

Brochure

# How cloud security posture management will help you

**W / T H**<sup>®</sup>  
secure



# Why cloud security posture management is needed

Over 90% of enterprises have a hybrid, multi-cloud strategy. The benefits of cloud computing are clear: more flexibility; reduced need for scarce resources; better support and in some respects, security becomes easier. But there are risks: not least because security responsibility is shared, giving rise to errors.

Misconfiguration is the leading cause of data breaches and from our research, it is the most common source of major cloud security incidents. Gartner predicts that “Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.”

Cloud vendors have developed tools to spot misconfigurations, but to be effective, they must be configured and managed by someone skilled. The scarcity of cloud security skills makes products hard to maintain, and users can have difficulty interpreting their outputs. Added pressure also comes from regulators requesting evidence that security controls governing data in the cloud are working. Cloud security risk is often managed by regular auditing.

**“Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.”**

Gartner



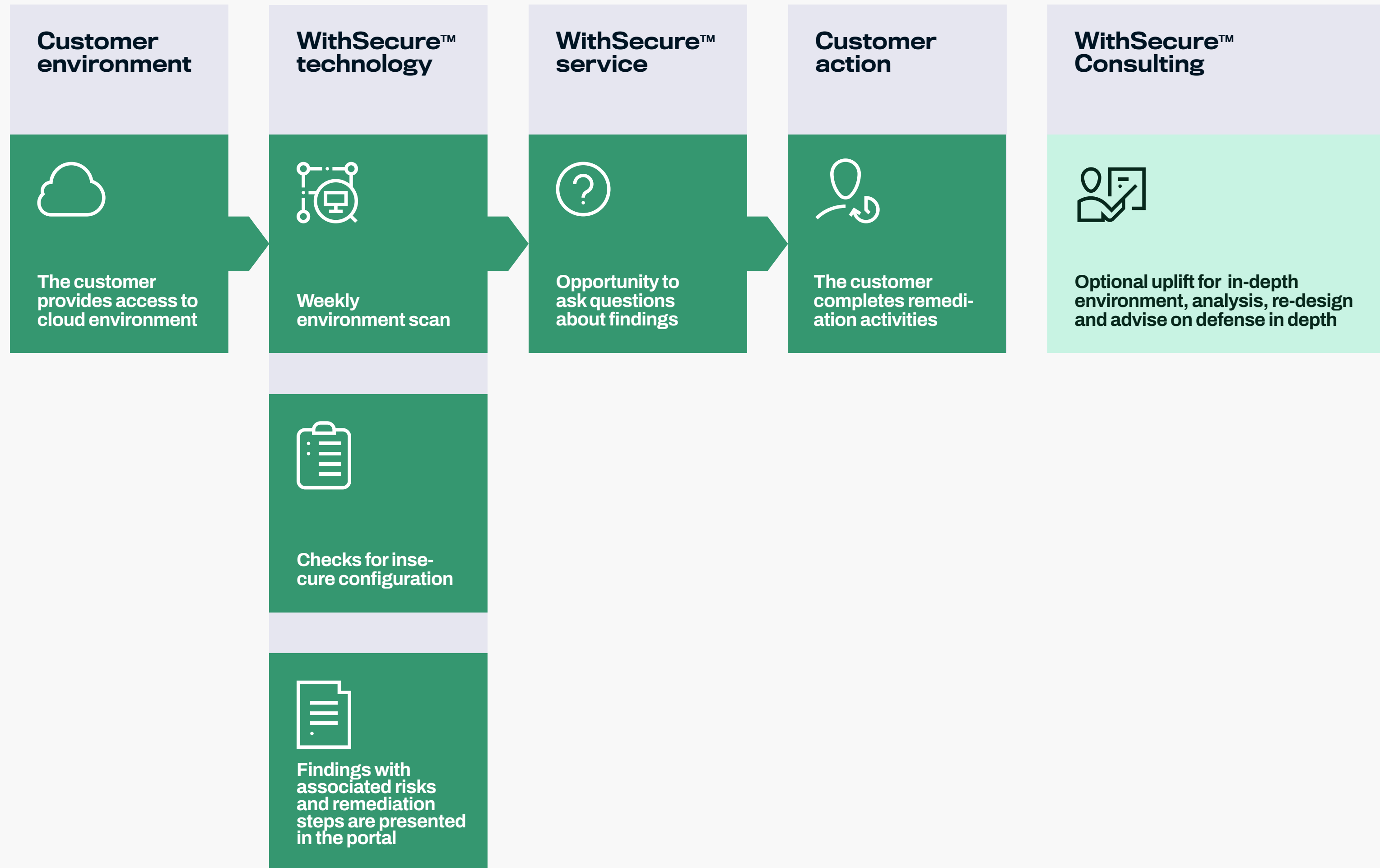
## How can organizations ensure that they have effective controls to secure the cloud?

WithSecure's Countercept Cloud Security Posture Management (CSPM) Service provides the answer:

- **Security engineering partnership** to help you assess the impact of misconfigurations and to implement secure configurations
- **Deterrence value** in the form of on-going security improvements that make your organisation less attractive to attackers
- **Assurance to auditors and regulators** of adequate cloud security risk and governance controls.



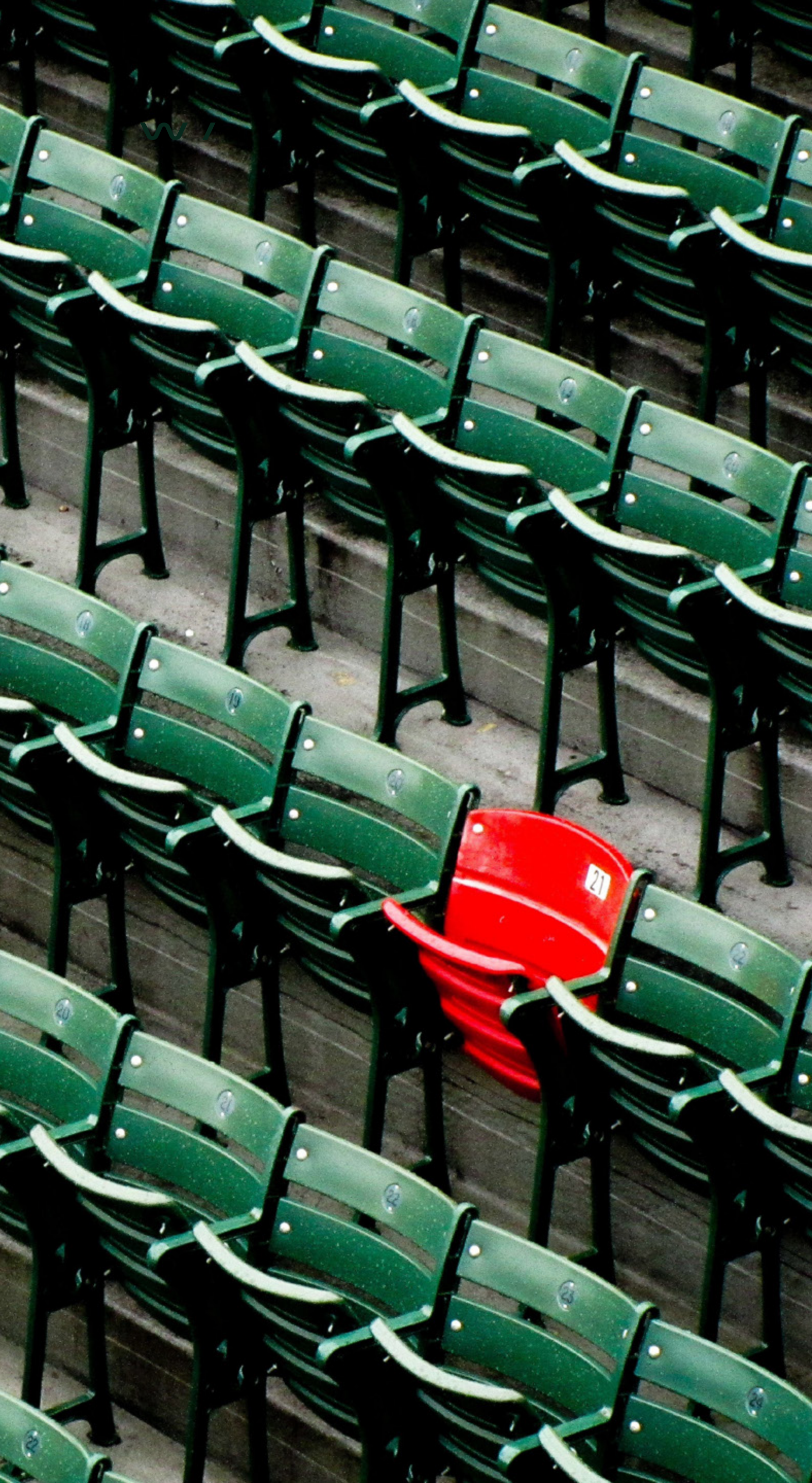
## How WithSecure's Countercept CSPM service works



## Why we deliver CSPM as a service

CSPM solutions on the market come in a bewildering range of flavors. The majority are simple, easy-to-implement SaaS solutions, but they require a PhD to understand their outputs and make sensible security decisions. At WithSecure™, we believe that organisations can best manage their security posture by using a service that combines high-quality people with our own purpose-built technology. By this means we can solve specific complex problems, innovate quickly and to meet consistently our clients' needs. Three pillars define our CSPM service:

- 1. Security through partnership:** an Engineer will be on-hand to answer queries you may have with cloud misconfigurations we identify.
- 2. Keep up with the latest cloud changes:** WithSecure™ is continuously developing new misconfiguration checks, so you don't have to keep an eye on how the secure cloud platform configurations are changing.
- 3. Compliance assurance through cloud security checks:** we will employ an algorithm developed by WithSecure™ consultants that specialize in securing cloud environments to check for misconfigurations. The checks go beyond industry standards and benchmarks as they have been shaped by experience on the front line.
- 4. Supply chain risk management:** with agreement of key suppliers, we will monitor the cloud configurations of services you consume, alerting you to misconfigurations that present risk.



# Key features

The evidence provided by the tool can be used to demonstrate how your organization aligns to cyber security frameworks and standards. For example, the following checks may be used to align to NIST requirement for PR.DS-1: Data-at-rest is protected:

- API Gateway stage cache data is encrypted
- S3 Buckets are publicly accessible
- EBS volume is encrypted
- ElasticSearch domain is encrypted at rest
- SQL Databases allow unrestricted ingress traffic
- Azure storage account does not use infrastructure encryption.

## Key features of our Countercept CSPM service

Feature	Included
<b>Weekly scan of chosen cloud environments</b>	✓
<b>Weekly report available through the portal</b>	✓
<b>Queries to Security Engineer (fair usage cap = 12 per quarter)</b>	✓
<b>Continuous improvement of new and existing checks</b>	✓
<b>Consulting support for analysis and remediation</b>	Available as an option

# Key features

**Checks that matter** - we have circa 150 configuration checks for AWS and Azure. These have been built with security in mind and have been aligned to the Centre of Information Security (CIS) benchmark for AWS and Azure. The checks include identification of overly permissive Identity and Access Management privileges, unencrypted data at rest, cloud instances with access to public IP addresses and whether logging is enabled for incident investigation.

**Scan and re-scan on a weekly basis** – the scan is scheduled to run on a weekly basis to give you time between reporting cycles to remediate activities. You can also request a rescan to confirm if remediation has taken place.

**On-hand configuration expertise:** the ability to ask questions and be guided in managing misconfigurations. The service is an opportunity to lean on WithSecure's expertise and develop your cloud security knowledge and improve your security posture and raise awareness of cloud cyber security best practice.

**Access to a deep well of cloud security resources:** as your security partner, we provide a streamlined method for you to get deeper insight from our consulting team. If you require expertise outside of the scope of Cloud Security Posture Management for example, in-depth analysis of your cloud estate, guidance on a re-design or advice on defense in depth strategies; we provide an option to engage with WithSecure™ Consulting.



The AWS and Azure misconfiguration checks we perform are shown overleaf.

Service	Number of checks	Logging enabled	Encrypted at rest	Encrypted in transit	Integrity & certificate	Secret management & key management	Access policies & restrictions	Public access	Version control & use of AWS vulnerability scanning	Recovery - backups
<b>AWS Certificate Manager (ACM)</b>	1									
<b>API Gateway</b>	4	 AWS API.Gateway.1	 AWS API.Gateway.5	 AWS API.Gateway.2			 AWS API.Gateway.4			
<b>AWS Config</b>	3						 CIS Section 3.5  AWS Config.1			
<b>Cloudformation</b>	2									
<b>Cloud-Front</b>	6	 AWS Cloudfront.5		 AWS Cloudfront.3						
<b>CloudTrail</b>	9	 CIS Section 3.1 & 3.6  AWS Cloud-Traill.1 & 4	 CIS Section 3.7  AWS Cloud-Traill.2		 CIS Section 3.2			 CIS Section 3.3		
<b>Dynamo-DB</b>	1					 AWS DynamoDB.3				
<b>EBS</b>	3		 CIS Section 2.2.1							
<b>EC2</b>	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	Number of checks	Logging enabled	Encrypted at rest	Encrypted in transit	Integrity & certificate	Secret management & key management	Access policies & restrictions	Public access	Version control & use of AWS vulnerability scanning	Recovery - backups
Elastic Container Registry ECR	4		✓				✓ CIS Section 1.16		✓	
ECS	8	✓		✓		✓	✓			
EKS	4	✓					✓	✓		
Elasticbeanstalk	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	✓ AWS RDS.4					✓ AWS RDS.1		✓

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

Service	Number of checks	Logging enabled	Encrypted at rest	Encrypted in transit	Integrity & certificate	Secret management & key management	Access policies & restrictions	Public access	Version control & use of AWS vulnerability scanning	Recovery - backups
Redshift	7	 AWS Red- shift. 3 & 4		 AWS Redshift.2				 AWS Redshift.1		
Route53	2									
S3	6		 CIS Section 2.1.1	 CIS Section 2.1.2				AWS S3.1		
			 AWS S3.4	 AWS S3.5						
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	Total	Encrypted at rest	Encryption in transit	Key and Secret Mgmt	Access policies & Restrictions	Public Access	Security Monitoring	Recovery & Back up
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

## How the service will evolve

The service will continue to evolve over time, our planned capability enhancements are outlined below.

The Azure Active Directory (AD) service configuration will be evaluated to identify users that are overprivileged. For example, guests able to invite external users into a cloud service without your approval.

Additional checks to limit audit findings will identify whether encryption at rest and in transit is applied. This will be valuable for clients that are aligning to CIS, HIPAA and other compliance frameworks that mandate that data should be encrypted. This is particularly relevant for Azure, as some configuration setting defaults fall below the recommended version of the Transport Layer Security (TLS) protocol, used to encrypt data in transit.

Additional checks will be created that align to the CIS benchmarks; those that are deemed to be useful by our Security Consultants. They will cover overprivileged users with direct access to systems that put the organization at risk, and other advanced indirect access checks. Indirect access checks consider permissions of applications, which are an extension of user access. These permissions would not be considered if reviewing the users permissions only. For example, giving users access to applications that access production, in this case a potential attacker could affect your service availability, if a legitimate user account gets into the wrong hands.

Please get in touch if you have any questions about the service.



# Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

Founded in 1988, WithSecure™ (former F-Secure for Business) is listed on the NASDAQ OMX Helsinki Ltd

