mitarbeiter greifen von überall

auf Unternehmensressourcen zu, oft über ungesicherte Netzwerke oder private Geräte. Für Angreifer ist das ein einfacher Einstiegspunkt. Gleichzeitig verschwimmen die Grenzen zwischen internen und externen IT-Umgebungen. Cloud-Services, hybride Infrastrukturen und mobile Arbeitsplätze schaffen neue Angriffsflächen, die klassische Sicherheitsarchitekturen nicht mehr zuverlässig abdecken.

Erfolgreiche Cyberresilienz erfordert daher integrierte Lösungen, die Endgeräte, Netzwerke und Identitäten ganzheitlich schützen.

**Die Bedrohungslandschaft** ist damit nicht nur vielfältiger, sondern auch dynamischer geworden. Klassische Konzepte reagieren oft zu spät. Unternehmen müssen ihre Sicherheitsstrategien daher neu denken: Weg von reaktiver Verteidigung, hin zu proaktiver Erkennung, kontinuierlichem Monitoring und automatisierter Abwehr.

## ERKENNUNG

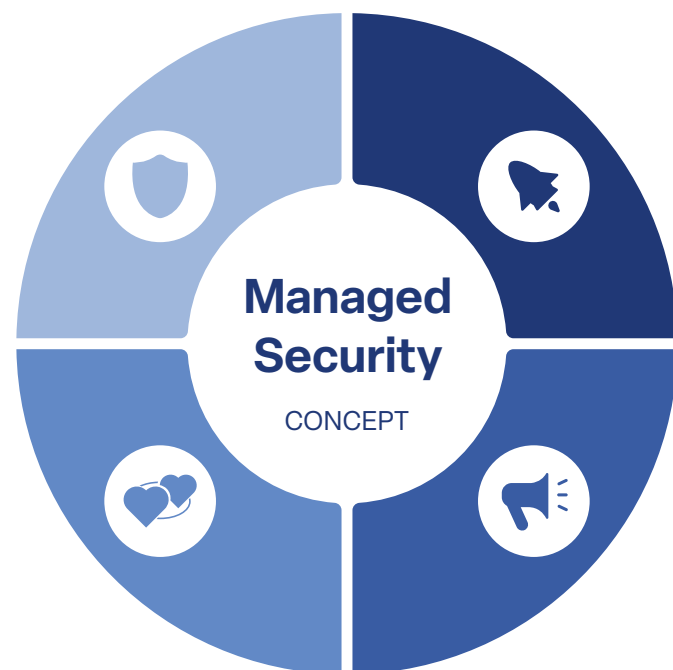
Neue Bedrohungen in Echtzeit identifizieren, statt erst im Nachhinein reagieren.

- Threat Intelligence
- Zero-Day Awareness
- Predict & Prevent

## MONITORING

24/7 Überwachung, Bewertung und Priorisierung durch Spezialisten.

- 24/7 Visibility SIEM
- Always On
- Expert Oversight



## REAKTION

Technische und organisatorische Minimierung von Ausfallzeiten und Schäden.

- Instant Response
- Rollback Ready
- Contain & Control

## RESILIENZ

Entlastung der internen IT und Fokus auf das Kerngeschäft.

- Secure by Design
- Compliance First
- Business Continuity

# Entwicklung der Cyberangriffe

## Das Risiko steigt

**Seit dem Jahr 2020** hat sich die Cyberkriminalität in der Schweiz dramatisch verschärft: Die Zahl der digitalen Straftaten hat sich mehr als verdoppelt, im Jahr 2024 wurden in der polizeilichen Kriminalstatistik 59'034 Cyberverbrechen erfasst – ein Plus von etwa 35 % gegenüber dem Vorjahr. Auch im ersten Quartal 2025 meldeten Schweizer Unternehmen spürbar mehr Angriffe. Ein deutliches Indiz für die weiter eskalierende Lage.

**In Deutschland** stieg die Cyberkriminalität ebenfalls deutlich an. Im Jahr 2023 verzeichnete das Bundeskriminalamt (BKA) einen Anstieg um 28 % bei Angriffen durch ausländische Täter im Vergleich zum Vorjahr. Für das Jahr 2024 wurden insgesamt 131'391 Fälle innerstaatlicher Cyberkriminalität gemeldet – hinzu kamen weitere 201'877 Vorfälle aus dem Ausland oder unidentifizierten Quellen.

## Fazit für den Zeitraum 2020-2025

**Cyberkriminalität** hat 2025 eine neue Dimension erreicht und verursacht immense wirtschaftliche Verluste. Besonders Ransomware und Phishing dominieren die Vorfälle in der gesamten DACH-Region.

- **Schweiz:** Cyberkriminalität hat sich mehr als verdoppelt, mit nahezu 60'000 Fällen im Jahr 2024.
- **Deutschland:** Starker Anstieg bei ausländischen Angriffen (plus 28 % in 2023), fast 200'000 Vorfälle in 2024.
- **Österreich:** Deutlicher Anstieg der Cyberdelikte seit 2020; prominente Angriffe zeigen ein wachsendes Risiko, insbesondere für kritische Infrastruktur und Institutionen.

## Aktuelle Kennzahlen



## TOP 5 RISIKEN FÜR FIRMEN

### 1. AI Phishing & Deepfakes

KI erzeugt realistische Mails, Stimmen & Deepfakes. Die Erkennung wird schwieriger.



### 2. Crypto-Ransomware

Moderne Angriffe verbinden Verschlüsselung mit Datendiebstahl & Erpressung.



### 3. Cloud-Infiltration

Entwendete Zugangsdaten öffnen Cloudlösungen und interne Systeme.



### 4. Living-off-the-Land Angriffe

Versierte Angreifer nutzen systemeigene Programme, um unbemerkt zu agieren.



### 5. Hybride Bedrohungen

Cyberangriffe werden mit Sabotage und Propaganda kombiniert.

# Relevanz für KMU & Grossunternehmen



## Cybercrime betrifft uns alle

**Bedrohungen treffen Unternehmen jeder Grösse:** Vom kleinen Betrieb bis zum globalen Konzern geraten alle ins Visier von Angreifern. Während grosse Organisationen komplexe IT-Strukturen absichern müssen, fehlen kleineren Firmen häufig Ressourcen und Know-how. Managed Security füllt diese Lücke, kombiniert Technologie mit Expertise und stellt sicher, dass Prozesse resilient bleiben.

Branche	% Anteil Angriffe	Top-Bedrohung (kurz)	Ø Schaden je Vorfall (EUR)	Typische Ziele	Trend
Produktion / Fertigung	26%	Ransomware, Public-Apps-Exploits	5.56 M	OT / Produktions-IT, ERP	steigend
Finanzen & Versicherungen	23%	Phishing, App-Exploits	6.08 M	Kundenportale, AD	konstant
IT- & Business-Services	18%	Credential Harvesting, Public Apps	4.88 M	Cloud, Mail, Web-Apps	steigend
Gesundheitswesen	5%	Ransomware, Server-Access	9.77 M	klinische Systeme, PII	exponiert
Regierung / Public Sector	3%	DDoS / Erpressung, Credentials	4.88 M	Bürgerdienste, Netz	DDoS aktiv

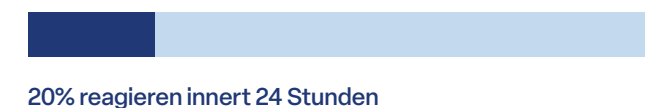
## Auswirkung auf den Betrieb

**Die Folgen von Cybercrime** in der DACH-Region zeigen sich vor allem in langen Ausfällen, Datenverlust und hohen Lösegeldforderungen. Jeder Angriff bedeutet Risiko für Stabilität, Daten und wirtschaftliche Existenz.



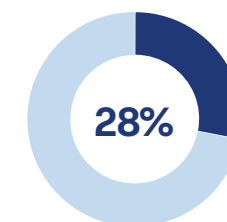
## Angriffe bleiben lange unentdeckt

**Erschreckend**, denn zirka 60% der Unternehmen bemerken Vorfälle erst durch externe Hinweise. Nur 20% reagieren innert der ersten 24 Stunden.

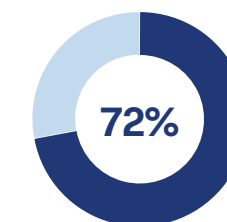


## Interne vs. externe Akteure

**Laut Bitkom-Wirtschaftsschutz 2024:** 28% der Angriffe auf deutsche Firmen entstanden durch Mitarbeiter, Dienstleister oder Partner. In der CH und AT ist es ähnlich.

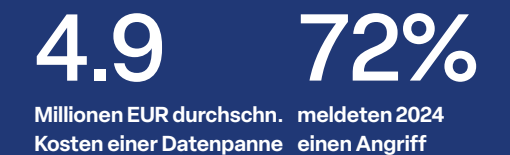


**interne Herkunft**  
durch Fahrlässigkeit oder vorsätzliche Handlungen.



**externe Verursacher**  
Kriminelle mit unterschiedlichen Motivationen und Zielen.

## DEUTSCHLAND IN ZAHLEN



## RANSOMWARE-MELDUNGEN 2023 VS 2024 IN DER SCHWEIZ

Die Dunkelziffer wird auf das 5- bis 10-Fache der gemeldeten Vorfälle geschätzt



## ENTWICKLUNG NACH REGION

Schweiz	+113% (Q1 2025 vs. 2024)
Deutschland	+55% (Q1 2025 vs. 2024)
Österreich	+69% (Q1 2025 vs. 2024)
Italien	+89% (Jahresbasis '24 vs '23)
Frankreich	+15% (Jahresbasis '24 vs '23)

- Externe Angriffe verursachen den grössten Schaden, interne werden oft unterschätzt.
- Phishing, Crypto-Ransomware und Social Engineering stehen an der Spitze.
- Interne Risiken entstehen oft durch Fehlverhalten und mangelnde Awareness.

35%

der Schweizer Firmen meldeten 2024 mindestens einen Angriff

74%

der DE-Unternehmen waren 2024 von Datendiebstahl betroffen

68%

der österreichischen Firmen sahen 2024 steigende Attacken

40%

aller DACH-Unternehmen nennen Ransomware als grösstes Risiko

## Rein reaktive Lösungen sind überfordert

**Die aktuellen Fallzahlen zeigen deutlich**, dass Bedrohungen nicht nur häufiger werden, sondern auch existenzielle Folgen haben können. Managed Security sorgt dafür, dass diese Risiken kalkulierbar bleiben – durch Prävention, kontinuierliches Monitoring und schnelle Reaktion, gepaart mit maschineller Intelligenz.

Cyberangriffe sind längst ein Massenphänomen und betreffen die Mehrheit der Unternehmen in der DACH-Region auf unterschiedliche Art und Weise:

- Cybercrime:** Angriffe machen keinen Unterschied in der Unternehmensgrösse, da sowohl kleine Betriebe als auch globale Player lohnende Ziele sind. Besonders KMU unterschätzen oft ihr Risiko und sind dadurch noch anfälliger.
- Datenklau, Spionage und Sabotage:** Angreifer haben es nicht nur auf Geld abgesehen, sondern auch auf sensible Informationen und Produktionsprozesse. Solche Vorfälle führen zu Reputations- und Vertrauensverlusten.
- Organisierte Kriminalität:** Professionelle Gruppen agieren arbeitsteilig und hochgradig vernetzt, oft sogar international. Dadurch steigt die Effizienz der Angriffe und die Zahl erfolgreicher Erpressungsversuche drastisch.

# Typische Schwachstellen

Die meisten Angriffe gelingen nicht primär wegen hochentwickelter Technologien, sondern aufgrund trivialer Fehler und Schwachstellen, die im Alltag entstehen.

Diese Risiken betreffen uns alle gleichermassen.

Menschliches Verhalten, fehlende Updates oder unklare Prozesse öffnen Angreifern immer wieder die Tür.

## Der Faktor Mensch

Kriminelle nutzen vermehrt technische, organisatorische und menschliche Schwächen aus. Moderne Schutzkonzepte müssen genau an diesen Stellen ansetzen.



Die Schulung bleibt ein wichtiges Thema, um das Sicherheitsbewusstsein zu stärken.



Mit Social Engineering werden die menschlichen Schwächen ausgenutzt.



Durch gezielte Ablenkung wird das Personal anfällig für Angriffe.

## Angreifer missbrauchen jede Gelegenheit

Nicht nur Technik, auch Menschen sind ein Ziel für Angreifer. Manipulation und Social Engineering gehören zu den häufigsten Einfallstoren und haben weitreichende Konsequenzen für das Unternehmen, Mitarbeiter, Kunden und Partner.

- **Ablenkung & Stress:** Zeitdruck oder Überlastung führen dazu, dass Mitarbeitende unachtsam handeln und Fehler machen.
- **Social Engineering:** Angreifer nutzen Täuschung und Manipulation, um Mitarbeitende zur Preisgabe sensibler Informationen zu bewegen. Oft reicht schon ein einziger Klick oder eine unbedachte Antwort, um einen umfassenden Angriff auszulösen.

## Digitalisierung und Transformation

Die digitale Transformation eröffnet Unternehmen enorme Potenziale.

**Bestehende Prozesse werden automatisiert**, Daten stehen in Echtzeit zur Verfügung, neue Geschäftsmodelle entstehen. Gleichzeitig führt die zunehmende Vernetzung von Systemen, Geräten und Mitarbeitern aber auch zu einer deutlich grösseren Angriffsfläche für Cyberkriminelle.

Besonders problematisch ist, dass viele Organisationen die Geschwindigkeit der Transformation unterschätzen. Neue Cloud-Dienste, hybride Arbeitsmodelle und IoT-Geräte werden eingeführt, ohne dass Sicherheitskonzepte von Anfang an konsequent mitgedacht werden. Das Resultat sind ungleiche Sicherheitsniveaus, technische Schulden und eine wachsende Komplexität, die interne IT-Teams häufig überfordert.

**Hinzu kommt die menschliche Dimension:** Mitarbeitende müssen nicht nur die neuen Tools und Proz-

esse beherrschen, sondern auch sicher damit umgehen – von der Nutzung starker Passwörter bis zum Erkennen von Phishing-Versuchen. Fehlt es an Schulung und Bewusstsein, wird Digitalisierung selbst zum Einfallstor für Angriffe.

**Um von den Vorteilen nachhaltig zu profitieren**, brauchen Unternehmen daher eine ganzheitliche Sicherheitsstrategie, die Technologie, Prozesse und Menschen gleichermassen berücksichtigt. Nur so lässt sich sicherstellen, dass Innovation nicht zur Schwachstelle wird.

Das Zusammenspiel von Security Services mit klaren Sicherheitskonzepten und kontinuierlichen Schulungen der Mitarbeitenden erweist sich dabei als massgeblicher Erfolgsfaktor. Entscheidend hinter Managed Security ist der richtige Anbieter. Er übernimmt nicht nur einen wesentlichen Teil der Sicherheitsaufgaben, sondern wird zum verlässlichen Partner im täglichen Schutz der IT-Infrastruktur.

# Herausforderungen verstehen

## Challenges der IT-Sicherheit

In vielen Unternehmen existieren bereits Sicherheitslösungen wie Firewalls, VPNs, E-Mail-Security, NAC, IAM oder Endpoint-Schutz. Doch erst im Gesamtzusammenspiel entfalten sie ihre Wirkung. Entscheidend ist deshalb, neue Lösungen nicht isoliert einzuführen, sondern sie sauber in die bestehende Umgebung zu integrieren und die Umsysteme im Blick zu behalten.

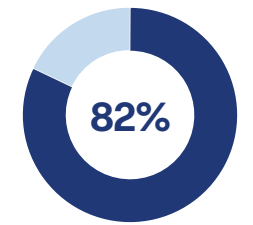
**Managed Security** bedeutet nicht nur Technologie einzusetzen, sondern auch auf Expertise, Prozesse und schnelle Reaktionsfähigkeit vertrauen zu können. Wird ein ungeeigneter Partner gewählt, drohen gravierende Folgen: Alarmer werden falsch priorisiert, Angriffe bleiben zu lange unentdeckt oder Sicherheitsvorfälle werden unkoordiniert behandelt und verschlimmern die Situation.

Dies kann nicht nur zu finanziellen Schäden und langen Ausfallzeiten führen, sondern auch zu Vertrauensverlust bei Kunden und Partnern. Ein zuverlässiger Managed Security Partner hingegen schafft Transparenz, reagiert im Ernstfall rasch und sorgt dafür, dass Massnahmen in die bestehende IT integriert werden.

## Entscheidungsfaktoren

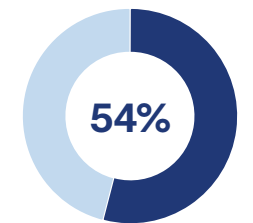
**Die Mehrheit der Unternehmen** unterschätzen die tatsächlichen Kosten von Cyberangriffen und sehen IT-Sicherheit primär als Kostenfaktor statt als Investition in die Geschäftskontinuität. Häufig wird versucht, durch minimale Budgets oder Insellösungen Geld zu sparen. Die Realität zeigt: Die Kosten für Ausfälle, Datenverlust, rechtliche Folgen und Reputationsschäden übersteigen die vermeintlichen Einsparungen um ein Vielfaches. Ein weiterer Fehler ist, dass Kunden die laufenden Betriebskosten von Sicherheit unterschätzen – sie kalkulieren nur die Lizenzkosten, vernachlässigen aber Aufwände für Betrieb, Monitoring und Incident Response. Managed Security bietet hier Transparenz und Planbarkeit:

## Wesentliche Kennzahlen



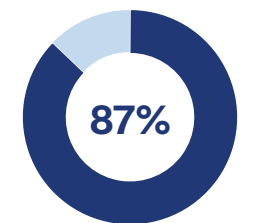
### Human Risk Factor

Mitarbeiter stellen auch Heute noch das grösste Sicherheitsrisiko dar.



### Fachkräftemangel

Mehr als die Hälfte berichten von unbesetzten Positionen in der IT.



### Skill-Gap in der IT

87% der Befragten geben an, dass ihr IT-Personal nicht die notwendigen Security-Kenntnisse besitzt.



# Managed Security

## Intelligenter Security-Service für eine ganzheitliche Verteidigung

**Galaxyweb** liefert eine moderne Sicherheitsplattform, die KI-gesteuerte Automatisierung in den Mittelpunkt stellt. Sie nutzt agentische Intelligenz, um Sicherheitsprozesse ähnlich wie ein menschlicher Analyst zu denken und auszuführen: Alerts werden priorisiert, untersucht und vollautomatisch beantwortet. Diese Hyperautomation ermöglicht Deep Security Reasoning, also fundierte Abwehraktionen auf Maschinengeschwindigkeit. Wir stellen nicht einfach eine Sicherheitslösung bereit, sondern bieten einen Rundum-Service. Wir kombinieren modernste KI mit unserem Know-how, damit Bedrohungen nicht nur erkannt, sondern auch schnell, automatisiert und nachhaltig abgewehrt werden.

### Breite Unterstützung

**Vom Client, zum Server bis in die Cloud:** Unsere Managed Security-Lösung schützt Windows 7–11 und Windows Server 2012R2–2025, macOS ab High Sierra, zahlreiche Linux-Distributionen sowie PaaS-Umgebungen mit Kubernetes. So bleibt Ihre gesamte IT-Landschaft zuverlässig abgesichert und zentral verwaltet über alle Standorte hinweg.

- **Microsoft Windows Clients & Server**
- **Linux Clients & Server**
- **Apple macOS**
- **Kubernetes-Cluster**

### Unsere Security-Bundles

**Unsere Bundles** sind darauf ausgelegt, sich passgenau an die jeweilige Unternehmenssituation anzuschmiegen. Gemeinsam erarbeiten wir die optimale Lösung, damit Ihre Organisation den Schutz erhält, der wirklich benötigt wird.

- **Managed Security Standard**
- **Managed Security Advanced**
- **Managed Security Professional**

### Modulare Bausteine

**Standard und Advanced** lassen sich modular erweitern: Add-ons werden je nach Bedarf, IT-Anforderungen und unserer Empfehlung einzeln ergänzt. Managed Security Professional enthält alle Erweiterungen.

- **Identity Posture: Härting sowie Erkennung von AD-Fehlkonfigurationen**
- **Threat Intelligence: Kontextualisierte Früherkennung von Angriffen**
- **Purple AI: KI-gesteuerte Spracheingabe sowie automatische Untersuchung**
- **Vulnerability Management: Schwachstellenfindung sowie Risikobeurteilung**

## Fokus auf Transparenz

**Wir übernehmen die vollständige Überwachung Ihrer Systeme - standort- und Plattformunabhängig.**

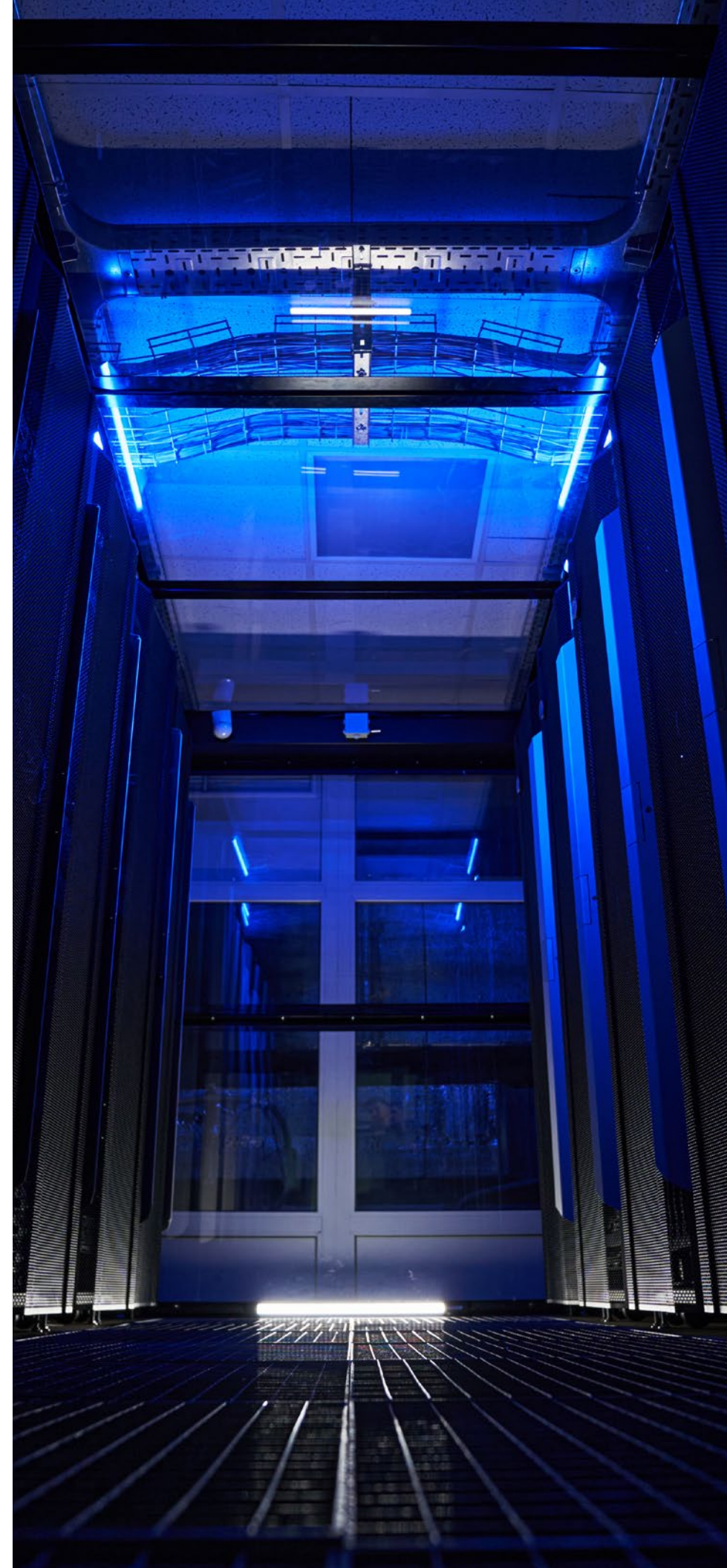
**Transparenz ist die Grundlage** für Vertrauen und nachhaltige Zusammenarbeit. Deshalb erfassen und überwachen wir alle sicherheitsrelevanten Aktivitäten Ihrer Systeme über Standorte, Plattformen und Anwendungen hinweg.

**Die Ergebnisse** stellen wir in regelmäßigen, detaillierten Reports bereit, die nicht nur technische Daten, sondern auch verständliche Handlungsempfehlungen enthalten.

Auf Wunsch gewähren wir Ihnen zusätzlich direkten Zugriff auf unser zentrales Management-System. Damit erhalten Sie jederzeit eine Echtzeitansicht Ihrer gesamten Umgebung und können Sicherheitszustände und Vorfälle unmittelbar mitverfolgen. So behalten Sie stets den vollen Überblick – und wissen genau, wie sicher Ihre IT-Landschaft ist.

**Website:** [galaxyweb.ch](https://galaxyweb.ch)

**Galaxyweb AG, Switzerland**



# Ihre Vorteile

## Mehr Sicherheit, weniger Aufwand

Die Bedrohungslage im Cyberraum verändert sich ständig. Mit Galaxyweb haben Sie einen Partner an Ihrer Seite, der Risiken frühzeitig erkennt, sofort reagieren kann und Ihnen dabei Kostensicherheit sowie Entlastung verschafft. So bleibt Ihre IT jederzeit geschützt – und Ihr Unternehmen zukunftssicher aufgestellt.

**Bei einer Zusammenarbeit mit Galaxyweb** wissen Sie stets, womit Sie rechnen dürfen: Anstelle hoher Einmalinvestitionen in Lizenzen und Hardware, erhalten Sie einen transparenten Service mit planbaren monatlichen Kosten. Dank klarer Servicepakete haben Sie jederzeit Transparenz über Ihre Ausgaben und profitieren gleichzeitig von modernster Sicherheitsinfrastruktur, die sonst nur Grossunternehmen zur Verfügung steht. Unerwartete Ausgaben für Sicherheitsvorfälle werden minimiert – Ihre Budgets bleiben stabil und kalkulierbar.

**Entlastung der internen IT** – Durch die Übernahme der laufenden Updates der Sicherheitslösung, die Bereitstellung von Empfehlungen sowie das Management von Sicherheitsvorfällen entlastet Galaxyweb Ihr IT-Team und schafft Freiraum für wichtige Projekte im Unternehmen.

In den allermeisten Fällen fehlt der internen IT die nötige Tiefe im Umgang mit modernen Bedrohungen. Oft ist unklar, wie Frühzeichen zu erkennen und richtig zu interpretieren sind, wie man auf akute Risikosituationen reagiert oder welche Schritte bei einer Sicherheitsverletzung zwingend einzuleiten sind. Genau hier setzt Galaxyweb an: Wir stellen das Fachwissen, die Erfahrung und die klar definierten Prozesse bereit, damit Sicherheitsvorfälle schnell, strukturiert und wirksam behandelt werden – bevor grösserer Schaden entsteht.

## Ganzheitlicher Ansatz

**IT-Sicherheit ist kein einmaliges Projekt**, sondern ein kontinuierlicher Prozess. Damit Unternehmen dauerhaft geschützt bleiben, braucht es eine klare Struktur: Risiken rechtzeitig vorbeugen, Bedrohungen zuverlässig erkennen und im Ernstfall sofort reagieren.

Galaxyweb bündelt diese drei Schritte in einem umfassenden Managed Security-Ansatz. Darüber hinaus unterstützen wir Unternehmen auch in angrenzenden Bereichen wie Netzwerkdesign und -segmentierung, Firewalling, Backupkonzepten, Business Continuity sowie Disaster Recovery. Diese Punkte sind nur ein kleiner Ausschnitt unserer Leistungen und keineswegs abschliessend – je nach Bedarf entwickeln wir gemeinsam mit Ihnen individuelle Lösungen, die perfekt zu Ihrem Unternehmen passen.



## Rundum abgesichert - und transparent begleitet

**Mit Galaxyweb Managed Security erhalten Sie einen ganzheitlichen Schutz**, der weit über herkömmliche Sicherheitslösungen hinausgeht. Unsere Plattform überwacht Server, Arbeitsplätze und Cloud-Umgebungen kontinuierlich und reagiert in Echtzeit auf Bedrohungen. Modernste Technologien sorgen dafür, dass Angriffe zuverlässig erkannt und automatisch blockiert werden, bevor Schaden entsteht. Transparente Reports und auf Wunsch der direkte Zugang zu unserem Management geben Ihnen jederzeit volle Kontrolle und Einblick. So entsteht eine vertrauensvolle Partnerschaft, die Ihre digitale Sicherheit nachhaltig stärkt und Ihnen die Freiheit gibt, sich auf Ihr Kerngeschäft zu konzentrieren.

- **Erkennung in Perfektion:** Wir erreichen eine überragende Erkennungsrate von 100 %, wie in den unabhängigen 2024 MITRE ATT&CK® Evaluations bestätigt – unsere Lösung entdeckt alle simulierten Angriffe sofort und ohne Verzögerung auf Windows, Linux und macOS.
- **Automatisierte Blockierung:** Über 99,84 % der Bedrohungen werden vollautomatisiert gestoppt – für den Rest stehen unsere Experten bereit, um alle Fälle zu bearbeiten und Hintertüren zu schliessen. Die Plattform reagiert autonom mit automatischer Isolierung, One-Click-Rollback und umfassender Storyline-Forensik, die den gesamten Angriffspfad nachvollziehbar darstellt.

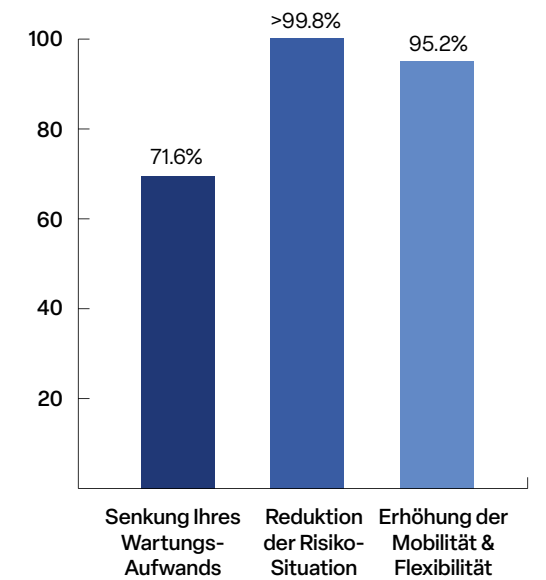
## Ohne Kompromisse

**Die Leistungsfähigkeit lässt sich belegen:** 100 % Abdeckung im MITRE ATT&CK Framework, eine drastische Reduktion von Fehlalarmen und sofortige Erkennung in allen Angriffsszenarien. So gewinnen unsere Kunden maximale Sicherheit – ohne Rauschen, ohne Verzögerung.



## Spürbare Ergebnisse

**Die durchschnittlichen Ergebnisse** belegen eine spürbare Reduktion des Wartungsaufwands, eine deutliche Risikominimierung sowie mehr Flexibilität.



## Zufriedenheit:

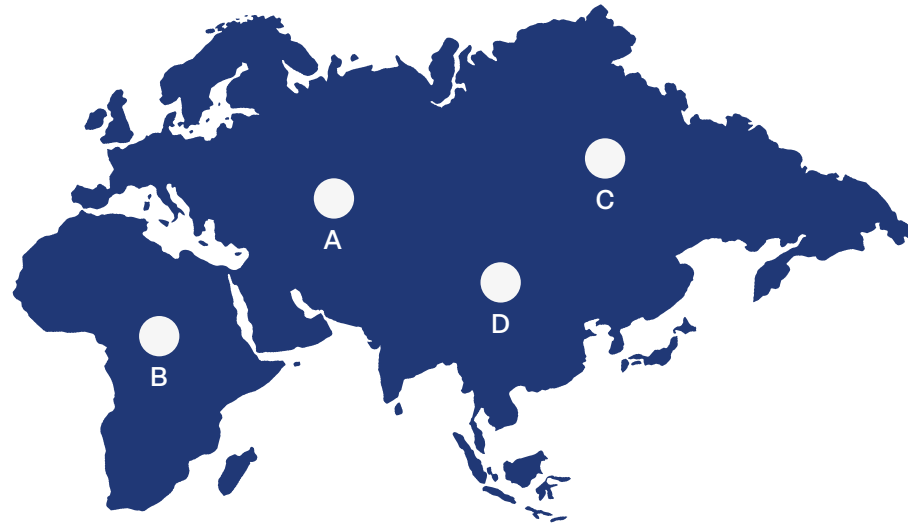


# Roadmap zur Einführung

In nur vier Schritten erhöhen wir die Endpunktsicherheit Ihrer Systeme in kürzester Zeit deutlich und schaffen zugleich mehr Sichtbarkeit und senken Ihren Aufwand.

## 4 SCHRITTE

- 1: Gewünschte Produktwahl
- 2: Einrichtung Ihres Tenants
- 3: Trainierung der künstlichen Intelligenz
- 4: Bereinigungen und Optimierungen



## Unkomplizierte Implementierung

**Die Einführung erfolgt schnell und unkompliziert.** Auch Unternehmen, die sich bereits in einem akuten Sicherheitsvorfall befinden, können sofort auf unsere Lösung setzen und innerhalb kürzester Zeit Schutz erhalten. Sie wählen einfach das gewünschte Paket, wir richten Ihre persönliche Managed Security-Umgebung vor. Die Installation auf Arbeitsgeräten erfolgt entweder durch Sie oder – auf Wunsch – durch uns. Anschliessend übernimmt unsere KI die Analyse der gesamten Umgebung. Wir kümmern uns um Bereinigungen, Optimierungen und stellen sicher, dass Ihre Systeme sofort bestmöglich geschützt sind.

Nach der schnellen Implementierung stehen Ihnen zahlreiche Funktionen zur Verfügung – darunter Device Protection, lokales Firewall-Management und viele weitere Sicherheits-Features. Gemeinsam mit Ihnen planen wir die nächsten Schritte, priorisieren die relevanten Funktionen und passen die Konfiguration gezielt an Ihre Unternehmensanforderungen an.

## Granulare Einstellungen pro Standort & System

- **Individuelle Standortbereiche:** Für jeden Standort richten wir einen eigenen Bereich ein, in dem alle Geräte verwaltet und mit individuellen Sicherheitsrichtlinien versehen werden können.
- **Fein abgestufte Systemgruppen:** Die Systeme werden nach Bereichen aufgeteilt - z.B. Clients, virtuelle Server, PaaS, DMZ, Produktion oder mobile Endgeräte. So lassen sich Richtlinien zielgenau anwenden.
- **Vielfältige Sicherheits-Tools:** Mit Managed Security steuern wir pro Bereich gezielt Funktionen wie Device Control (USB/Thunderbolt/Bluetooth), lokales Firewall-Management, Application Control und Rogue Device Discovery. So bleibt Ihre Umgebung flexibel geschützt.

## Add-ons

**Unsere Pakete** lassen sich jederzeit flexibel mit Add-ons erweitern. So ergänzen wir gezielt zusätzliche Sicherheitsfunktionen, genau abgestimmt auf Bedarf und Unternehmensanforderungen.

### Identity Posture

Fehlkonfigurationen erkennen und ID-Services stärken.

### Threat Intelligence

Früherkennung von Threats und Kontextualisierung von Bedrohungen.

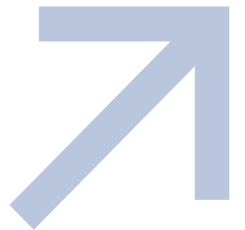
### Purple AI

Natürliche KI-Spracheingabe mit automatischer Untersuchung und Rekonstruktionen.

### Vulnerability Management

Schwachstellenüberwachung und risikobasierte Priorisierung der Anwendungen.

## Unsere gemeinsame Sicherheitsreise



## Vertrauen, Sicherheit und Zukunft im Fokus

**Cybersicherheit endet nicht mit der Einführung einer neuen Lösung.** Die Bedrohungslandschaft entwickelt sich täglich weiter, Angriffe werden raffinierter und gezielter, und Unternehmen müssen Schritt halten, um ihre Werte und Daten zu schützen. Mit Managed Security von Galaxyweb stellen wir sicher, dass Ihre IT-Umgebung nicht nur heute, sondern auch morgen den höchsten Sicherheitsstandards entspricht.

Unser Ansatz verbindet modernste Technologie mit kontinuierlicher Überwachung und praxisnaher Expertise. Wir verstehen die individuellen Herausforderungen, vor denen Unternehmen in unterschiedlichen Branchen stehen, und passen unsere Sicherheitskonzepte gezielt an. So entsteht eine Lösung, die nicht nur zuverlässig funktioniert, sondern sich auch flexibel mit Ihrem Unternehmen weiterentwickelt. Besonders wichtig ist uns dabei die Transparenz. Sie behalten jederzeit den Überblick über den Sicherheitsstatus Ihrer Systeme, erhalten regelmässige Reports und können auf Wunsch in Echtzeit Einblick in unsere Management-Plattform nehmen.

So entsteht nicht nur technischer Schutz, sondern auch Vertrauen – eine Grundvoraussetzung für langfristige Zusammenarbeit. Abschliessend möchten wir unterstreichen: IT-Sicherheit ist keine lästige Pflicht, sondern ein entscheidender Erfolgsfaktor für jedes Unternehmen.

**Galaxyweb AG**  
Sonnenburgweg 10  
8215 Hallau SH - Schweiz

Hotline CH: 0800 80 80 00  
Email: support@galaxyweb.ch  
www.galaxyweb.ch

**GALAXYWEB AG**  
**Security Report 2025**  
galaxyweb.ch

