

# HOW CLOUD SECURITY POSTURE MANAGEMENT WILL HELP YOU



A person with a backpack is climbing a rocky ridge at sunset. The sky is a mix of orange, yellow, and blue, with clouds visible. The person is in silhouette, wearing a green jacket and dark pants, and is moving upwards on the ridge.

## 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.”

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

- Gartner

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.

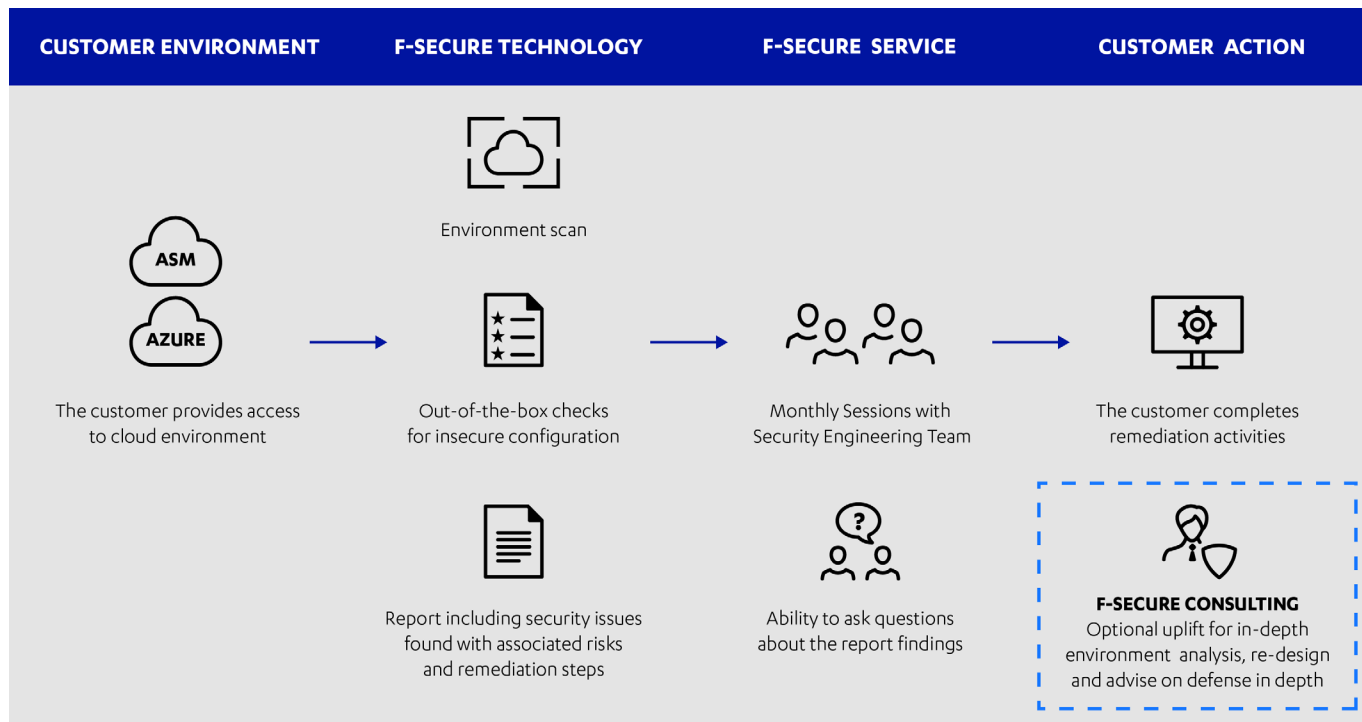
How can organizations ensure that they have effective controls to secure the cloud?

F-Secure'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 F-Secure's Countercept Cloud Security Posture Management (CSPM) service works





## WHY WE DELIVER CSPM AS A SERVICE

CSPM solutions on the market come in a bewildering range of flavours. The majority are simple, easy-to-implement SaaS solutions, but they require a PhD to understand their outputs and make sensible security decisions. At F-Secure, 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:** we will appoint a Security Engineer that understands your environment to assist your understanding of misconfigurations and their impact, to help you assess your cloud security risk, which goes far beyond what a product can offer.
- 2. Unmetered access to cloud configuration expertise:** F-Secure Security Engineers will help you prioritize findings, provide actionable steps to fix insecure configurations and address your cloud configuration management queries.
- 3. Compliance assurance through out-of-the-box cloud security checks:** we will employ an algorithm developed by F-Secure 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. Our service is continuously improved to account for changing standards, new attack methods and evolution of the underlying cloud platform.

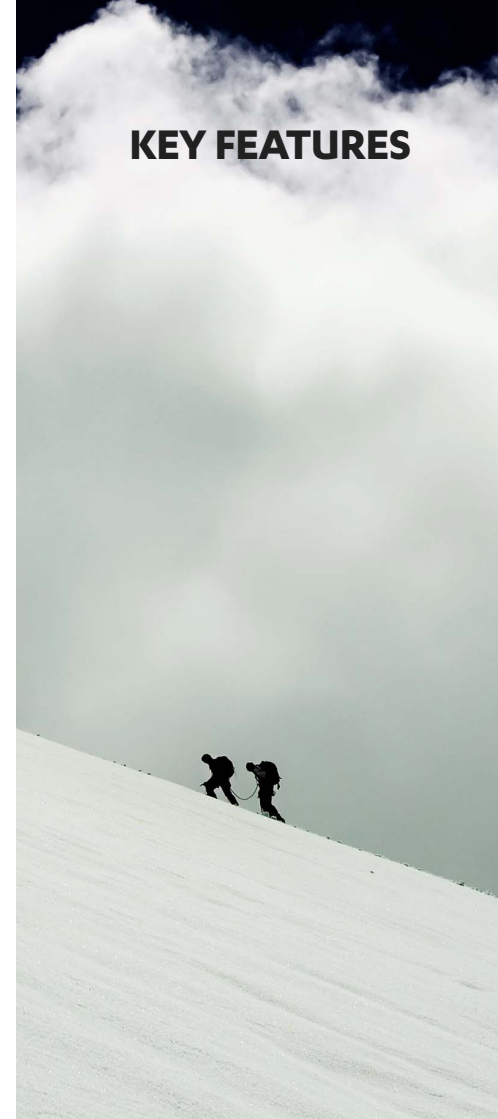
The evidence provided by the tool can be used to demonstrate how your organization aligns to cyber security frameworks and standards. For example, the following checks may be used to align to NIST requirement for PR.DS-1: Data-at-rest is protected:

- API Gateway stage cache data is encrypted
- S3 Buckets are publicly accessible
- EBS volume is encrypted
- ElasticSearch domain is encrypted at rest.

#### Key features of our Countercept CSPM service

FEATURE	INCLUDED
Monthly scan of AWS cloud environment	✓
Monthly report	✓
Monthly re-scan (as requested)	✓
One hour monthly meeting with dedicated Security Engineer	✓
Queries to Security Engineer (fair usage cap = 12 per quarter)	✓
Continuous improvement of new and existing checks	✓
Consulting support for analysis and remediation	Available as an option
Security Assessments for cloud environments other than AWS (e.g. Azure)	Available in Spring 2022

## KEY FEATURES







## KEY FEATURES

**Number of checks** – the AWS version has circa 100 configuration checks. These have been built inline with the Centre of Information Security AWS benchmark and further developed by consultants. The checks include identification of overly permissive IAM 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 monthly basis** – the scan is scheduled to run on a monthly basis to give you time between reporting cycles to remediate activities. You can also request a rescan to confirm if remediation has taken place.
























**Face-to-face session:** Security Engineers will lead a monthly meeting tailored to the findings from the report, your preferential topics, level of cloud expertise and cloud maturity. These meetings are an opportunity to lean on F-Secure'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 F-Secure Consulting.

The AWS misconfiguration checks we perform are shown overleaf.

























The Azure misconfiguration checks are coming in Spring 2022 and will be included.

Key:  CIS Foundational Benchmark       AWS Security Best Practice       Additional F-Secure 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
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									
CloudFront	6	 AWS Cloudfront.5		 AWS Cloudfront.3						
CloudTrail	9	 CIS Section 3.1 & 3.6  AWS Cloud-Trait.1 & 4	 CIS Section 3.7  AWS Cloud-Trait.2		 CIS Section 3.2			 CIS Section 3.3		
DynamoDB	1					 AWS DynamoDB.3				
EBS	3		 CIS Section 2.2.1							
EC2	5		 AWS EC2.7					 AWS EC2.1 & 9	 AWS EC2.8 susceptible to server-side request forgery	



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	✓					✓	✓		
Elasticbean Stalk	5	✓					✓		✓ AWS Elastic Beanstalk.2 & 8	
ElasticSearch	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 2.3.1 ✓ AWS RDS.4					✓ AWS RDS.1		✓

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 Redshift. 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			

## ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

**[f-secure.com/business](https://f-secure.com/business) | [twitter.com/fsecure](https://twitter.com/fsecure) | [linkedin.com/f-secure](https://linkedin.com/f-secure)**

