

# Cyber Security: Wie es jetzt weitergeht

Wir präsentieren die Ergebnisse unserer globalen Marktstudie Pulse 2023: konkrete Antworten für MSSPs, um die Herausforderungen von heute zu meistern.

**W / T H**®  
secure



# Einleitung

WithSecure™ Pulse 2023 ist eine globale Marktstudie, zu der 3.072 IT-Experten aus 12 verschiedenen Ländern befragt wurden. Die Teilnehmer waren Entscheidungsträger und Meinungsführer in den Bereichen IT, Netzwerke und Cloud, verantwortlich für den Kauf von IT-Sicherheitsprodukten und -dienstleistungen für ihre Unternehmen.

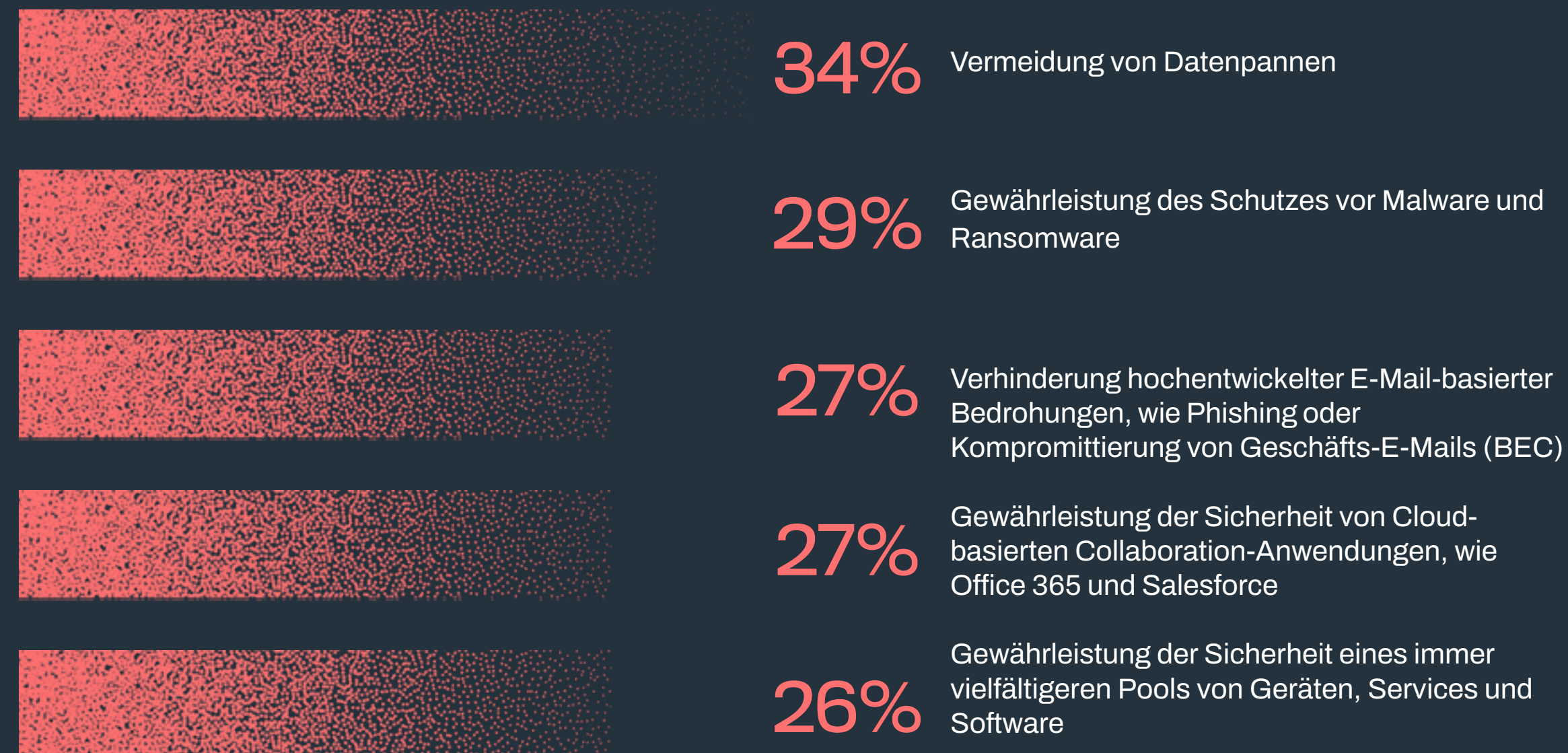
Wir haben ihnen eine Reihe von Fragen zu ihren Prioritäten und Besorgnissen für 2023 gestellt und Themen wie Datenpannen, Anbieterwechsel und Ausgaben für Sicherheit diskutiert.



# Prioritäten für 2023

Die Ergebnisse unserer Pulse 2023-Umfrage zeigen eine breite Übereinstimmung zwischen den Verantwortlichen für Cybersicherheit über die Bedeutung der Erkennung von und Reaktion auf Bedrohungen. Das wichtigste Anliegen ist die Verhinderung von Datenschutzverletzungen, gefolgt von der Notwendigkeit, sich vor Ransomware und Malware zu schützen.

## Die Top 5 der technischen Prioritäten für 2023



## Die Top 5 Sicherheitsherausforderungen für Unternehmen



## Woran es fehlt

Peter Page, Leiter der Abteilung Solution Consulting bei WithSecure™, meint, dass genau das, was für die Sicherheit eines Unternehmens am wichtigsten ist, oft nicht zu den Top-Prioritäten des Unternehmens gehört. Wie Page sagt, "sind dies erfahrungsgemäß die Kompetenzen und Praktiken, die in vielen Organisationen fehlen".

Bei der Zusammenarbeit mit Kunden müssen Sie herausfinden, welche Kompetenzen im Bereich Cybersicherheit fehlen, und diese mit den aktuellen Prioritäten vergleichen. Fehlende Kompetenzen sind oft wichtiger als vermeintliche Prioritäten. Helfen Sie Ihren Kunden, indem Sie diese fehlenden Kompetenzen abdecken.

WithSecure™ Elements ist unsere cloudbasierte Cybersicherheitsplattform, die Risiken, Komplexität und Ineffizienz reduziert. Sie umfasst die Bereiche Endpoint Protection (EPP), Endpoint Detection and Response (EDR), Schwachstellenmanagement und Collaboration Protection – ein komplettes Paket an Funktionen, das alle Sicherheitsanforderungen Ihrer Kunden erfüllt. Mit Elements können unsere Partner auch ihre eigenen Dienste hinzufügen, um ein noch besseres Produkt für ihre Kunden zu schaffen.



# Datenpannen

Die Verhinderung von Datenpannen wurde in unserer Pulse 2023-Umfrage als wichtigste technische Priorität genannt. Allerdings waren die Meinungen von IT-Meinungsführern und -Entscheidern zu diesem Thema geteilt.

## Kontroverse Meinungen

44 % der IT-Influencer stufen die Verhinderung von Datenpannen als ihr wichtigstes Problem ein, aber nur 29 % der IT-Entscheider stimmten dem zu. 38 % der Befragten aus dem Top-Management stufen die Verhinderung von Datenpannen ebenfalls als das wichtigste Thema ein, was wiederum bedeutet, dass für IT-Entscheider dieses Thema am seltensten Priorität hat. Wenn Sie mit Ihren Kunden sprechen, sollten Sie sie dazu anhalten, gemeinsam mit ihrem Sicherheitsteam sicherzustellen, dass alle Beteiligten in dieser Frage übereinstimmen.

Wenn es darum geht, Datenpannen zu vermeiden, ist WithSecure™ so konzipiert, dass es wie ein zusätzliches Mitglied Ihres Sicherheitsteams funktioniert, das Ihnen jederzeit zur Verfügung steht. Mit dem Service [Elevate to WithSecure™](#) verfügen Sie über zusätzliches Personal, das Sie bei der Bewältigung der herausforderndsten Fälle unterstützt. Unser Bekenntnis zu einem 24/7-Support verleiht WithSecure™ ein Alleinstellungsmerkmal.

# Anbieterwechsel

Der Anbieterwechsel im Sicherheitsbereich ist keine triviale Aufgabe. Vielmehr erfordert dies einen erheblichen Aufwand an Zeit und Ressourcen. Daher ist es schon überraschend, dass über 30 % der Teilnehmer an unserer Pulse 2023-Umfrage ihren Sicherheitsanbieter innerhalb der letzten sechs Monate gewechselt haben und weitere 30 % dies in den nächsten sechs Monaten vorhaben. Warum also dieser massive und anhaltende Wechsel?

## Kosten sind nicht der springende Punkt

Die Gründe für einen Anbieterwechsel liegen nicht allein im Kostenbereich. Nur 13,2 % der Befragten sagten, der Preis sei für sie der wichtigste Faktor. 21,8 % maßen hingegen dem 24/7-Support die größte Bedeutung zu, während 16,7 % das Vertrauen in den Anbieter als wichtigstes Kriterium nannten.

Einer der Faktoren für einen Anbieterwechsel ist, dass der Umstieg immer einfacher wird. Bis vor kurzem erschien vielen Unternehmen der Wechsel des Sicherheitsanbieters so kompliziert und zeitaufwändig, dass sie kaum dazu bereit waren – auch nicht bei suboptimaler Leistung ihres Anbieters. Heute sind Benutzer mit dem Prozess vertrauter und daher eher zu einem Wechsel bereit, wenn sie nicht ganz zufrieden sind.

Wenn Sie mit einem potenziellen Kunden über einen Anbieterwechsel sprechen, empfehlen Sie ihm, sich möglichst frühzeitig zu entscheiden, idealerweise mindestens 12 Monate vor Ablauf seines Vertrags. Nach unserer Erfahrung gelingen Anbieterwechsel am besten mit einer Vorlaufzeit von 1 Jahr oder länger.

# Das Sicherheitsbudget

Für viele Unternehmen sind Kosten der wichtigste Aspekt bei der Cybersicherheit. Das bedeutet nicht unbedingt, so wenig wie möglich auszugeben, sondern eher, das beste Preis-Leistungsverhältnis zu erzielen. Unsere Umfrage zeigt, dass die Kosten bei der Entscheidungsfindung im Bereich der Cybersicherheit eine immer geringere Rolle spielen.

## Höhere Ausgaben für Sicherheit

Bis 2024 wird der Markt für Informationssicherheit weltweit voraussichtlich 174,7 Mrd. Dollar wert sein. Dies deutet darauf hin, dass viele Unternehmen auf die verschärften Risiken reagieren, indem sie ihre Ausgaben für Cybersicherheit erhöhen.

Diese Aussage wird durch unsere Pulse 2023-Umfrage bestätigt. 87,9 % der in der EU ansässigen Befragten gaben an, dass sie in den nächsten 12 Monaten eine Erhöhung ihrer Sicherheitsausgaben planen. Aber 8,3 % der Befragten denken, dass ihr Unternehmen bereits ausreichend geschützt ist, oder überlegen, ihr Budget für Cybersicherheit zu kürzen.

## “Wie viel sollte ich für Cybersicherheit ausgeben?”

Diese Frage treibt viele IT-Experten um. Laut Paul Brucciani, Head of Product Marketing bei WithSecure™, hängt die Entscheidung von diversen Faktoren ab, z. B. wie viel Risiko das Unternehmen bereit ist zu akzeptieren und wie viel an Betriebsstörungen es in Kauf nehmen kann.

Teemu Myllykangas, Director of B2B Product Management bei WithSecure, meint dazu: "Ich sage immer, man sollte mit einem absoluten Minimum von 5 % beginnen. Eines gilt dabei uneingeschränkt: Je wichtiger die Sicherheit für den Kunden ist, desto höher ist der Prozentsatz. Und umgekehrt."

Dieser Prozentsatz ist allerdings nicht allgemeingültig. Laut Brucciani geben Unternehmen, die Sicherheit als besonders wichtig einstufen, in der Regel 12-15 % des IT-Budgets für Cybersicherheit aus. Das belegt einmal mehr, dass es hier keine Zauberformel gibt, sondern dass dies von vielen und für jedes Unternehmen individuellen Faktoren abhängt.

WithSecure™ unterstützt Sie dabei, indem wir die jährliche Verlusterwartung des Unternehmens, die Wahrscheinlichkeit eines Zwischenfalls im Bereich der Cybersicherheit und die zu erwartenden Folgen eines Worst-Case-Szenarios errechnen. Anhand dessen können wir ermitteln, wie viel Ihr Unternehmen für die Cybersicherheit ausgeben sollte.

Unabhängig von den Ausgaben Ihrer Kunden für Sicherheit bietet WithSecure™ flexible Preismodelle, die sich an die jeweiligen Bedürfnisse anpassen, darunter eine Jahreslizenz, ein monatliches Abonnement und nutzungsbasierte Sicherheit.

# Fazit

Die Pulse 2023-Umfrage zeigt, dass der Schutz von remote und hybrid tätigem Personal für viele Unternehmen eine der größten Sicherheitsherausforderungen ist, ebenso wie schnellere und effektivere Reaktionen auf Cybersicherheitsvorfälle. WithSecure™ Elements eignet sich dank der kraftvollen prädiktiven, präventiven und reaktionsschnellen Sicherheitsfunktionen optimal für beide Aufgaben.

Als Partner können Sie mit nur einer WithSecure™-Plattform viele Kunden zugleich effizient betreuen und so eine betriebliche Effizienz erreichen, die andere Anbieter nicht liefern können.

Darüber hinaus sind Endpoint Protection und Endpoint Detection and Response kraftvolle Tools zur Vermeidung von Datenpannen – Top-Priorität von Sicherheitsexperten. Sie sind auch hochwirksam gegen Ransomware und Malware sowie gegen hochentwickelte E-Mail-basierte Bedrohungen wie Phishing.

WithSecure™ Elements Collaboration Protection bietet zuverlässige Sicherheit für Cloud-basierte Kollaborationsanwendungen wie Office 365 und Salesforce. Mit WithSecure™ Elements Vulnerability Management wird die Sicherheit vieler Geräte, Dienste und Software einfach und intuitiv gewährleistet.

WithSecure™ Elements wurde mit unseren Partnern und für sie entwickelt, um die Aktivierung zusätzlicher Dienste maximal zu

vereinfachen. Wir haben die Technologie mit unserem eigenen Managed Detection & Response-Team entwickelt und wissen daher, wie erstklassiger Service-Design-Support abläuft. So sind wir der ideale Partner für MSSPs, die ihre eigenen Services auf unserer Technologie aufbauen wollen.

Wenn Sie sich für das WithSecure™-Partnerprogramm entscheiden, um in Sachen Cybersicherheit die Weichen neu zu stellen, haben Sie auch Zugang zu Elevate to WithSecure™, dem 24/7-Support-Service, den kein anderer Anbieter leistet.

Das WithSecure-Partnerprogramm bietet eine umfassende Kompetenzentwicklung für Ihre nächsten Schritte als Managed Service Provider. Wir bieten eine breite Palette von Cross- und Up-Selling-Möglichkeiten mit nahtlosen Produkt- und Serviceoptionen, die wir laufend weiterentwickeln.

Die Pulse 2023-Umfrage gibt Aufschluss über Prioritäten, Bedenken und Erwartungen von IT-Experten für das kommende Jahr. Als Mitglied des WithSecure™-Partnerprogramms sind Sie in einer einzigartigen Position, diese Anliegen zu erfüllen und die Erwartungen zu übertreffen. Zögern Sie nicht, uns zu kontaktieren, wenn Sie mehr zur Umfrage wissen wollen.

Niemand kann Cybersecurity-Probleme alleine lösen, aber wenn wir zusammenarbeiten, können wir eine sicherere Welt schaffen.

## Stärken Sie Ihr Geschäft als Managed Service Provider

Werden Sie der vertrauenswürdige Partner, den Ihre Kunden suchen, und bauen Sie Ihr Geschäft aus, indem Sie WithSecure™ Elements as a managed service anbieten.

# Über WithSecure™

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endgeräte und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

