DATA SHEET

Zscaler™ Workload Posture

Zscaler Workload Posture remediates misconfigurations, secures sensitive data, and enforces least-privileged access across your public cloud footprint.

Multiple trends have made digital transformation possible—and necessary. Many organizations are moving their private applications from the data center to public clouds, such as Azure, AWS, and GCP. Moreover, they are also building new cloud-native apps using IaaS, PaaS, and SaaS capabilities, eliminating IT complexity as cloud providers manage all the infrastructure. This complex mix of cloud services introduces compliance and security concerns that put organizations' confidential data at risk. Traditional security policies and technologies provide little value in cloud environments, as workloads are controlled by the DevOps team that accelerate the pace of development and deployment, making it difficult for security teams to keep up. Legacy network security doesn't align with the agile development and DevOps processes that have come to define cloud operations. If organizations are to benefit from public cloud adoption, the organization must understand and mitigate ecosystem risks while maintaining compliance.

Key Challenges

- **Misconfiguration and excessive permissions are the biggest security threats**
  Data breaches resulting from misconfigurations of cloud infrastructure and excessive permissions continue to expose enormous amounts of confidential customer data, leading to legal liability and financial losses. According to Gartner analysts, "Through 2023, 99% of security failures will be the customer's fault—and 75% of those failures will be the result of the inadequate management of identities, access, and privileges.[1]

- **Sensitive data protection**
  Sensitive data is distributed and stored across multiple cloud environments, applications, cloud storage, and services. This creates data visibility, control, access, compliance, and remediation challenges, potentially putting organization-sensitive data at risk. Misconfiguration, excessive permission to cloud storage services, and application vulnerabilities have led to many high-profile exposures of sensitive data over the past few years. Therefore, organizations must identify and protect sensitive cloud data across their cloud footprints, and leverage automation to ensure consistent enforcement in dynamic cloud environments.

- **Risk governance and compliance**
  Compliance for cloud-based workloads requires deep knowledge of cloud services and regulatory frameworks, making it difficult for most enterprises to prove and maintain compliance. The challenges of implementing cloud governance (visibility, policy enforcement across business units, least privileges, lack of knowledge about cloud security controls) continue to increase as cloud adoption grows within the organization.

- **Cloud service providers offer basic capabilities**
  Cloud service providers (CSPs) offer tools to enable visibility into security, permissions, and compliance posture. These solutions offer basic security policy coverage and support a limited set of compliance frameworks. Native CSP capabilities can be a good start for organizations, but most will seek third-party tools that cut across a diverse cloud strategy—especially as their cloud footprint grows. Security leaders must take proactive steps to increase visibility, control, and secure cloud environments to address cloud security threats.

"Nearly all successful attacks on cloud services result from 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," according to Gartner.[2]

Enter Zscaler Workload Posture

3-in-1 with configuration security, entitlements and permissions, and data protection
Zscaler Workload Posture makes it simple to secure cloud configurations, access permissions, and data protection across multi-cloud environments. Zscaler Workload Posture secures workloads with cloud security posture management (CSPM), simplifies cloud infrastructure entitlement management (CIEM), and delivers best-in-class data loss prevention (DLP).

CONFIGURATION

Cloud Security Posture Management (CSPM)

Ensure cloud resources have proper configurations for authentication, data encryption, internet connectivity, and more for compliance and a strong security posture.

ACCESS

Cloud Infrastructure Entitlement Management (CIEM)

Identify and remediate excessive permissions that humans and machines have by using machine learning analysis for increased visibility into access policies, resource policies, actions, and roles.

DATA

Data Loss Prevention (DLP)

Identify and secure confidential content in cloud data repositories, such as S3 buckets, by applying sensitive data classification, data loss prevention, malware, and threat prevention.

Cloud Configuration Security (CSPM)

Unified visibility across multi-cloud environments: A single dashboard that provides compliance visibility and mitigates violations across SaaS applications and cloud service providers, ensuring adherence to laws and industry regulations.

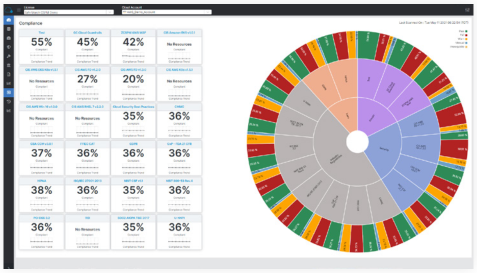
Risk prioritization: Enables cloud governance features, reporting policy violations, and risk-based prioritization of the security posture while ensuring business continuity.

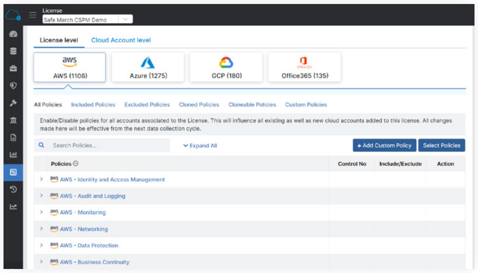
Guided + automated remediation: Ensure configurations of all cloud applications follow industry and organizational best practices, including manual, guided, and automated remediations.

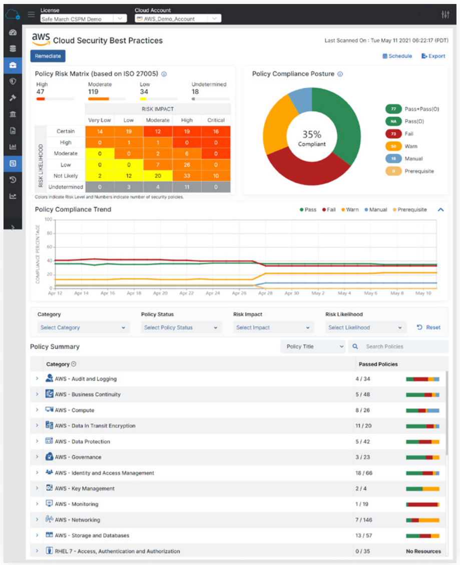
Automate regulatory compliance standards: Enforce regulatory compliance controls for CIS benchmarks, NIST, PCI DSS, HIPAA, etc., across cloud infrastructure and applications through automated workflows.

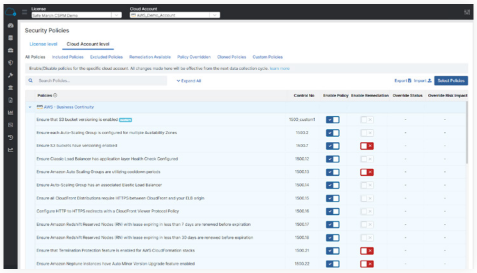
Private benchmarks: Security requirements vary significantly across organizations based on factors like industry and size. Zscaler offers flexibility to create and implement private benchmarks across all compliance frameworks and best practices.

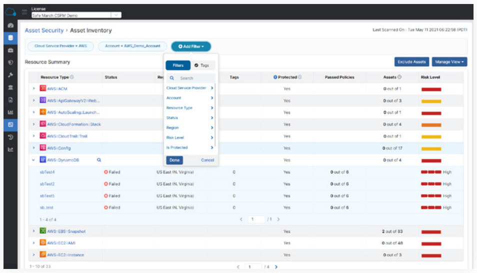
Secure K8S configurations: Identifies Kubernetes misconfigurations, processes running as root, privileged containers, and compliance violations, and secures various Kubernetes deployments like AKS and EKS.











Cloud Identity and Entitlements (CIEM)

Entitlements discovery and correlation: Centralized dashboard and visualization to discover and control all identities (human and nonhuman), their access, and permissions to resources.

Reduce risk: Harden your IAM configuration by cleaning up best-practice violations with AI-driven recommendations.

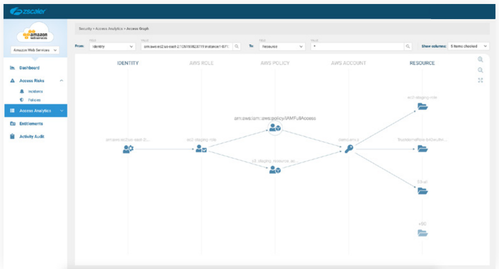
Identity access analytics: Get blast radius analysis (user, role, group, resource) using a deep identity-centric view of all access paths to cloud assets.

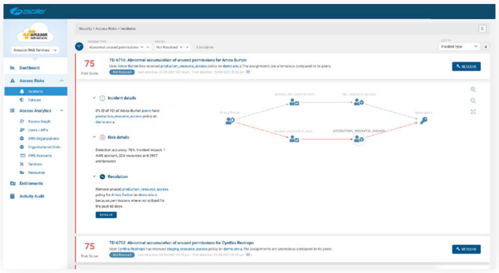
Data access analytics: Resource-centric access graphs to monitor data exposures. Map all users and machines and their access and permission to sensitive resources to protect business-critical data assets and meet compliance requirements.

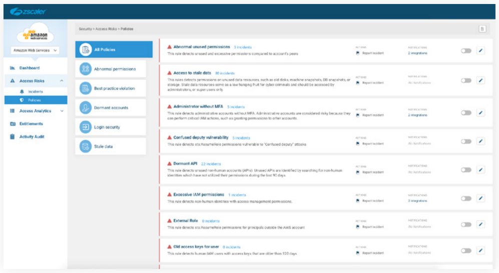
Privilege right-sizing: ML models, cohort analysis, and other techniques identify over-privileged identities and risky access paths to sensitive resources that can be removed to minimize the attack surface without slowing innovation.

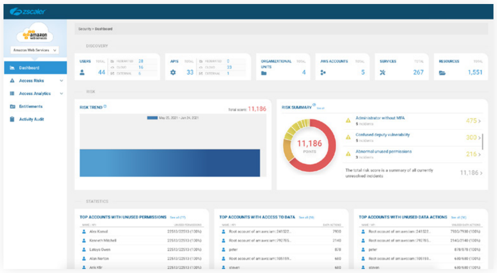
DevSecOps: Integrate security and compliance checks, and enforce automated guardrails for identities, resources, and network configuration at every development stage, empowering developers to innovate and deploy rapidly and securely.

Enforce cloud least privilege: Quickly and easily apply cloud least privilege at scale without disrupting productivity.









Cloud Data Protection

Data governance: A single pane of glass to discover, monitor, and manage misconfiguration, user activity, access permission to business-critical data such as AWS S3 storage in a multi-cloud environment.

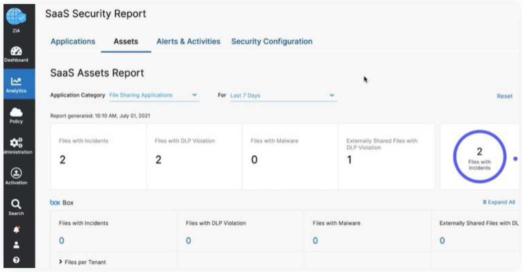
Data protection: Prevent the accidental sharing of sensitive data and stop internal threats such as stealing intellectual property.

Data categorization: Leverage machine learning to identify sensitive, regulated data within S3 and categorize data to empower data owners to manage access to their data and reduce the burden on IT.

Threat prevention: Identify potentially malicious activity, protect against malware threats that can infiltrate AWS S3 storage.

Compliance assurance: Ensure public cloud deployments follow industry and organizational best practices with step-by-step guided, or automated remediation to prevent data exposure and compliance violations.

Data exposure reporting: Leverage ML-driven data analytics to detect suspicious behavior, privilege escalation or deletion, and unusual resource data access. Simplify reporting with a unified management console.



SaaS Security Report

SaaS Assets Report

Application Category: File Sharing Applications
For: Last 7 Days

Report generated: 10:10 AM, July 01, 2021

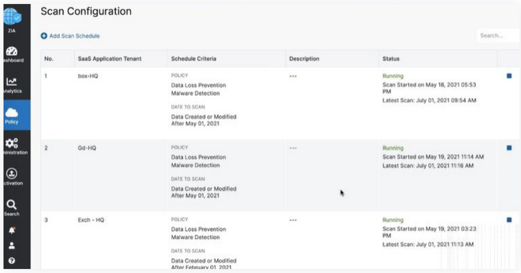
Files with Incidents	Files with DLP Violation	Files with Malware	Externally Shared Files with DLP Violation
2	2	0	1

2 Files with Incidents

Box

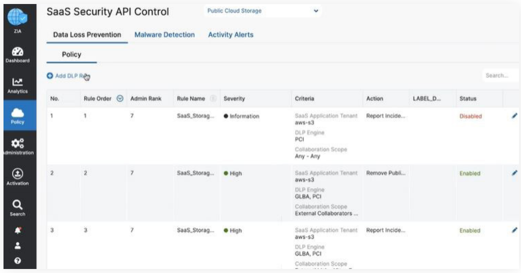
Files with Incidents	Files with DLP Violation	Files with Malware	Externally Shared Files with DL
0	0	0	0

Files per Tenant



Scan Configuration

No.	SaaS Application Tenant	Schedule Criteria	Description	Status
1	box-HQ	POLICY Data Loss Prevention Malware Detection DATE TO SCAN Data Created or Modified After May 01, 2021	...	Running Scan Started on May 18, 2021 05:53 PM Latest Scan: July 01, 2021 09:54 AM
2	Gd-HQ	POLICY Data Loss Prevention Malware Detection DATE TO SCAN Data Created or Modified After May 01, 2021	...	Running Scan Started on May 19, 2021 11:14 AM Latest Scan: July 01, 2021 11:16 AM
3	Exch - HQ	POLICY Data Loss Prevention Malware Detection DATE TO SCAN Data Created or Modified After February 01, 2021	...	Running Scan Started on May 19, 2021 03:23 PM Latest Scan: July 01, 2021 11:13 AM

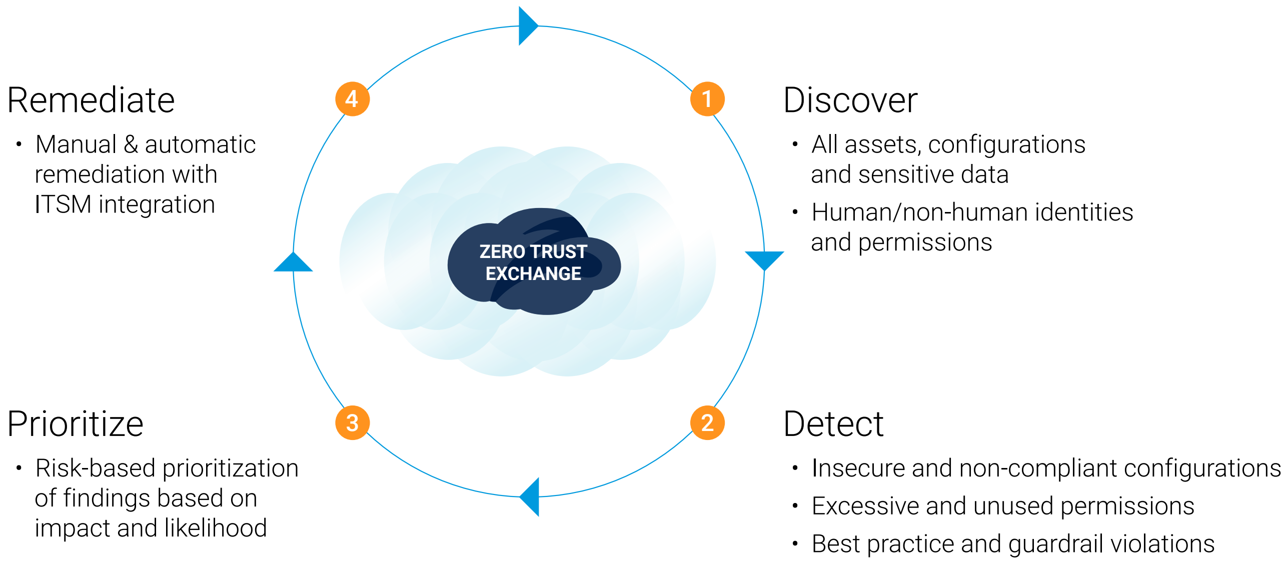


SaaS Security API Control — Public Cloud Storage

No.	Rule Order	Admin Rank	Rule Name	Severity	Criteria	Action	LABEL_D...	Status
1	1	7	SaaS_Storag...	● Information	SaaS Application Tenant aws-s3 DLP Engine PCI Collaboration Scope Any - Any	Report Incide...		Disabled
2	2	7	SaaS_Storag...	● High	SaaS Application Tenant aws-s3 DLP Engine GLBA, PCI Collaboration Scope External Collaborators ...	Remove Publi...		Enabled
3	3	7	SaaS_Storag...	● High	SaaS Application Tenant aws-s3 DLP Engine GLBA, PCI Collaboration Scope	Report Incide...		Enabled

How does Zscaler Workload Posture work?

Zscaler Workload Posture follows a four-step process to achieve continuous security, compliance, and governance for Public cloud infrastructure:



Discover

- All assets, configurations and sensitive data
- Human/non-human identities and permissions

Detect

- Insecure and non-compliant configurations
- Excessive and unused permissions
- Best practice and guardrail violations

Prioritize

- Risk-based prioritization of findings based on impact and likelihood

Remediate

- Manual & automatic remediation with ITSM integration

Discover assets, identities, and sensitive data

Zscaler Workload Posture works with read-only access to cloud environments (AWS, Azure, and Google Cloud). It collects metadata information that gives consolidated visibility of deployed assets, identities (human and non-human), sensitive data, configuration, and associations across the environment.

Detect misconfigurations, entitlements, and data exposure

Zscaler Workload Posture compares discovered configurations, identity permissions, and data access against built-in security policies and best practices, and identifies misconfigurations and policy violations 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.

Prioritize risk

Zscaler Workload Posture enables various cloud governance features, including risk-based prioritization of the security posture based on the ISO 27005 standard. The risk matrix automatically categorizes each security policy by risk impact and likelihood calculated dynamically based on multiple metrics and a machine learning algorithm, so that security teams can accurately identify and focus on top risks.

Remediate violations

Remediation for every security policy, identity and access misconfigurations, and auto-remediation for a subset of the most critical security policies can be applied. Integrates with the SecOps ecosystem and ITSM for efficient and effective incident management.

Compliance frameworks

Zscaler Workload Posture offers 16 compliance frameworks and 2700+ industry best practices, including cybersecurity and industry benchmarks, laws, and regulations.

NIST
NIST CSF | NIST 800-53r4
NIST
FRAMEWORK DOCUMENTS
CIS
CSA cloud security alliance
HIPAA COMPLIANCE
General Data Protection Regulation
PCI DSS COMPLIANT
LEVEL 1 VERSION 3.2
ISO 27001 Certified
AICPA SOC 2
FFIEC
RESERVE BANK OF INDIA
GxP
GC-Cloud Information Centre
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

KEY BUSINESS ADVANTAGES

- **Easy implementation:** Multi-tenant, SaaS API-based solution deploys in minutes with read-only access permission at scale without limitations and complexities.
- **Seamless integration:** Easily integrate with current SecOps ecosystems such as ServiceNow, Zendesk, or Splunk, so that the SecOps team can act immediately and effectively.
- **Operational excellence:** Automate common cloud security operational tasks, freeing up resources and optimizing cloud investments.
- **Team collaboration:** Enable team collaboration between InfoSec, Security Operations Center (SOC), and application development (AppDev) teams.
- **Accelerate cloud adoption:** When cloud security, IAM, data protection, and compliance are under control, executives can give the green light to faster cloud adoption. Digital transformation initiatives can accelerate, giving organizations a competitive advantage.

References:

1. Gartner Analyst and Report:
   Neil MacDonald, Innovation Insight for Cloud Security Posture Management
   Paul Mezzera, Managing Privileged Access in Cloud Infrastructure
2. Innovation Insight for Cloud Security Posture Management
   Published: 25 January 2019
   ID: G00377795
   Analyst(s): Neil MacDonald

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.