Cybersecurity Leaders Fonds

Sicherheit wird Pflicht

Souveränität zum Vorteil

Jahresbericht 2025 & Strategie 2026

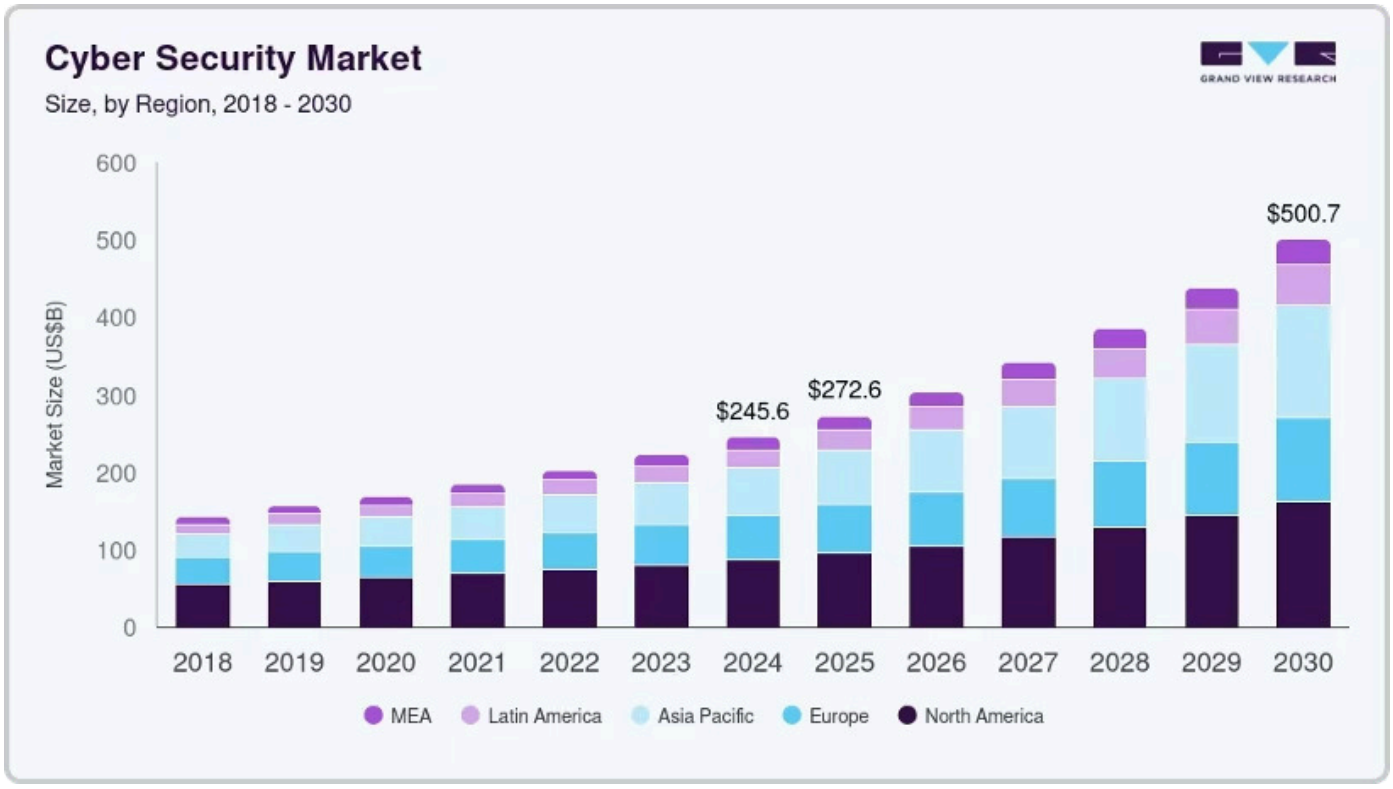
Vom Wahlfach zur Pflichtaufgabe: Digitale Resilienz als Fundament der Transformation

Sehr geehrte Anlegerinnen und Anleger,

das Jahr 2025 hat gezeigt: **Cybersecurity ist keine Option mehr.** Digitale Resilienz ist heute für Unternehmen ebenso überlebenswichtig wie Liquidität oder physische Sicherheit.

In den vergangenen zwölf Monaten ist Cybersecurity vom IT-Budget in die Vorstandsagenda aufgestiegen. Die durchschnittlichen Kosten einer Datenpanne erreichten 2025 mit **6.08 Millionen US-Dollar** einen neuen Höchststand - ein Anstieg von 10 Prozent gegenüber dem Vorjahr. Unternehmen, die in Cybersecurity investieren, schützen nicht nur ihre Daten, sondern ihre gesamte Existenzgrundlage.

Vor diesem Hintergrund ist es nicht überraschend, dass für den gesamten Cybersecurity-Markt weiterhin ein starkes Wachstum prognostiziert wird – Schätzungen gehen hier von einem jährlichen Marktwachstum zwischen 12 und 15 Prozent aus.



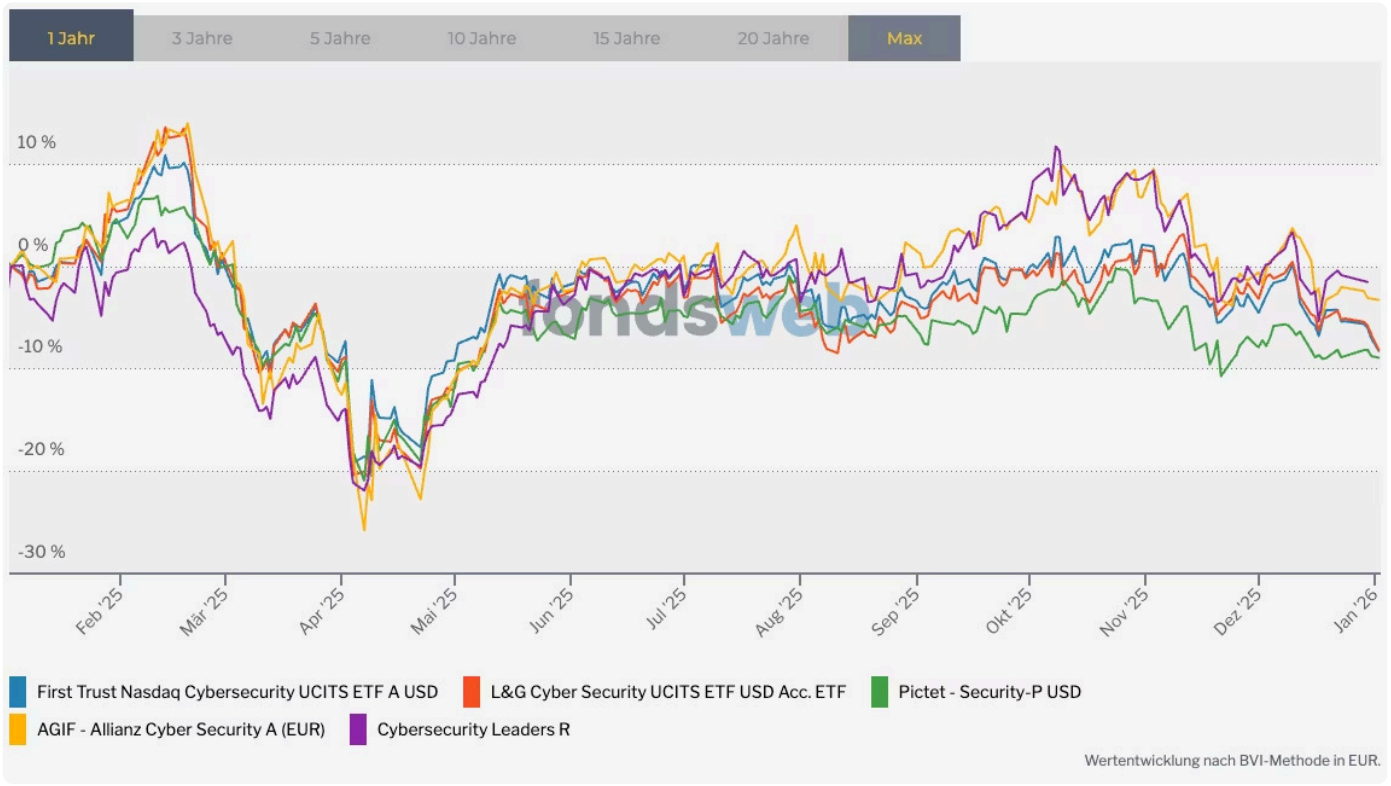
Quelle: grandviewresearch

Jahresperformance 2025 im Peergroup Vergleich

Der gesamte Cybersecurity-Sektor stand 2025 unter erheblichem Marktdruck. In diesem schwierigen Umfeld haben wir im Vergleich zur Peer-Group zwar sehr gut abgeschnitten, dennoch bleibt die absolute Rendite enttäuschend. Sie liegt aktuell weit hinter der durchschnittlichen Performance von 20 % pro Jahr zurück, die ich mit dieser Strategie bisher erzielen konnte. Die folgenden Chart-Vergleiche verdeutlichen diese Entwicklung im Branchenvergleich.

Annualisiert | Kumuliert

	1 Jahr	3 Jahre
First Trust Nasdaq Cybersecurity UCITS ETF A USD	-4,85%	+17,16%
L&G Cyber Security UCITS ETF USD Acc. ETF	-4,71%	+17,20%
Pictet - Security-P USD	-7,83%	+8,74%
AGIF - Allianz Cyber Security A (EUR)	-2,17%	+21,68%
Cybersecurity Leaders R	+1,00%	n.v.



https://www.fondsweb.com/de/vergleichen/tabelle/isins/IE00BF16M727,IE00BYPLS672,LU0256846139,LU2286300715,DE000A3D0588

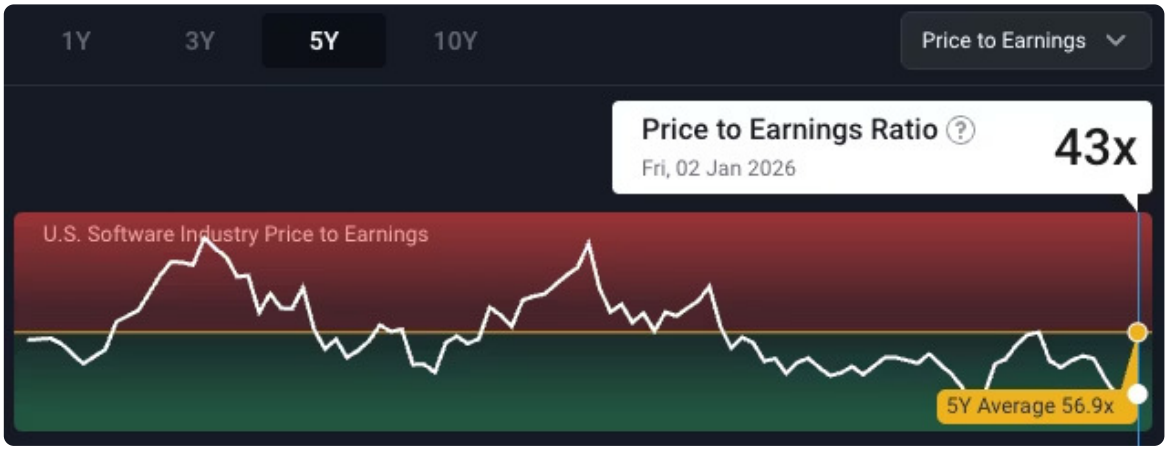
Marktanalyse: Bewertungskonsolidierung trifft auf strukturelles Wachstum

Sektor-Performance und Bewertungsniveau

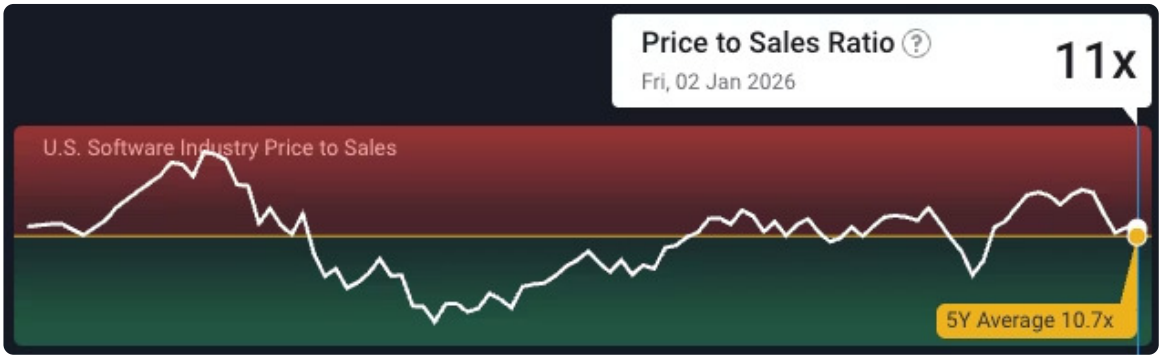
Die Underperformance des Cybersecurity-Sektors im Jahr 2025 hat zu einer attraktiven Bewertungskonsolidierung geführt. Während die Aktienkurse stagnierten, haben die Treiber - die verschärfte Bedrohungslage, die fortschreitende Cloud-Transformation und vor allem die massive Regulierungswelle - kontinuierlich an Kraft gewonnen.

Diese Divergenz zwischen Kursentwicklung und Fundamentaldaten hat einen **Bewertungsstau** erzeugt, der für 2026 erhebliches Aufholpotenzial signalisiert. Die Forward-KGVs der führenden Pure-Play-Anbieter notieren aktuell 15 bis 25 Prozent unter ihren historischen Durchschnittswerten - eine Situation, die wir zuletzt 2019 beobachtet haben, unmittelbar vor einer signifikanten Sektor-Rally.

Durchschnitts KGV der US Software Industrie in 5 Jahren:



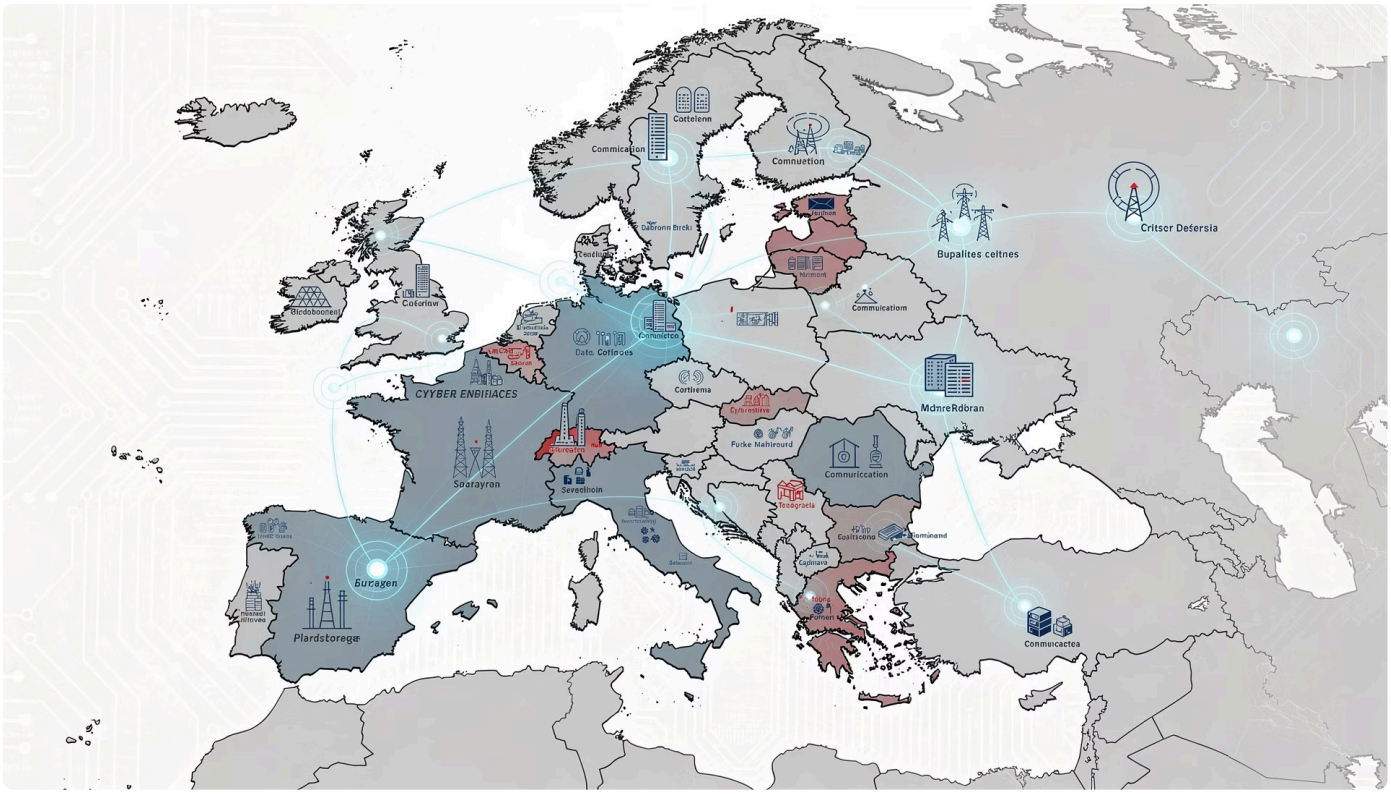
Durchschnitts KUV der US Software Industrie in 5 Jahren:



Geopolitische Katalysatoren

Die geopolitische Lage hat sich 2025 als starker Katalysator für Cybersecurity-Investitionen erwiesen. Staatlich gesponserte Cyberoperationen haben ein neues Niveau erreicht. Die Vorfälle im Baltikum - einschließlich der dokumentierten Angriffe auf kritische Unterwasser-Infrastruktur - haben europäischen Entscheidungsträgern die Verwundbarkeit digitaler und physischer Infrastrukturen vor Augen geführt.

Diese Ereignisse haben den politischen Willen zur Stärkung der digitalen Souveränität massiv beschleunigt. Der Cybersecurity Leaders Fonds ist 2026 positioniert, um von diesem Wandel zu profitieren: Unsere Investments umfassen sowohl die defensiven Technologien, die Unternehmen zur Absicherung benötigen, als auch die offensiven Kapazitäten, die staatliche Akteure und kritische Infrastrukturbetreiber nachfragen.



Einige Positionen, die 2025 aktiv im Cyber Defence-Bereich gehandelt worden sind, sind Airbus, Thales und Clavister. Clavister bleibt weiterhin Bestandteil des Fonds.

Regulatorisches Umfeld: Der europäische Investitionszwang

Die regulatorische Landschaft hat sich 2025 von der Vorbereitungs- in die Umsetzungsphase bewegt. Drei zentrale EU-Regelwerke definieren nun einen rechtlich verbindlichen Rahmen für Cybersecurity-Investitionen:

DORA (Digital Operational Resilience Act)

Mit Inkrafttreten im Januar 2025 verpflichtet DORA Finanzinstitute zu umfassenden Maßnahmen der digitalen Resilienz. Die Verordnung betrifft mehr als 22.000 Finanzunternehmen in der EU - von Großbanken bis zu Vermögensverwaltern. Die Anforderungen umfassen regelmäßige Penetrationstests, Incident-Response-Pläne und die Überwachung von Drittanbietern. Für den Cybersecurity Leaders Fonds bedeutet dies: Ein regulatorisch garantierter Absatzmarkt für Security-Operations-Plattformen und Threat-Intelligence-Dienste.

NIS2-Richtlinie

Ein wesentlicher Wachstumstreiber für 2026 ist das seit dem 6. Dezember 2025 in Deutschland verbindliche NIS2-Umsetzungsgesetz. Damit weitet sich der Kreis der regulierten Unternehmen allein in Deutschland massiv auf rund 30.000 Betriebe aus - europaweit sind es schätzungsweise 160.000. Entscheidend für die Marktdynamik ist dabei das neue Haftungsregime: Die persönliche Haftung des Managements bei Verstößen rückt Cybersecurity endgültig in den Fokus der Vorstandsebene. Dieser regulatorische Rahmen schafft einen faktischen Investitionszwang, der weit über bisherige Standards hinausgeht und die Nachfrage nach Sicherheitslösungen langfristig absichert.

Cyber Resilience Act

Der Cyber Resilience Act adressiert erstmals systematisch die Sicherheit von IoT-Geräten und vernetzten Produkten. Hersteller müssen künftig Security-by-Design nachweisen und über den gesamten Produktlebenszyklus Sicherheitsupdates bereitstellen. Diese Anforderungen schaffen neue Märkte für Embedded Security, sichere Entwicklungspraktiken und Compliance-Monitoring-Lösungen.

Investment-Highlight: Strategische Neuausrichtung mit Fokus auf Europa

Der Investment Case OVHcloud

Ein wesentlicher Meilenstein meiner Strategie im Jahr 2026 ist die signifikante Erhöhung des Anteils europäischer Infrastruktur- und Security-Anbieter. Die Wiederaufnahme von OVHcloud in das Portfolio illustriert diese Ausrichtung.

In einem Marktumfeld, in dem Datensouveränität zu einem harten Wettbewerbsvorteil wird, besetzt das französische Unternehmen eine Schlüsselrolle. Als europäischer Cloud-Anbieter mit Zertifizierungen wie SecNumCloud - dem höchsten Sicherheitsstandard der französischen ANSSI - profitiert OVHcloud unmittelbar von den Anforderungen aus NIS2 und DORA.

Dieses hohe Sicherheitsniveau wird durch die Zusammenarbeit mit Partnern wie Airbus und der NATO validiert, die bei ihren Projekten unter anderem auf die souveräne Cloud-Infrastruktur von OVHcloud vertrauen.

01

Regulatorischer Burggraben

Europäische Unternehmen und Behörden sind zunehmend gezwungen, auf Infrastrukturen zu setzen, die nicht dem US Cloud Act unterliegen. Während US-Provider gesetzlich verpflichtet werden können, Daten an US-Behörden herauszugeben, bietet OVHcloud einen rechtlich abgesicherten Raum innerhalb der EU.

02

Investitionszwang als Wachstumshebel

Die steigenden Anforderungen an die digitale Belastbarkeit führen zu einem automatischen Investitionsbedarf. Unternehmen müssen ihre Infrastruktur absichern, um Bußgelder und persönliche Haftungsrisiken für das Management zu vermeiden.

03

Souveränitätsprämie

Die zunehmende Nachfrage nach europäischer digitaler Souveränität schafft eine Prämie für zertifizierte Anbieter, die OVHcloud als First Mover nutzen kann.

Portfolio-Strategie: Der Trend-in-Trend-Ansatz

Die Investmentphilosophie des Cybersecurity Leaders Fonds basiert auf dem **Trend-in-Trend-Ansatz**: Wir identifizieren aufkommende Sub-Sektoren innerhalb des Cybersecurity-Megatrends, bevor sie vom breiten Markt erkannt werden. Dieser Ansatz hat sich bewährt - von der frühen Identifikation von Cellebrite im Jahr 2021 bis zur zeitgerechten Positionierung in Rubrik nach dem CrowdStrike-Vorfall 2024.

Aktuelle Schwerpunkte im Portfolio

KI-gestützte Threat Detection

CrowdStrike bleibt eine Kernposition im Portfolio. Die Falcon-Plattform hat sich als führende Lösung für KI-gestützte Bedrohungserkennung etabliert. Analysten von Wedbush haben CrowdStrike kürzlich als eines der Top-Investments im KI-Bereich identifiziert - eine Einschätzung, die unsere langjährige Überzeugung bestätigt. Die Integration von generativer KI in die Charlotte-AI-Funktionen positioniert das Unternehmen an der Spitze der nächsten Evolutionsstufe der Cybersecurity.

Zero Trust und Netzwerksicherheit

Zscaler und **Palo Alto Networks** repräsentieren unsere Überzeugung im Bereich Zero-Trust-Architekturen. Der Wechsel von perimeterbasierten zu identitätsbasierten Sicherheitsmodellen ist unumkehrbar - beschleunigt durch hybride Arbeitsmodelle und die Auflösung traditioneller Unternehmensgrenzen. Beide Unternehmen profitieren zudem von der Cloud-Migration, die Unternehmen zu einer Neukonzeption ihrer Sicherheitsarchitektur zwingt.

Data Protection und Backup Security

Rubrik adressiert die „letzte Verteidigungslinie“: die schnelle Wiederherstellung nach Angriffen. Da Ransomware gezielt Backups attackiert, ist Datensicherung heute ein kritischer Security-Perimeter. Die Vorfälle der letzten Jahre haben gezeigt, dass diese Fähigkeit existenziell ist..

Digital Forensics und Investigation

Palantir und Micro Systemation bilden eine differenzierte Säule für digitale Ermittlungen. Der Bedarf an Aufklärungstools wächst durch die geopolitische Lage und strengere Compliance-Vorgaben rasant – sowohl bei Behörden als auch in Konzernen. Diese Titel geben dem Portfolio eine Tiefe, die weit über reine Abwehrsoftware hinausgeht.

Risikomanagement: Die Options-Overlay-Strategie

Ein wesentliches Differenzierungsmerkmal (neben der Dividende in Höhe der Vorabsteuerpauschale) des Cybersecurity Leaders Fonds ist die aktive Risikomanagement-Strategie durch den Einsatz von Optionen.

Downside Protection

Durch den systematischen Einsatz von Put-Optionen auf Index-Ebene begrenzen wir das Abwärtsrisiko in Marktkorrekturphasen.

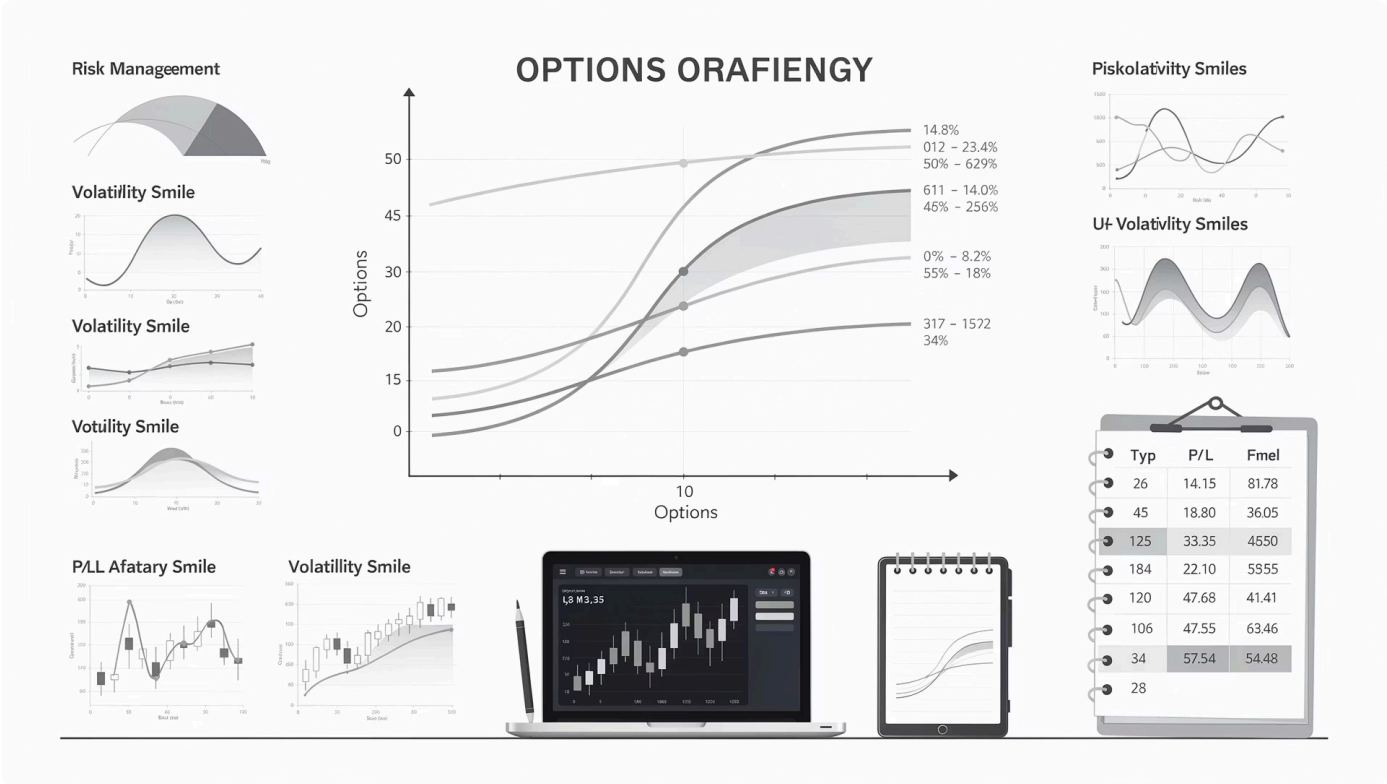
Income Generation

Der Verkauf von Covered Calls auf ausgewählte Positionen generiert zusätzliche Erträge und senkt die effektive Kostenbasis.

Volatilitätsnutzung

Die erhöhte Volatilität im Tech-Sektor bietet attraktive Prämien, die wir systematisch vereinnahmen.

Diese Strategie hat im Jahr 2025 zu einer Reduktion der Portfolio-Volatilität beigetragen und wird 2026 weiter optimiert.



Ausblick 2026: Katalysatoren und Positionierung

Die Treiber für eine Neubewertung des Cybersecurity-Sektors sind intakt. Für 2026 sehen wir folgende Schlüsselkatalysatoren:

Treiber	Status 2025	Ausblick 2026
Bewertung	Konsolidiert und historisch günstig	Potenzial für Multiple-Expansion
Regulatorik	Vorbereitungsphase, NIS2-, DORA-Fristen	Operative Umsetzung, Sanktionsdruck
KI-Integration	KI als Angriffsbeschleuniger	KI als unverzichtbares Verteidigungstool
Geopolitik	Eskalation hybrider Kriegsführung	Erhöhte Investitionen in kritische Infrastruktur
Markt-Sentiment	Abwartend und vorsichtig	Rückkehr des Kapitals in Mission-Critical IT

Strategische Prioritäten für 2026

Für das kommende Jahr setze ich auf folgende Prioritäten:

01

Europäische Souveränität

Weitere Aufstockung von Positionen, die von der EU-Souveränitätsagenda profitieren.

02

KI-Security

Fokussierung auf Anbieter, die KI sowohl in ihre Produkte als auch in ihre Bedrohungserkennung integrieren.

03

Identitäts- und Zugriffsmanagement

Ausbau von Positionen im Zero-Trust-Segment angesichts der Auflösung traditioneller Netzwerkperimeter.

04

Deepfake-Detection und Media Security

Frühe Positionierung in einem Segment, das durch generative KI explosives Wachstumspotenzial zeigt.

Fazit und Ausblick

Wir starten in das Jahr 2026 mit einem Portfolio, das die US-Innovationskraft bei **AI-Security** und Threat Detection mit der regulatorischen Stabilität europäischer Anbieter verbindet. Mein Ziel ist es, den Fonds genau dort zu positionieren, wo technologische Marktführerschaft auf gesetzlich verankerte Absatzmärkte trifft. Die Kombination aus attraktiven Bewertungen und regulatorischem Rückenwind schafft ein Umfeld, das aktives Management belohnt.

Dabei ist eines klar: Die gesamte **KI-Revolution** steht und fällt mit der Sicherheit. Ohne den Schutz von Daten und Modellen ist generative KI im Unternehmenseinsatz schlicht nicht nutzbar.

Cybersecurity ist somit das Fundament, auf dem die KI-Transformation überhaupt erst stattfinden kann – das gilt für die Software ebenso wie für die physische Basis in Form von **Rechenzentren und AI-Fabriken**.

Cybersecurity bleibt die einzige IT-Infrastruktur, die nicht zyklisch, sondern existenziell notwendig ist. Da digitale Resilienz zum entscheidenden Faktor für Erfolg und Überleben geworden ist, bietet der Cybersecurity Leaders Fonds eine fokussierte, aktiv gemanagte Beteiligung an diesem Markt.

Herzlichen Dank für Ihr Vertrauen.

Dirk Althaus
Fondsmanager, Cybersecurity Leaders Fonds

Beispielhafte Transaktionen 2025: Aktives Risikomanagement in der Praxis

Anbei einige Transaktionen aus dem Jahr 2025. Die Übersicht zeigt (Teil-)Käufe, (Teil-)Verkäufe sowie die erzielten Ergebnisse unserer aktiv gemanagten Positionen. Hierbei wird deutlich, wie die Stop-Loss-Strategie funktioniert.

Palantir

Unrealisierter Gewinn	-40.177,21 €
Realisierter Gewinn	1.329.132,01 €
Dividenden (brutto)	0 €
Summe	**1.288.954,81 €**

Zscaler

Unrealisierter Gewinn	-147.548,76 €
Realisierter Gewinn	335.093,70 €
Dividenden (brutto)	0 €
Summe	**187.544,95 €**

JFrog

Unrealisierter Gewinn	132.164,92 €
Realisierter Gewinn	142.114,03 €
Dividenden (brutto)	0 €
Summe	**274.278,95 €**

CrowdStrike

Unrealisierter Gewinn	-137.585,08 €
Realisierter Gewinn	532.164,23 €
Dividenden (brutto)	0 €
Summe	**394.579,15 €**

CoreWeave

Unrealisierter Gewinn	—
Realisierter Gewinn	409.581,93 €
Dividenden (brutto)	0 €
Summe	**409.581,93 €**

Cisco

Unrealisierter Gewinn	201.419,32 €
Realisierter Gewinn	20.718,09 €
Dividenden (brutto)	0 €
Summe	**222.137,41 €**