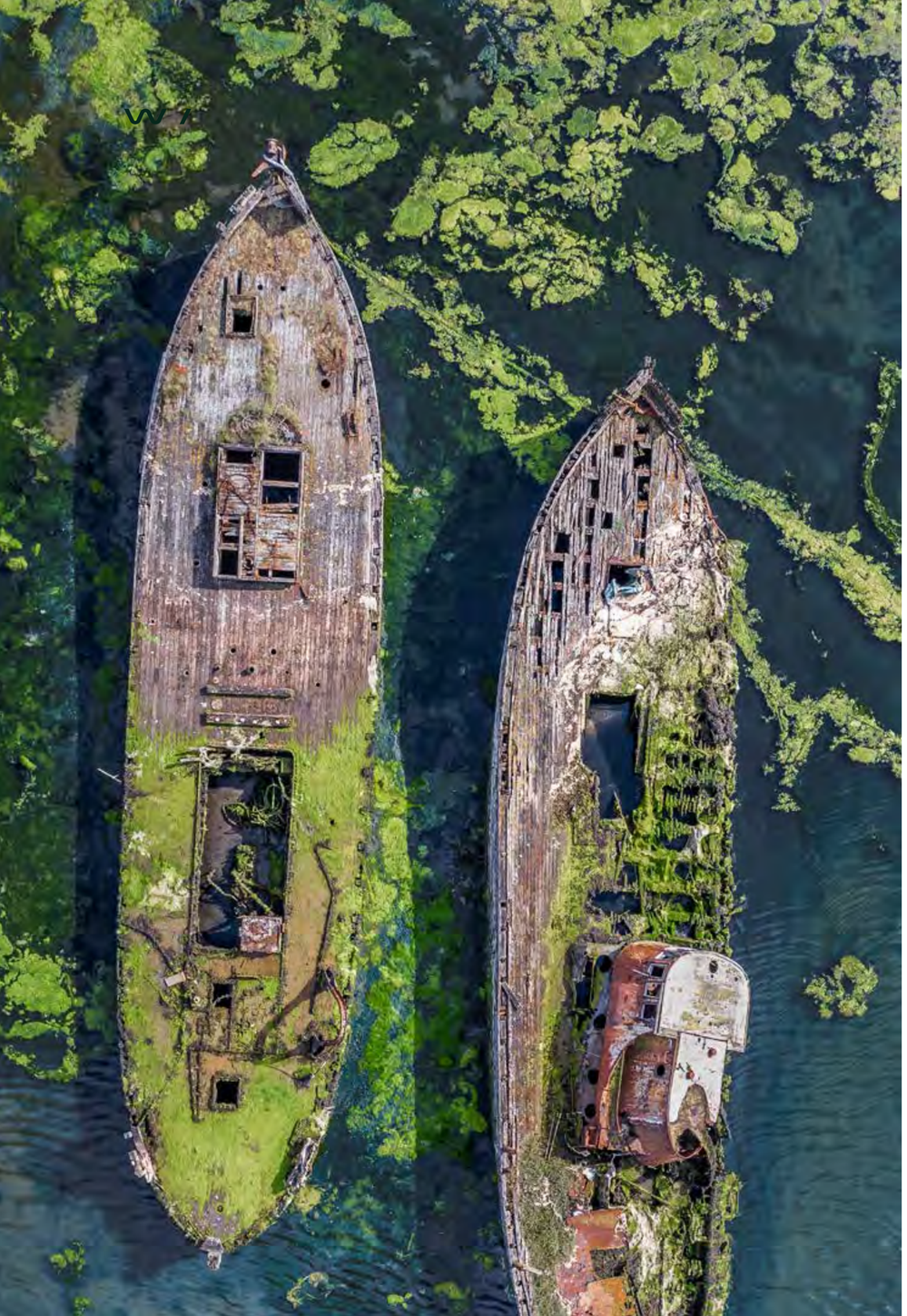
Broschüre

Verwaltung der Cloud-Sicherheitslage
Die Vorteile für Sie

WITH secure



Warum Verwaltung der Cloud-Sicherheitslage eine Notwendigkeit ist

Über 90 % der Unternehmen fahren eine hybride Multi-Cloud-Strategie. Die Vorteile des Cloud Computing liegen auf der Hand: mehr Flexibilität, weniger Einsatz an knappen Ressourcen, besserer Support, und teilweise wird auch die Gewährleistung der Sicherheit einfacher. Aber es gibt auch Risiken – nicht zuletzt, weil die geteilte Verantwortung für die Sicherheit eine.potentielle Fehlerquelle ist.

Fehlkonfigurationen sind die Hauptursache für Datenpannen, und nach unseren Untersuchungen sind sie die häufigste Ursache für größere Cloud-Sicherheitsvorfälle. Gartner prognostiziert: "Bis 2025 werden 90 % der Unternehmen, die die Nutzung der öffentlichen Cloud nicht kontrollieren, sensible Daten vorschriftswidrig weitergeben."

Zur Erkennung von Fehlkonfigurationen gibt es Tools von Cloud-Anbietern. Um effektiv zu sein, müssen diese aber fachgerecht konfiguriert und verwaltet werden. Experten für Cloud-Sicherheit sind jedoch rar, darum sind die Produkte schwer zu warten, und Nutzer können ihre Ergebnisse kaum interpretieren. Erschwerend hinzu kommt die behördliche Nachweispflicht, dass die Sicherheitskontrollen für Daten in der Cloud funktionieren. Das Sicherheitsrisiko in der Cloud wird oft durch regelmäßige Audits kontrolliert.

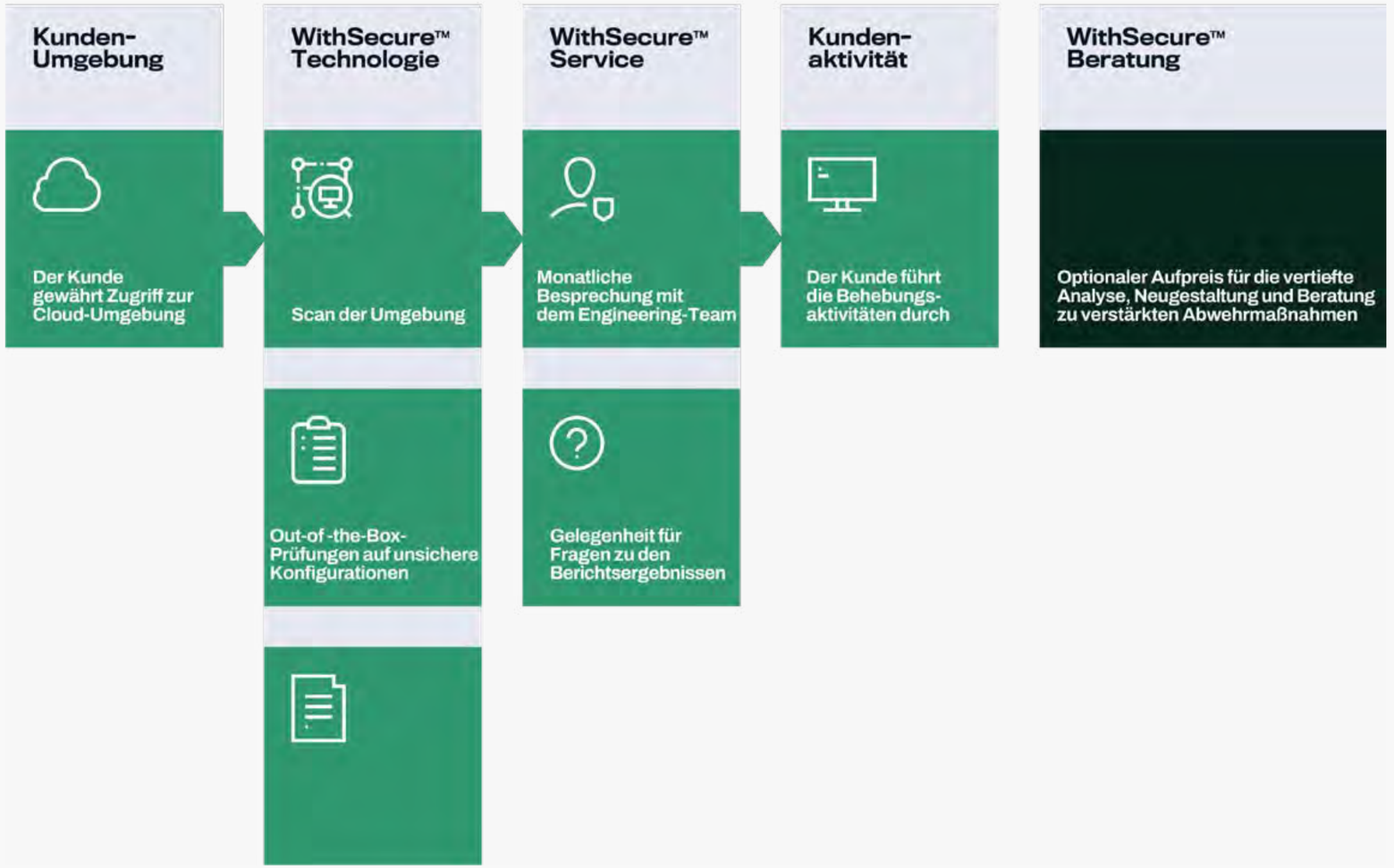
> **“ Bis 2025 werden 90 % der Unternehmen, die die Nutzung der öffentlichen Cloud nicht kontrollieren, sensible Daten vorschriftswidrig weitergeben."**
>
> Gartner

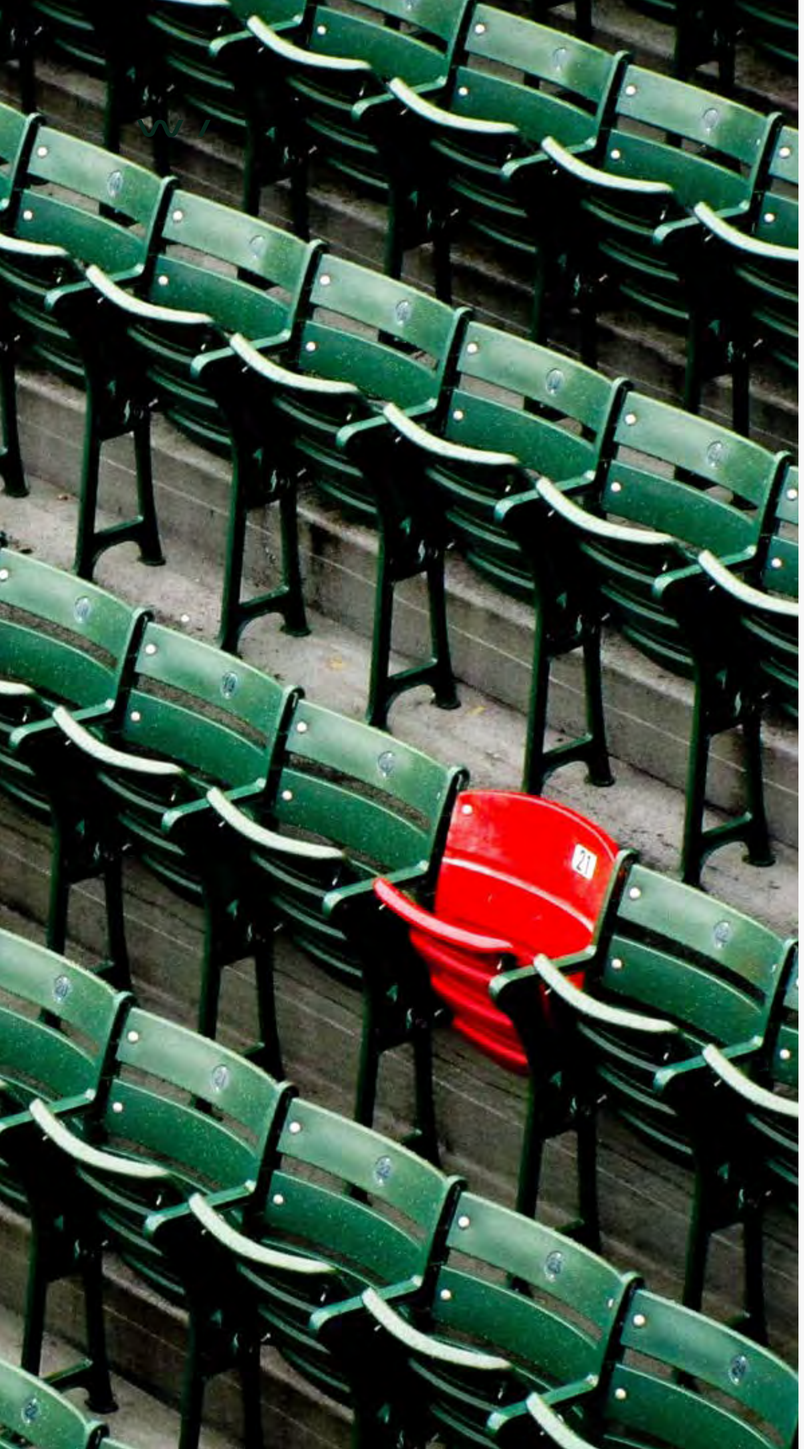
Wie können Unternehmen effektive Kontrollen zur Sicherung der Cloud gewährleisten?

Der Countercept Cloud Security Posture Management (CSPM) Service von WithSecure liefert die Antwort:

- **Partnerschaft in der Sicherheitstechnik,** um Sie bei der Folgenabschätzung von Fehlkonfigurationen und bei der Implementierung sicherer Konfigurationen zu unterstützen
- **Abschreckungswirkung** durch kontinuierliche Optimierung der Sicherheit, die Ihr Unternehmen für Angreifer unattraktiv macht
- **Gewähr für Wirtschaftsprüfer und Aufsichtsbehörden,** dass die Kontrollen für Cloud-Sicherheitsrisiken und Unternehmensführung angemessen sind

So funktioniert der Countercept CSPM-Service von WithSecure





Warum wir CSPM als Service anbieten

CSPM-Lösungen kommen in einer verwirrenden Vielfalt auf den Markt, meist als einfache, leicht zu implementierende SaaS-Lösungen. Sie benötigen allerdings quasi ein Studium, um den Output zu verstehen und die richtigen Sicherheitsentscheidungen zu treffen. Wir bei WithSecure™ finden, dass Unternehmen ihre Sicherheitslage am besten mit einem Service verwalten, der erstklassige Fachkräfte mit unserer eigenen, speziell entwickelten Technologie kombiniert. So lösen wir spezifische, komplexe Probleme, führen schnell Innovationen ein und decken konsequent den Bedarf unserer Kunden ab. Unser CSPM-Service basiert auf drei Säulen:

1. **Sicherheit durch Partnerschaft:** Wir stellen Ihnen einen Security Engineer zur Seite, der sich mit Ihrer Umgebung auskennt und hilft, Fehlkonfigurationen und deren Auswirkungen zu erkennen sowie Ihr Cloud-Sicherheitsrisiko einzuschätzen. Das übertrifft bei weitem die Möglichkeiten, die ein Produkt bieten würde.
2. **Unbegrenzter Zugang zu Cloud-Know-how:** Die WithSecure™ Security Engineers helfen Ihnen bei der Priorisierung der Ergebnisse, bieten umsetzbare Schritte zur Behebung unsicherer Konfigurationen und beantworten Ihre Fragen zum Cloud-Konfigurationsmanagement.
3. **Compliance-Garantie durch direkt einsatzbereite Cloud-Sicherheitsprüfungen:** Wir verwenden einen von WithSecure™-Beratern entwickelten Algorithmus speziell für die Sicherung von Cloud-Umgebungen, um Fehlkonfigurationen zu erkennen. Die Prüfungen gehen über Industriestandards und Benchmarks hinaus, da sie durch Erfahrungen aus härtester Praxis geprägt sind. Wir verbessern unseren Service kontinuierlich, um veränderte Standards, neue Angriffsmethoden und die Weiterentwicklung der zugrunde liegenden Cloud-Plattform zu berücksichtigen.

Hauptmerkmale

Die von dem Tool bereitgestellten Hinweise lassen sich verwenden, um die Einhaltung von Richtlinien und Standards für die Cybersicherheit in Ihrem Unternehmen nachzuweisen. Die folgenden Prüfungen können zum Beispiel zur Anpassung an die NIST-Anforderung für PR.DS-1 verwendet werden: Data-at-rest ist geschützt:

- API-Gateway-Stufen-Cache-Daten werden verschlüsselt
- S3-Buckets sind öffentlich zugänglich
- EBS-Volume ist verschlüsselt
- ElasticSearch-Domain ist im Ruhezustand verschlüsselt
- SQL-Datenbanken erlauben unbeschränkten Datenverkehr
- Azure-Speicherkonto verwendet keine Infrastrukturverschlüsselung

Hauptmerkmale unseres Countercept CSPM-Services

Merkmal	Inklusive
Monatlicher Scan der AWS-Cloud-Umgebung	✓
Monatlicher Bericht	✓
Monatlicher Re-Scan (auf Wunsch)	✓
Monatliches 1-stündiges Treffen mit einem persönlichen Security Engineer	✓
Anfragen an den Security Engineer (Obergrenze für Fair Use = 12 pro Quartal)	✓
Laufende Optimierung neuer und bestehender Kontrollen	✓
Beratende Unterstützung bei Analysen und Problembehebung	Optional erhältlich
Sicherheitsprüfungen für andere als AWS-Cloudumgebungen (z. B. Azure)	Als Early-Adopter-Option erhältlich

Hauptmerkmale

Anzahl der Prüfungen: Die AWS-Version umfasst ca. 100 Konfigurationsprüfungen, die gemäß den Vorgaben des Centre of Information Security AWS konzipiert und von Beratern weiterentwickelt wurden. Zu den Prüfungen gehören die Identifizierung von übermäßigen IAM-Privilegien, unverschlüsselten Daten im Ruhezustand, Cloud-Instanzen mit Zugriff auf öffentliche IP-Adressen und die Feststellung, ob die Protokollierung für die Untersuchung von Vorfällen aktiviert ist.

Scan und Re-Scan auf monatlicher Basis: Der Scan wird monatlich durchgeführt, damit Sie zwischen den Berichtszyklen Zeit für die Behebung von Verstößen haben. Sie können auch einen erneuten Scan anfordern, um die Durchführung der Maßnahmen zu kontrollieren.

Persönliche Besprechungen: Die Security Engineers führen monatliche Meetings durch, die auf die Ergebnisse des Berichts, Ihre bevorzugten Themen, Ihr Cloud-Know-how und Ihren Cloud-Reifegrad ausgerichtet sind. Bei diesen Treffen können Sie sich auf das Fachwissen von WithSecure™ stützen, Ihr Wissen über Cloud-Sicherheit erweitern, Ihre Sicherheitslage verbessern und das Bewusstsein für bewährte Verfahren der Cloud-Cybersicherheit schärfen.

Zugang zu einer Vielzahl von Cloud-Sicherheitsressourcen: Als Ihr Partner im Sicherheitsbereich bieten wir Ihnen eine schlanke Methode, um tiefergehende Einblicke von unserem Beratungsteam zu erhalten. Wenn Sie Fachwissen benötigen, das über das Cloud Security Posture Management hinausgeht, z. B. eingehende Analysen Ihrer Cloud-Infrastruktur, Anleitung für ein Re-Design oder Beratung zu Defense-in-Depth-Strategien, dann können Sie sich an WithSecure™ Consulting wenden.

Die von uns angebotenen AWS- und Azure-Fehlkonfigurationsprüfungen finden Sie auf den folgenden Seiten.

Service	Anzahl der Prüfungen	Logging aktiviert	Im Ruhezustand verschlüsselt	Bei der Übertragung verschlüssselt	Integrität & Zertifikat	Secrets-Management & Schlüsselmanagement	Zugangsrichtlinien & -beschränkungen	Öffentlicher Zugang	Versionskontrolle & Nutzung von AWS-Schwachstellen-Scanning	Wiederherstellung - Backups
AWS Certificate Manager (ACM)	1	✓								
API Gateway	4	AWS API.Gateway.1	AWS API.Gateway.5	AWS API.Gateway.2			AWS API.Gateway.4			
AWS Config	3						CIS Section 3.5 AWS Config.1			
Cloudformation	2					✓				
Cloud-Front	6	AWS Cloudfront.5		AWS Cloudfront.3			✓			
CloudTrail	9	CIS Section 3.1 & 3.6 AWS Cloud-Trail.1 & 4	CIS Section 3.7 AWS Cloud-Trail.2		CIS Section 3.2			CIS Section 3.3		
Dynamo-DB	1					AWS DynamoDB.3				
EBS	3		CIS Section 2.2.1					✓		
EC2	5		AWS EC 2.7					AWS EC 2.1 & 9	AWS EC2.8 susceptible to server-side request forgery	

Key: CIS Foundational Benchmark · AWS Security Best Practice · Additional WithSecure™ checks

Service	Anzahl der Prüfungen	Logging aktiviert	Im Ruhezustand verschlüsselt	Bei der Übertragung verschlüssselt	Integrität & Zertifikat	Secrets-Management & Schlüsselmanagement	Zugangsrichtlinien & -beschränkungen	Öffentlicher Zugang	Versionskontrolle & Nutzung von AWS-Schwachstellen-Scanning	Wiederherstellung - Backups
Elastic Container Registry ECR	4		✓				✓ CIS Section 1.16		✓	
ECS	8	✓		✓		✓	✓			
EKS	4	✓					✓	✓		
Elasticbean Stalk	5	✓					✓		✓ AWS Elastic Beanstalk.2 & 8	
Elastic- Search	6	✓ AWS ES.4	✓ AWS ES.1	✓ AWS ES.3					✓ AWS ES.8	
ELB	6	✓ AWS ELB.5						✓	✓	
Guardduty	1	✓ AWS GuardDuty.1								
IAM	5						✓ CIS Section 1 ✓ AWS IAM. 4, 5, 6, &7			
KMS	2					✓ CIS Section 3.8	✓			
RDS	6	✓ AWS RDS.9	✓ CIS Section 3.3 ✓ AWS RDS.4					✓ AWS RDS.1		✓

Key: ✓ CIS Foundational Benchmark ✓ AWS Security Best Practice ✓ Additional WithSecure™ checks

Service	Anzahl der Prüfungen	Logging aktiviert	Im Ruhezustand verschlüsselt	Bei der Übertragung verschlüssselt	Integrität & Zertifikat	Secrets-Management & Schlüsselmanagement	Zugangsrichtlinien & -beschränkungen	Öffentlicher Zugang	Versionskontrolle & Nutzung von AWS-Schwachstellen-Scanning	Wiederherstellung - Backups
Redshift	7	AWS Red- shift. 3 & 4	✓	AWS Redshift.2				AWS Redshift.1		✓
Route53	2	✓					✓			
S3	6	✓	CIS Section 2.1.1 AWS S3.4	CIS Section 2.1.2 AWS S3.5				AWS S3.1		✓
SNS	2		AWS SNS.1					✓		
SQS	2		AWS SQS.1					✓		
VPC	2	CIS Section 3.9 AWS EC2.6	✓				✓			
VPC SECURITY GROUPS	4						CIS Section 5.2 & 5.3 AWS EC2.2 & 18	✓		

Key: CIS Foundational Benchmark · AWS Security Best Practice · Additional WithSecure™ checks

Azure Service	Insgesamt	Im Ruhezustand verschlüsselt	Bei Übertragung verschlüsselt	Secrets- & Schlüssel-management	Zugangsrichtlinien & -beschränkungen	Öffentlicher Zugang	Security Monitoring	Wiederherstel-lung & Backup
Azure Application Service	3		CIS 9.2 & 9.3					
Azure Key Vault	3			CIS 8.1 – 8.4				
Microsoft Defender for Cloud	4						CIS 4.1.1 & 7.1	
Azure Network Security Groups	4					CIS 6.1 – 6.2		CIS 6.4
Azure SQL Database	1					✓		
Azure SQL Server	7		✓			✓	CIS 4.2	✓
Azure Storage Accounts	15	CIS 3.6	CIS 3.1	✓	✓	CIS 8.7	✓	✓
Azure VM	9				✓	✓	✓	
Azure Virtual Networks	3				✓			✓

Key: ✓ CIS Foundational Benchmark ✓ Additional WithSecure™ checks

Wie sich der Service weiterentwickeln wird

Der Service wird sich ständig weiterentwickeln. Folgende Erweiterungen sind geplant:

Die Konfiguration des Azure Active Directory (AD) Services wird ausgewertet, um Benutzer mit überhöhten Rechten zu identifizieren, z. B. Gäste, die externe Benutzer ohne gesonderte Genehmigung zu einem Cloud-Dienst einladen können.

Zusätzliche Überprüfungen zur Begrenzung der Prüfungsergebnisse ermitteln, ob die Verschlüsselung im Ruhezustand und bei der Übertragung angewendet wird. Dies ist wichtig für Kunden, die CIS, HIPAA und andere Compliance-Richtlinien zur Verschlüsselung von Daten einhalten müssen. Das ist besonders für Azure relevant, da einige Konfigurationseinstellungen unter der empfohlenen Version des Transport Layer Security (TLS)-Protokolls liegen, das zur Verschlüsselung von Daten bei der Übertragung verwendet wird.

Außerdem gibt es zusätzliche Prüfungen, die sich an den CIS-Benchmarks orientieren und von unseren Sicherheitsberatern für sinnvoll erachtet werden. Sie umfassen überprivilegierte Benutzer mit direktem Zugang zu Systemen, die ein Risiko für das Unternehmen darstellen, sowie weitere indirekte Zugangskontrollen. Letztere berücksichtigen die Berechtigungen von Anwendungen, die eine Erweiterung des Benutzerzugangs darstellen. Diese Berechtigungen würden bei einer reinen Überprüfung der Benutzerberechtigungen nicht berücksichtigt werden. Wenn Sie etwa Benutzern Zugriff auf Anwendungen gewähren, die auf die Produktion zugreifen, könnte ein potenzieller Angreifer die Verfügbarkeit Ihrer Dienste beeinträchtigen, wenn ein legitimes Benutzerkonto in die falschen Hände gerät.

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 Endpoints 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.

WITH secure