Zscaler™ CSPM

zscaler™

Table of Contents

Introduction

We live in a fast-changing world. Every industry is undergoing a digital transformation, making software an integral part of any business. To stay competitive, new applications need to be developed quickly and the public cloud is the only environment that supports the necessary pace of change.

Yet, security, risk, and business leaders continue to battle the following problems:

1. Data breaches resulting from misconfigurations of cloud infrastructure continue to expose enormous amounts of confidential customer data, leading to legal liability and financial losses.
2. Continuous compliance for cloud-based workloads is impossible to achieve using traditional on-premises tools and processes.
3. Challenges implementing cloud governance (visibility, policy enforcement across business units, lack of knowledge about cloud security controls) continue to increase as cloud adoption grows within the organization.

This paper reviews the growing gap between the speed of cloud application development and lagging security enforcement, including native security assurance solutions from cloud providers which offer only basic capabilities. We discuss the need for enhanced, dynamic visibility into security posture and seamless collaboration between security and development teams to enforce security standards.

> “It isn’t so much about whether the cloud is secure…It’s mostly about how securely you are using it.
>
> **- Gartner**

The Cloud Requires a Different Security Approach

Data breaches have a significant impact on business

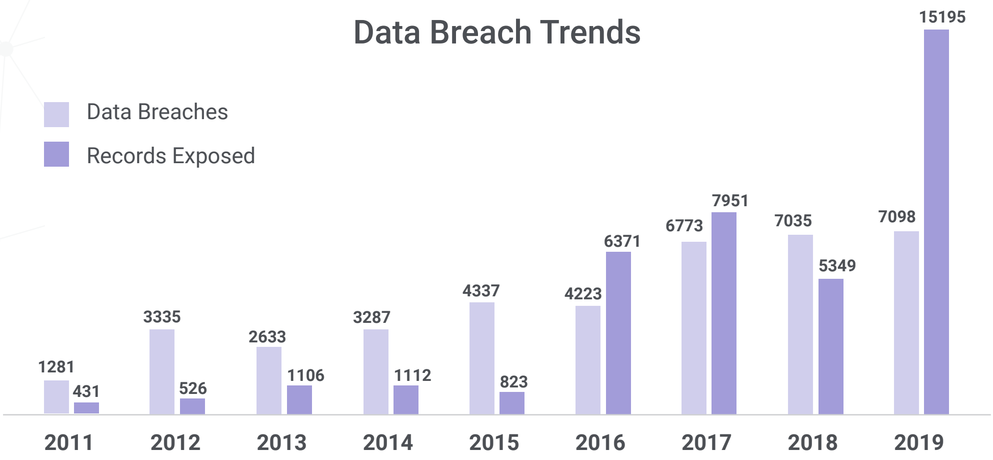
The IBM Cost of a Data Breach 2019 report[1] estimated the average cost of a data breach at $3.9 million globally and $8.2 million nationally. The loss of customer trust and subsequent loss of business is the largest component of this average cost calculation.

Average Cost of a Data Breach

Globally	United States
$3.9 million	$8.2 million

[1] Cost of a Data Breach Report, IBM, 2019

A recent data breach report from Risk Based Security[2] shows 15 billion records exposed in 2019, a significant jump from recent years. Four breaches caused by misconfigured databases exposed 6.7 billion records in Q4 2019.

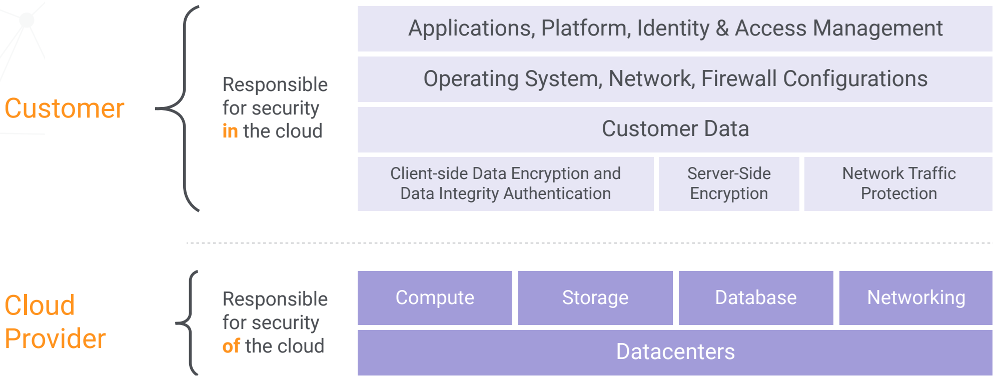


The IBM X-Force Threat Intelligence Index 2020 report[3] has shown a nearly tenfold year-over-year increase in records exposed due to misconfigurations, accounting for 86 percent of the total records compromised in 2019.

Shared security responsibility in the cloud

Cloud service providers (CSPs) have built infrastructure using various hardware and software components (compute, storage, database, networking). CSPs are responsible for the security "of" the cloud. They've made significant investments in cloud infrastructure security and offer multiple compliance certifications.

The Shared Responsibility Model

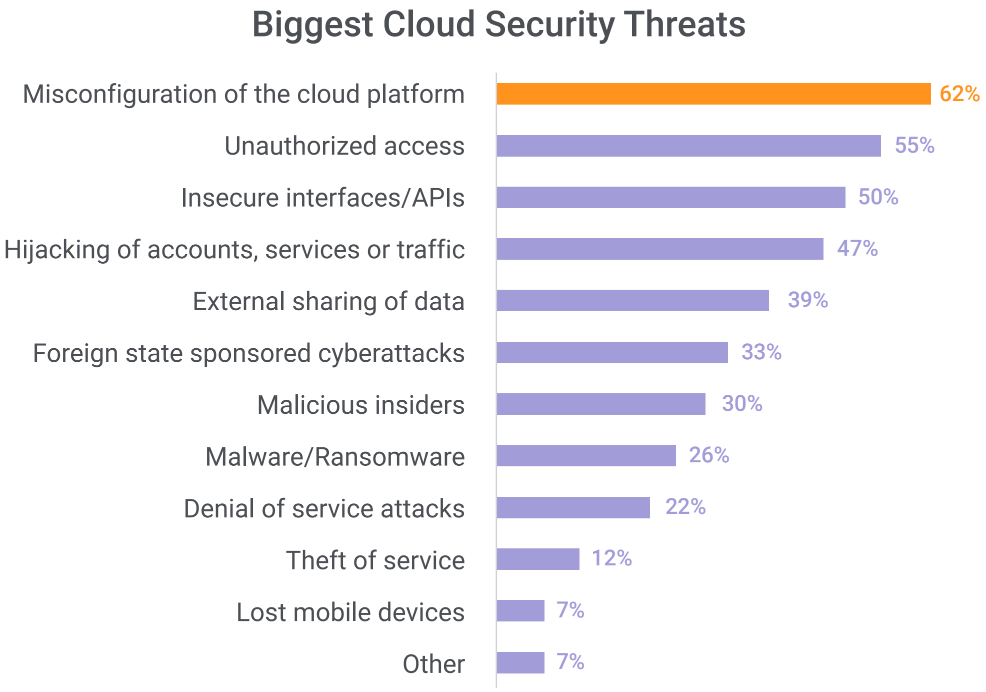

Customer
Responsible for security in the cloud
Applications, Platform, Identity & Access Management
Operating System, Network, Firewall Configurations
Customer Data
Client-side Data Encryption and Data Integrity Authentication
Server-Side Encryption
Network Traffic Protection
Cloud Provider
Responsible for security of the cloud
Compute
Storage
Database
Networking
Datacenters

While the CSPs ensure that the underlying infrastructure is secure, it is the customer's responsibility to ensure the applications are built correctly, data isn't exposed, and the configurations are securely set. This is true for all cloud services consumed by the customer, such as hosts and container clusters, IaaS, PaaS, SaaS, and security services.

[2] 2019 Year End Data Breach QuickView Report, Risk Based Security, 2020
[3] IBM X-Force Threat Intelligence Index, 2020

Misconfiguration is the biggest security threat

Security professionals identified misconfiguration as the biggest cloud security threat.[4] But if you look at the contributors to other possible threats (such as unauthorized access, insecure interfaces, hijacking of accounts), the likely causes of them happening are mostly attributed to misconfigurations.



The threat posed by misconfiguration has also been recognized by research analysts. "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes. Security and risk management leaders should invest in cloud security posture management processes and tools to proactively and reactively identify and remediate these risks," is stated in the Gartner Innovation Insight for Cloud Security Posture Management report.[5]

Traditional security approaches don't work

The network was once the secure perimeter organizations relied on to protect their valuable information stored in databases and file shares. In the cloud, a database can be individually exposed to the internet with a few simple configuration changes. A locked-down data store acts as an inhibitor for developers during development phases and they may keep it open. These configurations can unintentionally slip into production environments.

Traditional security assessments are too slow

Traditional security and compliance audits are tedious and slow manual processes. Assessors interview IT teams and take screenshots of product configurations as proof of compliance. In the cloud, the speed of cloud infrastructure change is so high that by the time an audit is complete, the infrastructure could have been rebuilt many times. Automation of security and compliance assurance is the only way for security to keep up with the speed of development and frequency of releases in the cloud.

[4] Cloud Security Report, Cybersecurity Insiders, 2018
[5] Innovation Insight for Cloud Security Posture Management, 2019

Challenges to prove compliance

Regulated industries have to adhere to specific industry benchmarks such as PCI DSS for retail, HIPAA for healthcare, FFIEC for financial services, NIST, and many more. Businesses still conduct mostly interview-based compliance assessments. Gathering evidence and mapping it to the control frameworks is a massive undertaking. These compliance frameworks provide high-level controls that need to be met on a continuous basis. Many compliance frameworks (such as PCI DSS) are incorporating the concept of continuous compliance as a requirement. All of these problems get compounded for cloud workloads that are changing rapidly.

Cloud service providers offer basic capabilities

CSPs offer tools to enable customer visibility into security and compliance posture. These products offer basic security policy coverage and support a limited set of compliance frameworks. To enable organization-wide security and compliance assurance, significant integration and custom development is required. As a result, organizations that deploy applications in the public cloud are forced to accept trade-offs between development speed and security risk. Larger organizations with hundreds of developers continuously releasing new code into production will have to implement a fully automated cloud security and compliance assurance solution.

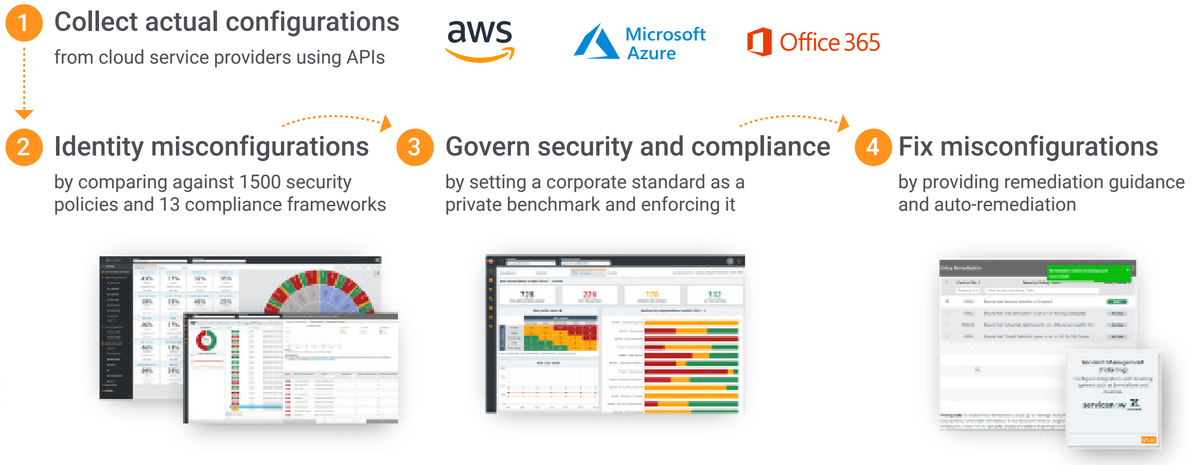
Enter Cloud Security Posture Management (CSPM)

Gartner defined a new category of products that solve multiple compliance problems with traditional security by automating security and compliance assurance and addressing the need for proper control over cloud infrastructure configurations, calling this category Cloud Security Posture Management (CSPM). In 2020, adoption of CSPM solutions is strong and growing and is projected to reach 25 percent in the next few years. Organizations are realizing that this is a “must have” cloud security tool.

The Zscaler Approach to CSPM

The challenge with many CSPM solutions is that, as point products, they can’t integrate into the larger organization’s security and data protection tools, so they provide siloed visibility and make it difficult to bring CSPM into a company’s existing processes.

Zscaler CSPM uniquely solves the integration problem by automatically identifying and remediating application misconfigurations as part of the comprehensive, 100% cloud-delivered data protection capabilities in the Zscaler Cloud Security Platform.



1 **Collect actual configurations** from cloud service providers using APIs

2 **Identity misconfigurations** by comparing against 1500 security policies and 13 compliance frameworks

3 **Govern security and compliance** by setting a corporate standard as a private benchmark and enforcing it

4 **Fix misconfigurations** by providing remediation guidance and auto-remediation

Zscaler CSPM delivers a breadth of innovations and product capabilities that automate security and compliance in the cloud, delivering continuous visibility and enforcing adherence to security policies and compliance frameworks.

Collect actual configurations

The Zscaler CSPM application is granted access to customer cloud environments (AWS, Azure, Office 365, Google Cloud, or any other CSP). It then collects actual configurations of cloud infrastructure over APIs. A small subset of policies may require installation of an agent.

Identify misconfigurations

Zscaler CSPM compares discovered configurations against built-in security policies and identifies misconfigurations at the security policy and resource level. It also provides a complete mapping of security policies within various compliance frameworks. Intuitive dashboards and reports help review this information.

Govern security and compliance

Zscaler CSPM enables various cloud governance features, including risk-based prioritization of the security posture, policy management (e.g., overrides, exceptions, third-party compensations), and configuration of private benchmarks for organizations that have multiple compliance standards or information security teams that need to customize the policy set for specific architecture.

Fix misconfigurations

Remediation steps for each and every security policy and auto-remediation for a subset of the most critical security policies can be applied.

Collect actual configurations

Onboarding

Providing access to customer cloud environments (onboarding) is a quick and easy process. Onboarding cloud accounts involves the creation of an App Registration role in Azure and Office 365 and a SecurityAudit role in AWS, then granting relevant (mostly read-only) access permissions.

For certain policies, CSPs do not provide the necessary APIs, so Zscaler CSPM developed agents to automate metadata collection and achieve the most comprehensive security policy coverage.

Multicloud

Many organizations are moving forward with multicloud initiatives to leverage for their business applications' best-in-class cloud services compared on cost, capabilities, security, and scale. Likewise, Zscaler CSPM supports multiple cloud environments and plans for further expansion as part of the product roadmap.

Multicloud

CSP	2018	2019	2020
Microsoft Azure	■	■	■
Office 365	■	■	■
aws		■	■
Google Cloud Platform			■

Multi-geo

Zscaler CSPM supports multiple deployment options, including public SaaS (default) and private SaaS for enterprises needing more control over their data. These deployments are hosted in multiple data-sovereign regions (geographies) as required by the customer's data sovereignty requirements.

Scalability

Enterprises with larger environments of more than 10,000 cloud resources require:

- high scalability in collecting configuration metadata across a wide range of cloud resources;
- the ability to store vast amounts of collected metadata in the database;
- keeping the scan time as short as possible; and
- quickly displaying security posture data on intuitive dashboards and reports.

Zscaler CSPM uses the latest advancements in cloud computing, such as serverless functionality for metadata collection and NoSQL databases (Cosmos DB) for storing information. For each cloud infrastructure scan, thousands of parallel serverless functions get created for parallel metadata collection and storing in the database. The NoSQL database is the most scalable and the fastest way for storing and retrieving data in the cloud. Zscaler CSPM requires only few minutes to complete a scan and generate reports for further analysis.

Data security

Information stored as part of the metadata collection process is about actual cloud infrastructure configurations. If such information becomes accessible it can lead to increased exposure to bad actors. Accordingly, CSPM products require full data encryption in transit and at rest, complying with the most stringent rules-based access controls (RBAC) and clearly defined data retention policies.

Companies offering CSPM as a SaaS offering go after SOC 2 certification to prove adherence to security best practices and organizational maturity in order to follow defined processes.

Identify misconfigurations

Security policy coverage

The breadth of security policy coverage in terms of the variety of supported cloud services determines whether CSPM solutions can properly assess all cloud services used by the customer and the comprehensiveness of coverage for each cloud service.

Zscaler CSPM offers a comprehensive set of 1,500+ security policies (cloud security best practices) and will be increasing policy coverage even further in the near term.

Security Policies Coverage

Cloud Infrastructure

IaaS Compute AWS EC2, Azure VMs, VM scale sets, Azure Service Fabric Cluster

PaaS and Serverless functions, Lambdas, web apps, API apps, mobile apps

Networking Azure Vnet AWS VPC, Cloud Firewall, NSG, security groups, DDoS, WAF, ports, protocols

Data Analytics HDInsight, data lake

Storage Azure Storage, AWS S3

PaaS Databases Azure SQL DB, SQL servers, SQL DW, NoSQL DBs, AWS RDS, AWS RedShift, AWS Aurora DB, AWS Dynamo DB, Postgres SQL, MySQL

Backups backup vaults, retention, encryption, access

Logging, Auditing and Monitoring Azure Monitor, Application Insights, CloudWatch, CloudTrail

Cloud Account Security root account settings, account IAM settings, monitoring profiles, security center/hub configurations

IAM Access controls MFA, use of built-in roles, guest user

Virtual Machine OS Baseline Windows 2012 R2, Windows 2016

Kubernetes Control Planes AKS patching, ASC integrations, AD integrations

Key Management Azure Key Vault, AWS KMS

Data-In-Transit TLS/SSL, certificate authentication, application gateway, OWASP WAF configurations

SaaS

Identity & Authentication basic and modern auth, self-service Password resets, global admins

Applications Permissions SafeLinks, external users, ATP

Applications Usage risky apps, insider threats, compromised account connects

Auditing logging, activity reports

Data and Data Management

Device Management mobile device mgmt., Intune configurations, device password policies

Email Security/Exchange

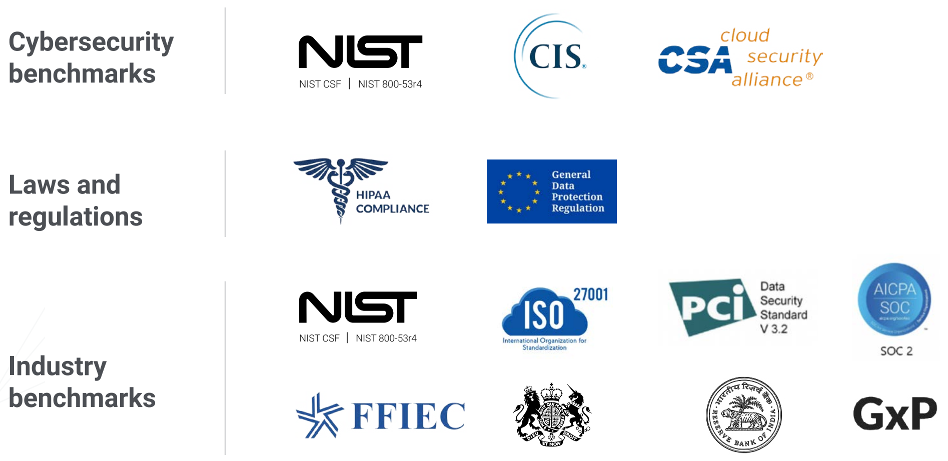
Document Sharing external domain whitelisting

The goal is to cover all of the most frequently consumed cloud services and address additional specific customer requirements. Each CSP has its own set of required policies. Zscaler CSPM has always led in policy coverage for Microsoft Azure and Office 365; and with recent additions, the AWS policy coverage is among the best in the industry.

Compliance frameworks

Zscaler CSPM offers 13 compliance frameworks, including cybersecurity and industry benchmarks, laws, and regulations. This set is currently being expanded to include regional compliance frameworks for Europe, as well as Australia and other countries.

Compliance Framework



Govern security and compliance

Zscaler CSPM enables various cloud governance features, including risk-based prioritization of the security posture, policy management, and configuration of private benchmarks.

Policy management

Zscaler CSPM offers various features to manage application of security policies to discovered assets.

- Policy exclusions allow customers to define a temporary (time-bound) or permanent exclusion of a policy to the cloud accounts.
- Policy overrides allow customers to mark certain policy as "pass" (indicating compliance) for cases when customers have third-party compensating controls that cannot be determined by CSPM product.
- Manual policies allow customers to track best practices where automation might not be available (e.g., CSPs don't provide an API, or customer might not have granted Zscaler CSPM access to scan their sensitive data).

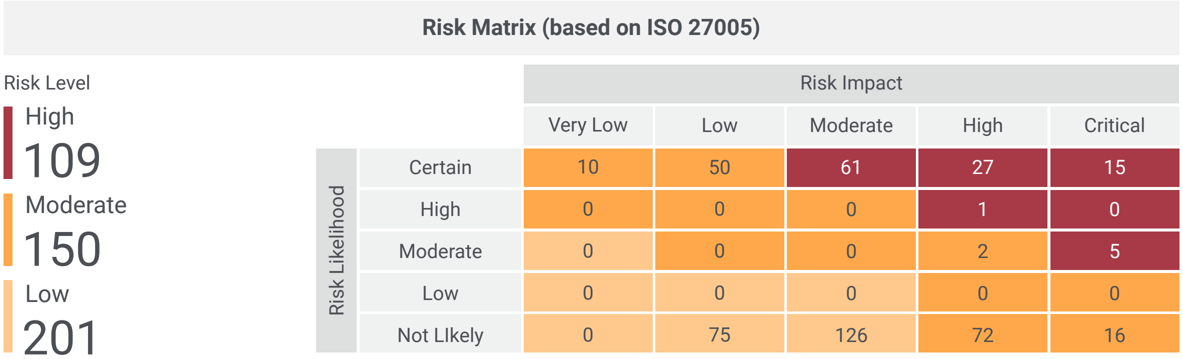
Private benchmarks

Security requirements vary significantly across organizations based on factors like industry and size. Customers could decide to bring all of their controls (across all compliance and best practices) into a private benchmark. Multiple individuals within the organization can collaborate in authoring the benchmark and applying it to specific cloud accounts.

Zscaler CSPM offers an easy-to-use configuration interface to create private benchmarks from an existing standard or from scratch, based on individual company requirements. As these private benchmarks are version controlled, customers also use it to continually enforce higher standards over a period of time. A v1 private benchmark will be enforced to start initially, a v2 private benchmark will be enforced to improve security posture in subsequent releases, and so on.

Risk matrix

The Zscaler CSPM risk-based prioritization matrix follows the ISO 27005 standard. The risk matrix automatically categorizes each security policy by risk impact and likelihood. Risk *impact* ranges from "Not Likely," "Low," "Moderate," and "High," to "Certain." Risk *likelihood* ranges from "Very Low," "Low," "Moderate," and "High," to "Critical." Risk impact is pre-set for each security policy. Risk likelihood is calculated dynamically based on multiple metrics and a machine learning algorithm.



Risk Matrix (based on ISO 27005)

Risk Level

High
109

Moderate
150

Low
201

		Risk Impact				
		Very Low	Low	Moderate	High	Critical
Risk Likelihood	Certain	10	50	61	27	15
	High	0	0	0	1	0
	Moderate	0	0	0	2	5
	Low	0	0	0	0	0
	Not LIkely	0	75	126	72	16

Colors indicate risk level and numbers indicate number of security policies.

The risk matrix has an X-axis and a Y-axis showing the number of security policies in each X / Y segment. Accordingly, security policies with high risk impact and high risk likelihood are classified as "High" risk level.

Fix misconfigurations

Remediation guidance

When organizations deploy cloud infrastructure manually, they need to update their configuration guides and remediate resources to make them compliant with all security policies in their private benchmark. Zscaler CSPM offers security policy remediation guidance in the form of easy-to-understand steps using the CSP console and command lines or scripts, when possible.

Auto-remediation

When certain types of misconfigurations occur in production, it may be too late to wait until a ticket is assigned to the right person or the right person is available in that work shift to fix it. Such critical security issues need to be resolved immediately.

Zscaler CSPM offers auto-remediation policies that get triggered within moments after a deployment change has been initiated by a customer (e.g., new deployment or manually changing configurations using cloud provider consoles). Zscaler CSPM provides a governance plane for customers to select auto-remediation policies among hundreds available and decide to pilot them for pre-production environments. After these policies are tested in pre-production, they can be enforced in production environments.

Deployment automation

While visibility into misconfigurations is important, it is also important to prevent misconfigurations from getting into production in the first place. Organizations that deploy cloud infrastructure manually should automate deployment for all critical resources.

Zscaler CSPM provides Quick Win automation scripts and recommendations. Companies are advised to establish a central repository for deployment automation. When deployment of critical resources is automated, the organization can start moving toward full DevSecOps automation.

Ticketing integration

Zscaler CSPM integrates with customers’ ticketing systems to automatically generate and assign tickets to the appropriate Cloud Operations (CloudOps) team member. These tickets contain vital information about non-compliant resources and remediation guidance. Zscaler CSPM auto-assigns priority to the tickets to make it easier for the CloudOps team to manage their capacity. A Zscaler CSPM administrator can configure and throttle the frequency of tickets created (e.g., don’t run, daily, weekly, monthly, etc.).

DevOps integration

Companies implementing cloud security and compliance assurance processes soon realize that manual or semi-automated cloud infrastructure deployment is still prone to human error.

Most organizations implement automation to increase their software release velocity. Frequent deployment changes have a large potential to alter security posture in an unintended direction. To ensure security posture is continually improved, these security validations are getting integrated into continuous compliance/continuous development (CI/CD) pipelines.

Zscaler CSPM supports all required CI/CD integrations. A newly created cloud account can be automatically onboarded to Zscaler CSPM. One request can be sent to initiate an infrastructure security scan, and another can be sent to retrieve security and compliance posture. An automatic analysis can be done to decide whether to keep a deployment in production or roll it back. These DevSecOps capabilities are in line with the intended security shift-left.

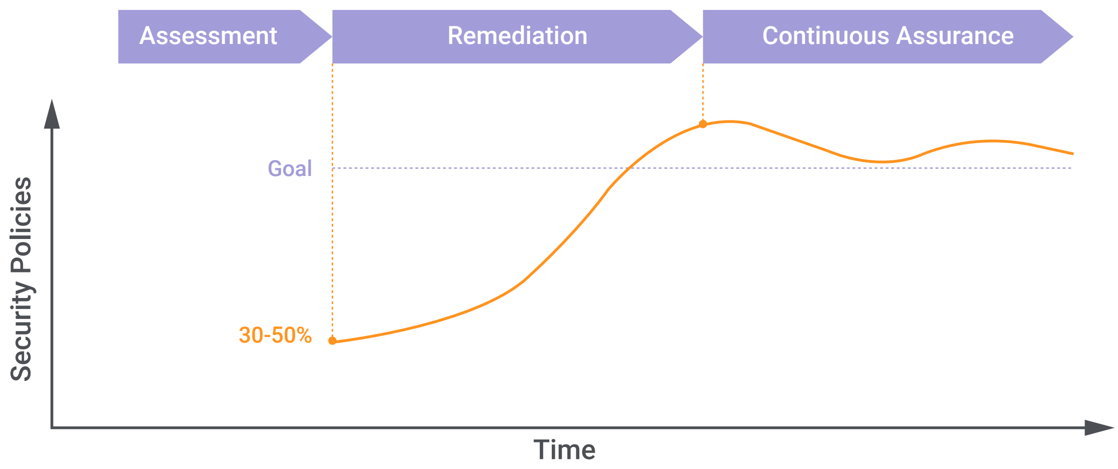
CSPM is a Multi-Team Collaboration

Adoption steps

Assess your security posture

Companies use CSPM solutions to provide compliance evidence based on common cybersecurity frameworks such as CIS or NIST; in regulated industries, they support industry-specific compliance frameworks such as HIPAA for healthcare, SOC 2 for ISVs, PCI DSS for ecommerce, ISO 27001 for enterprises with international operations, and FFIEC for financial services.

Adoption Phases



CSPM solutions can be used to conduct an assessment of existing cloud infrastructure to determine current security posture. Typically, a project is then initiated to identify "must have" security policies, in collaboration with the information security (InfoSec) team, and initiate remediation activities.

Remediate to achieve the goal

Remediation requires specialized CloudOps team training on cloud security best practices and new configuration requirements. Remediations are first validated in pre-production environments to make sure that new cloud infrastructure configurations won't break applications or impact performance. Dev/Test and pre-production environments are rebuilt per new configurations aligned with the desired security posture. As a result, the security posture improves to meet and/or exceed goals.

Continuous assurance

After remediation, CloudOps teams take responsibility for ongoing security and compliance assurance. They monitor security posture in the production environment daily to make sure that last-minute fixes or updates do not introduce any misconfigurations.

Security assurance tools are also used on an ongoing basis in the Dev/Test and pre-production environments to validate the accuracy of configurations before deploying new application releases into production environments.

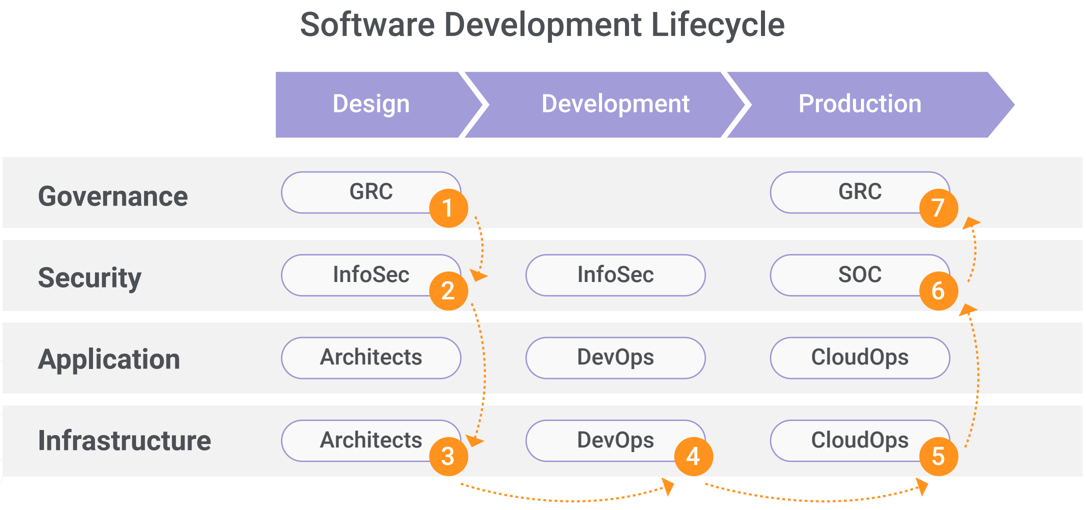
Security operations (SOC) teams should add security posture monitoring to their dashboards and escalate quickly any critical misconfigurations discovered in the production environment.

Cross-departmental collaboration

Deploying CSPM improves collaboration between InfoSec, SOC, and application development (AppDev) teams. While the InfoSec team is responsible for setting the corporate standard (goal), the application development and infrastructure management teams ultimately need to take responsibility for implementing security and compliance standards.

The CSPM process includes the following steps:

1. GRC specifies required compliance frameworks
2. InfoSec defines corporate information security standards
3. Cloud architects create secure application architecture configurations
4. DevOps deploys cloud infrastructure
5. CloudOps fixes discovered misconfigurations
6. SOC monitors security posture
7. GRC provides evidence of continuous compliance



Software Development Lifecycle

	Design	Development	Production
Governance	GRC 1		GRC 7
Security	InfoSec 2	InfoSec	SOC 6
Application	Architects	DevOps	CloudOps
Infrastructure	Architects 3	DevOps 4	CloudOps 5

GRC: Compliance frameworks

GRC teams specify the required industry compliance frameworks (industry benchmarks, laws, and regulations). Zscaler CSPM supports various compliance frameworks and continuously adds new ones based on customer requirements.

InfoSec: Corporate standard

The InfoSec team has the responsibility for defining a set of “must have” security policies for their organization, including cybersecurity benchmarks and additional company-specific policies. In addition, Zscaler CSPM offers the ability to add private benchmarks that customers can track and enforce.

Cloud architects: Configuration guides

Architects design cloud infrastructure, taking into account cloud architecture best practices, and create secure configuration guides for CloudOps teams. Zscaler CSPM provides detailed definitions for all security policies as well as configuration guidance in the form of remediation steps.

DevOps: Deploy infrastructure

In many organizations, cloud infrastructure is deployed manually by the infrastructure management team, while other organizations have automated cloud infrastructure deployment by the DevOps team. The infrastructure management team or DevOps team scan cloud infrastructure using Zscaler CSPM in the pre-production environment. Any discovered misconfigurations need to be fixed before proceeding to production deployment. We describe the fully-automated scenario later in the DevSecOps section of this document.

CloudOps: Fix misconfigurations

The CloudOps team initiates a scan immediately after deployment into the production environment. If the deployed cloud infrastructure is meeting the required standards, it can stay in production. CloudOps also schedules daily scans of the cloud infrastructure. Any discovered misconfigurations have to be fixed quickly based on priority and depending on their risk level.

SOC: Continuous monitoring

Production environments should be scanned daily to validate any last-minute manual configuration changes. SOC teams monitor for deviations and escalate critical misconfigurations that require immediate fixes.

GRC: Compliance evidence

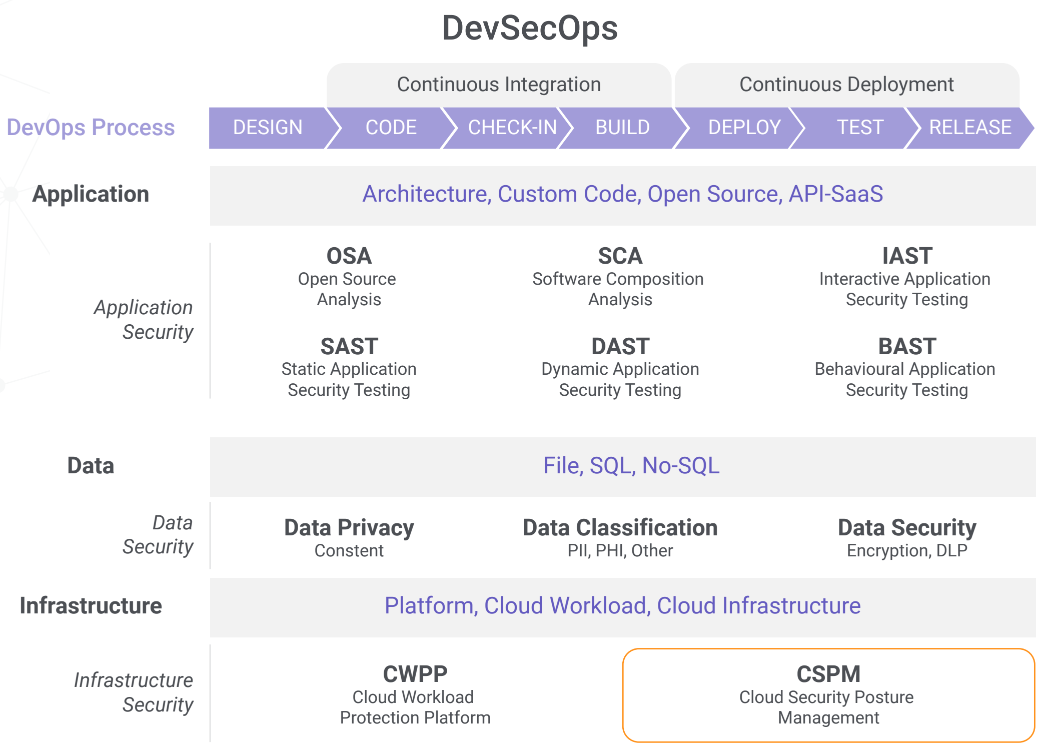
Compliance teams have access to daily monitoring results and can provide these reports as evidence for continuous compliance to regulators and auditors.

Achieving DevSecOps

DevSecOps practices

Application security: The term DevSecOps is normally used to describe the integration of application security practices into the application development lifecycle. Static application security testing (SAST), dynamic application security testing (DAST), and other tools are used to review against coding best practices, discover security issues, and log defects. Penetration tests are used to validate the robustness of the application code prior to release into production. Runtime application self-protection can be implemented.

Data security: Data security gained significant importance with the introduction of GDPR regulation. Data privacy, data classification, and data security practices need to be validated in the pre-production environment as part of DevSecOps.


DevSecOps
Continuous Integration
Continuous Deployment
DevOps Process
DESIGN
CODE
CHECK-IN
BUILD
DEPLOY
TEST
RELEASE
Application
Architecture, Custom Code, Open Source, API-SaaS
Application Security
OSA
Open Source Analysis
SCA
Software Composition Analysis
IAST
Interactive Application Security Testing
SAST
Static Application Security Testing
DAST
Dynamic Application Security Testing
BAST
Behavioural Application Security Testing
Data
File, SQL, No-SQL
Data Security
Data Privacy
Constent
Data Classification
PII, PHI, Other
Data Security
Encryption, DLP
Infrastructure
Platform, Cloud Workload, Cloud Infrastructure
Infrastructure Security
CWPP
Cloud Workload Protection Platform
CSPM
Cloud Security Posture Management

Cloud infrastructure: Consumed from CSP, cloud infrastructure can be deployed and configured using Infrastructure as Code (IoC). What is not commonly understood is that the configuration of cloud infrastructure is also an integral part of the overall DevSecOps operating model.

Ultimately, organizations need to move toward an integrated DevSecOps process covering security best practices across applications, data, and infrastructure. A security left-shift needs to happen to identify misconfigurations in pre-production environments and prevent them from getting into production environments.

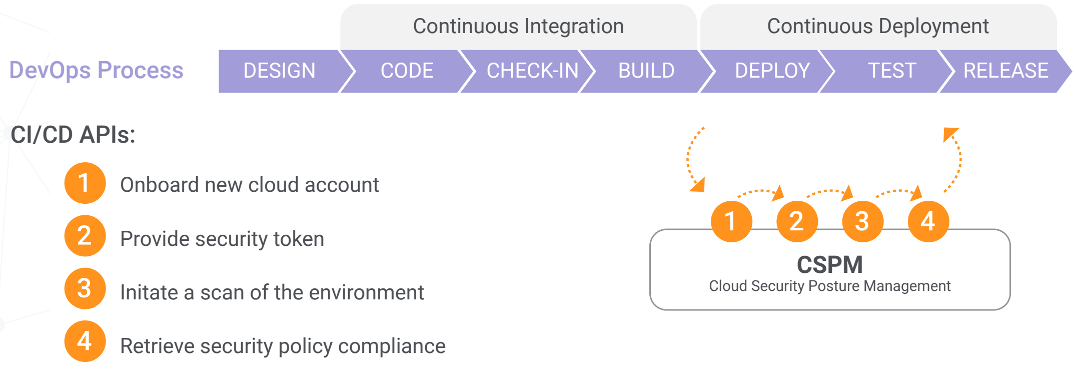
As deployment automation becomes part of the CI/CD pipeline, it is essential that cloud infrastructure configurations are also validated against cloud security best practices. CSPM products need to provide relevant APIs that can be called by CI/CD pipelines.

Required CI/CD APIs

CSPM products need to support end-to-end processes, including:

1. Onboarding a new cloud account
2. Providing security token
3. Initiating a scan of the environment (dev, test, other)
4. Getting security policy “pass” or “fail” information automatically to compare against corporate standards

CI/CD APIs for DevSecOps



Continuous Integration

Continuous Deployment

DevOps Process: DESIGN › CODE › CHECK-IN › BUILD › DEPLOY › TEST › RELEASE

CI/CD APIs:

1. Onboard new cloud account
2. Provide security token
3. Initate a scan of the environment
4. Retrieve security policy compliance

1 2 3 4

CSPM
Cloud Security Posture Management

DevOps teams can use Zscaler CSPM CI/CD APIs to automatically initiate a rescan after the environment has been built and receive the compliance status for all security policies. Teams can analyze the results of a scan and update their IoC automation repository in line with configuration standards. Zscaler CSPM remediation guidance is also available to support these efforts.

Zscaler CSPM

Zscaler CSPM automates security and compliance in the cloud, delivering continuous visibility and enforcing adherence to the most comprehensive set of security policies and compliance frameworks. Offered as a multi-tenant SaaS, the product enables seamless integration with customer cloud infrastructure, quick data collection, comprehensive dashboards and reports. Zscaler CSPM supports integrations with CI/CD pipelines and ticketing systems, enables auto-remediation, and supports private benchmarks. Customers can easily enforce their corporate information security standards across AWS, Azure, and Office365 environments to prevent misconfiguration-related data breaches.

Market leader

Zscaler CSPM automates visibility into the status of 1,500+ security policies and 13 compliance frameworks across AWS, Azure, and Office365. The product also allows organizations to create their own private benchmarks, supports large-scale application environments, and allows rapid adoption of DevSecOps.

Prevent misconfigurations

Misconfiguration of cloud infrastructure is the biggest cloud security risk. By automating cloud security and compliance assurance, organizations can significantly reduce their cybersecurity risks and prove continuous compliance to their regulators.

Implement DevSecOps

Manual security and compliance processes are of no use given the dynamic nature of cloud environments. Zscaler CSPM provides industry-leading security policy coverage and offers quick and easy API-based integration with DevSecOps tools.

Accelerate cloud adoption

When security and compliance are under control, executives can give a green light to faster cloud adoption. Digital transformation initiatives can accelerate, giving Zscaler CSPM customers a competitive advantage.

Adopt digital governance

CSPM is an important first step in transforming security, compliance, risk management, and data privacy functions to match the speed of cloud. Digital businesses benefit from automated governance processes.

For more information go to zscaler.com/CSPM

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com