White Paper

Accelerating NIST 800-53 Cloud Compliance with Zscaler for Workloads

Introduction

The NIST 800-53 Framework catalogs security and data privacy controls that are applicable to all information systems of an organization, including public cloud infrastructures. Zscaler for Workloads helps customers accelerate NIST 800-53 compliance in a frictionless and cloud-native approach. The solution ensures consistent application of security and governance across multicloud environments. This also includes supporting disparate cloud operational processes such as cloud automation and developer operations.

Contents

Zscaler for Workloads

The goal of this document is to map the capabilities of Zscaler for Workloads to the NIST control categories. Zscaler for Workloads provides comprehensive protection for your public cloud infrastructure and applications, unifying both build and runtime security for cloud native and virtual machine (VM)–based applications. Zscaler for Workloads includes two major platform capabilities. Zscaler Posture Control is a cloud native application protection platform (CNAPP) that provides prioritized, risk–based visibility and remediation for multicloud environments. Zscaler Workload Communications is built on the Zscaler Zero Trust Exchange platform and provides secure internet access and zero trust connectivity between cloud applications.

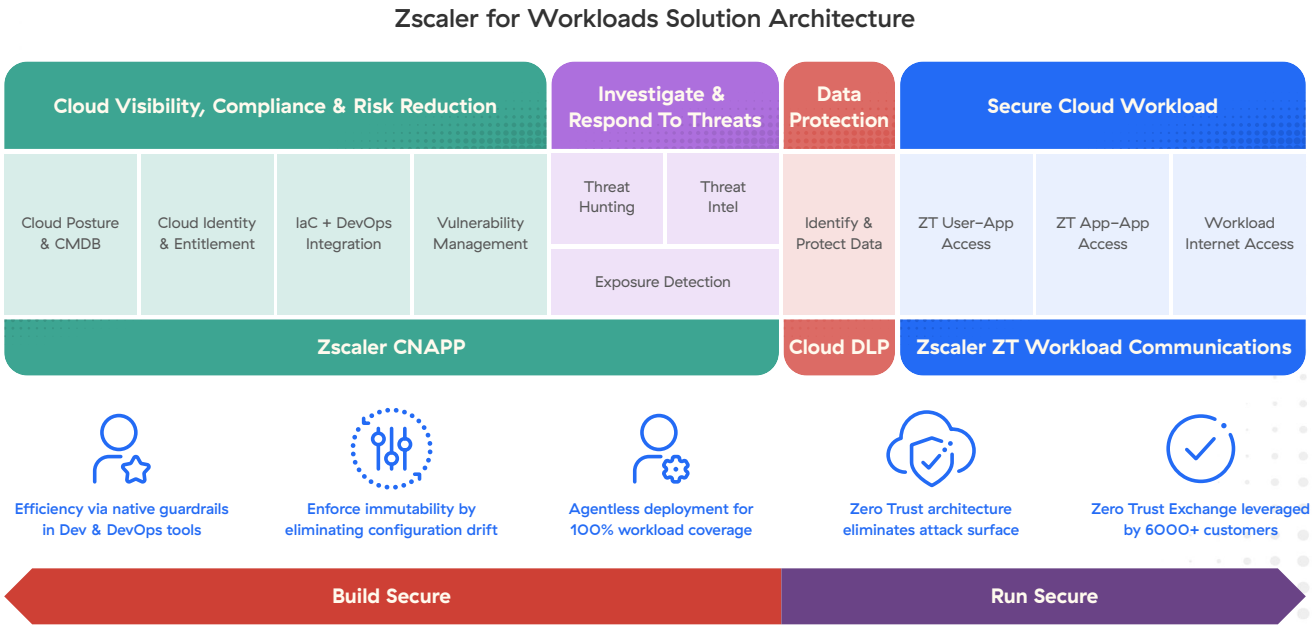


Figure 1: Zscaler for Workloads Solution architecture

NIST 800-53 Control Categories

The NIST Framework categorizes the security controls into 20 categories. For the purpose of brevity, we exclude the sub-controls and look at the combined outcome of each main category. The following groups from this category directly impact cloud infrastructure and its associated technical security controls:

Table 1: Mapping of NIST 800-53 Control Categories and Zscaler Workload Protection platform

ID	Family	Zscaler Solution Capability
AC	Access control	Posture Control, Workload Communications
AU	Audit and accountability	Posture Control
CA	Assessment, authorization, and monitoring	Posture Control
IA	Identification and authentication	Posture Control
CM	Configuration management	Posture Control
IR	Incident response	Posture Control
PT	PII processing and transparency	Cloud DLP, Posture Control, Workload Communications
RA	Risk assessment	Posture Control
SC	System and communications protection	Workload Communications, Posture Control
SI	System and information integrity	Posture Control
SR	Supply chain risk management	Posture Control

Control Categories and Supported Solution Capabilities

Access Control

The access control (AC) category deals with ensuring that effective security guardrails are applied to protect against unauthorized access to information systems. In the context of the cloud, this boils down to effective access control through authentication and authorization, encryption of data at rest and in use, and application of network access control policies. The AC category also enforces effective management of cloud identities, such as removal or deactivation of unused accounts.

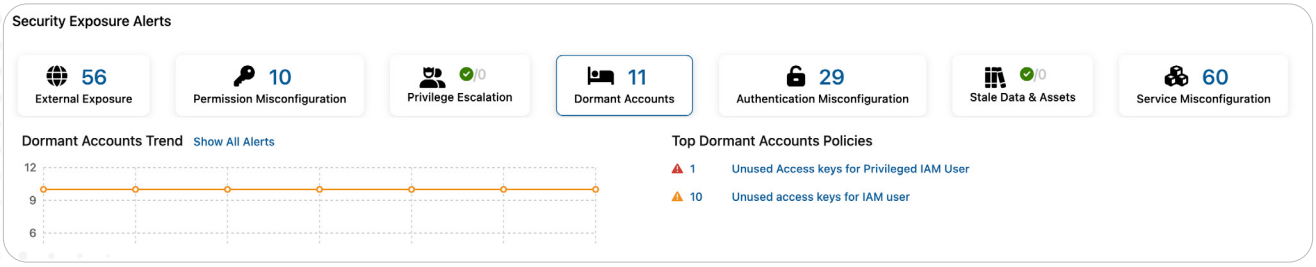
Cloud service providers offer multiple ways of applying AC to secure data in cloud-based workloads and services. However, as part of the shared responsibility model, it is the user's responsibility to assess the architecture of the necessary cloud service and apply the required access control configuration. The complexity and diversity of the services—combined with the multitude of security configuration options for each cloud service spread across multiple service providers—represent a daunting task for organizations that must gain enough risk and asset context to apply effective access control policies at scale.

Posture Control analyzes the cloud configuration metadata and identifies misconfigurations related to network access policies and storage access policies, as well as identity and access management policies for the various cloud services.

Policy ID	Control No	Policy Name	Cloud	Type	Category	Severity	Passed Assets	Status
ZS-AZURE-00071	AC-2	Ensure that 'Public access level' is set to Private...		Predefined	Access Control	High	9 / 11	Failed
ZS-GCP-00062	AC-2	Ensure API keys are not created for a project		Predefined	Access Control	Low	0 / 0	Manual
ZS-AWS-00024	AC-2	Ensure that S3 Buckets are configured with 'Blo...		Predefined	Access Control	Medium	49 / 54	Failed
ZS-AWS-00085	AC-2	Ensure credentials unused for 45 days or greate...		Predefined	Access Control	High	0 / 0	No Resour...
ZS-GCP-00068	AC-2	Ensure that there are only GCP-managed servic...		Predefined	Access Control	Medium	0 / 0	No Resour...
ZS-GCP-00063	AC-2	Ensure API keys are restricted to use by only sp...		Predefined	Access Control	Medium	0 / 0	Manual
ZS-GCP-00071	AC-2	Ensure user-managed/external keys for service ...		Predefined	Access Control	Medium	0 / 0	No Resour...
ZS-AZURE-00009	AC-2	Ensure FTP deployments are disabled for Web a...		Predefined	Access Control	High	0 / 0	No Resour...
ZS-AZURE-00034	AC-2	Ensure that Register with Azure Active Directory...		Predefined	Access Control	High	0 / 0	No Resour...
ZS-AZURE-00006	AC-2	Ensure FTP deployments are disabled for API app		Predefined	Access Control	High	0 / 0	No Resour...
ZS-AZURE-00007	AC-2	Ensure FTP deployments are disabled for Functi...		Predefined	Access Control	High	0 / 0	No Resour...
ZS-AWS-00084	AC-2	Ensure there is only one active access key availa...		Predefined	Access Control	High	0 / 0	No Resour...
ZS-GCP-00067	AC-2	Ensure that Security Key Enforcement is enable...		Predefined	Access Control	Medium	0 / 0	Manual
ZS-AWS-00090	AC-2	Ensure IAM users are managed centrally via ide...		Predefined	Access Control	High	0 / 0	Manual

Figure 1: Example set of access control policies

Posture Control also detects unused cloud identities and surfaces risks associated with it. For example, it pinpoints unused application programming interface (API) keys that are associated with an identity and access management (IAM) user.



Workload Communications provides zero trust access control of application traffic for cross-cloud workloads or workload-to-internet communications, extending the same advanced threat and data protection capabilities that are provided by Zscaler Internet Access to the cloud workloads.

Audit and Accountability

Audit and accountability (AU) is critical to ensure the integrity of an information system. The goal of this control category is to ensure organizations have the correct capability to validate if and when something has changed and who and what has made this change.

The cloud represents a dynamic IT environment where new workloads and services are continuously built, modified, and destroyed. In such a highly active and mission-critical environment, keeping track of both authorized and unauthorized changes is extremely important for security governance, as well as for forensics and incident response.

Posture Control continuously tracks asset changes and maps out a timeline of events related to individual assets, while also mapping to an interrelated chain of events.

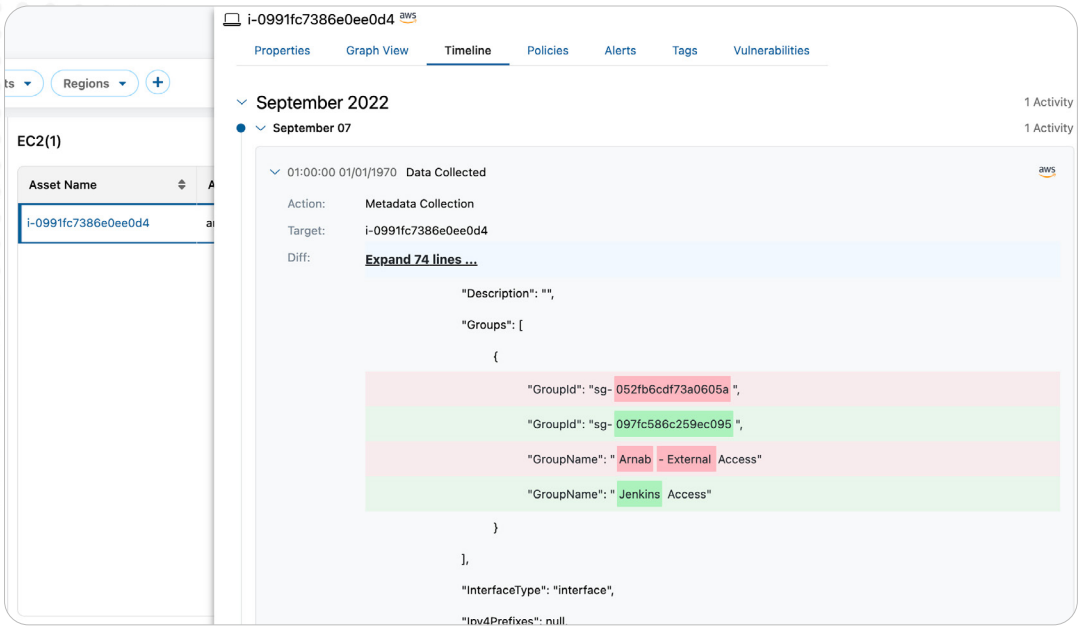


Figure 2: Audit of asset changes

Additionally, Posture Control provides context around change, potential impact, and any exploitation attempts related to that occurrence.

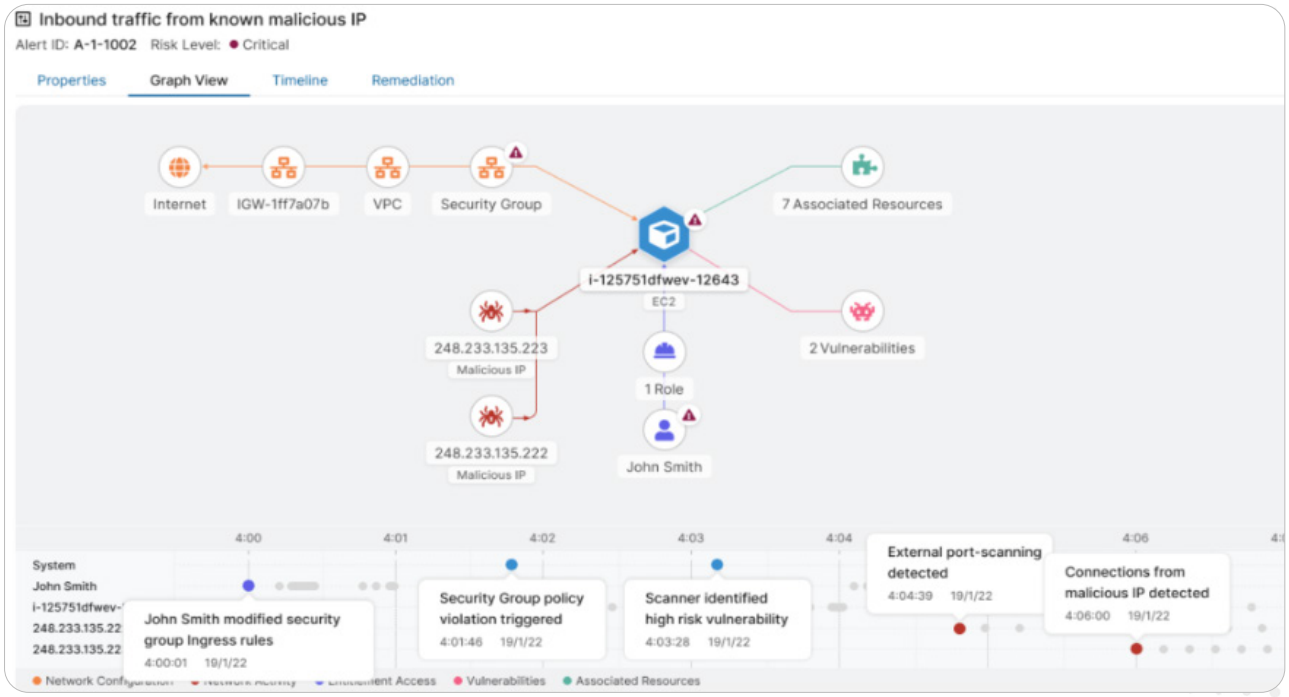


Figure 3: Correlated change and impact analysis

Assessment, Authorization and Monitoring, Identification and Authentication

In this section, we combined two control categories, assessment, authorization, and monitoring (CA) and identification and authentication (IA), as they all pivot around the identification of access attempts, authentication, and subsequent authorization. This control group is responsible for the application of least privileged access, as well as ensuring effective monitoring of the authentication and authorization process.

Cloud environments require a continuous assessment to deliver security assurance and governance. In addition to monitoring cloud assets, continuous assessment should also include evaluation and monitoring of cloud identities and their related entitlements. This ensures strict governance over who and what has access to specific cloud services and how the authorization model is enforcing least-privileged access. Identity and access management are one of the foundational elements that provide this capability. Most online services rely on this critical capability to secure API interactions between cloud administrators and services, as well as to secure workload-to-remote service interactions. In addition to securing human identities, the cloud also requires security for machine identities (examples: service principals, IAM instance profiles).

To deliver these requirements, Posture Control provides two core capabilities:

1. Continuous discovery of cloud assets, a centralized asset inventory, and mapping of the discovered assets to that of the associated identities, along with their effective permissions on other cloud resources.

2. Continuous assessment of asset posture against hundreds of predefined security governance policies.

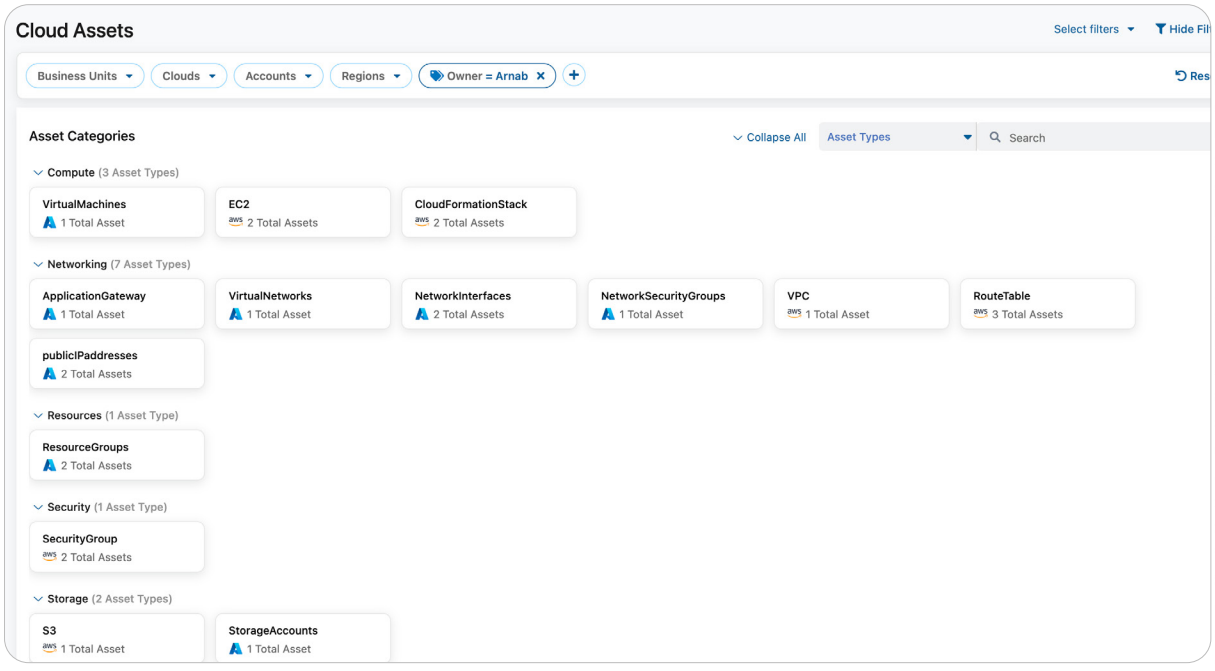


Figure 4: Multicloud asset inventory

The solution also automatically categorizes privilege drift over a period of time, where the effective permission of identity might give it service-level administrator privileges, bypassing the original scope of the identity and access management role.

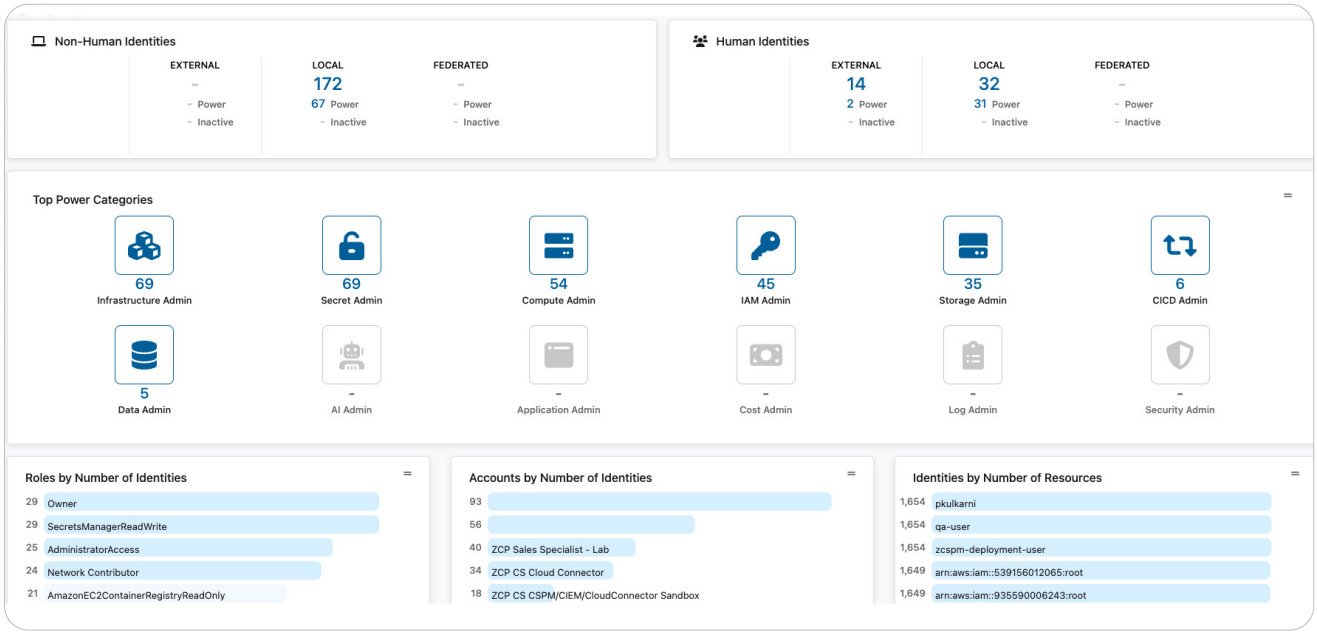
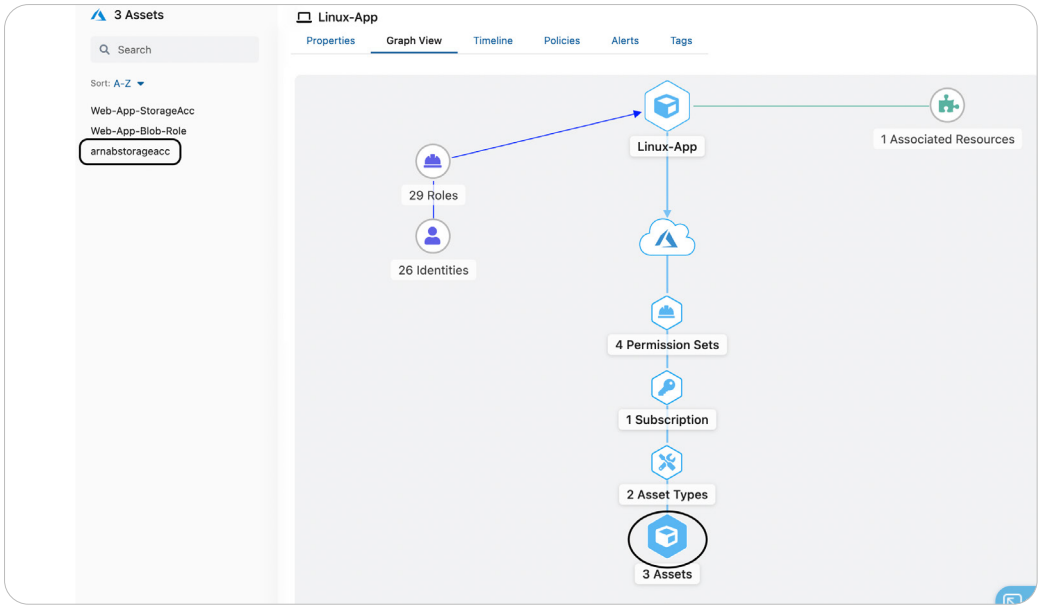


Figure 5: Multicloud visibility over cloud-user and machine identities permissions and IAM privilege drift

Posture Control also monitors for possibilities of lateral movement through cross-account/external identities (example: guest users in the Microsoft Azure Active Directory) by highlighting entitlements associated with non-organizational identities and making them highly visible through simplified dashboards.

Figure 6: Continuous visibility into human and machine identities and asset relationship



In the above example, the Posture Control asset graph continuously assesses and maps the relationship between the machine identity of the workload and its ability to have authorized access to other assets such as a storage account in Microsoft Azure. Similarly, the solution has advanced capabilities to continuously assess and detect the multilayer attack paths that have the potential to subvert role–based access control (RBAC) and monitor identity–related suspicious activities. An example would be the creation of new access keys for existing identities that might open additional paths to breaches via misconfigured or malicious modification of cloud identities.

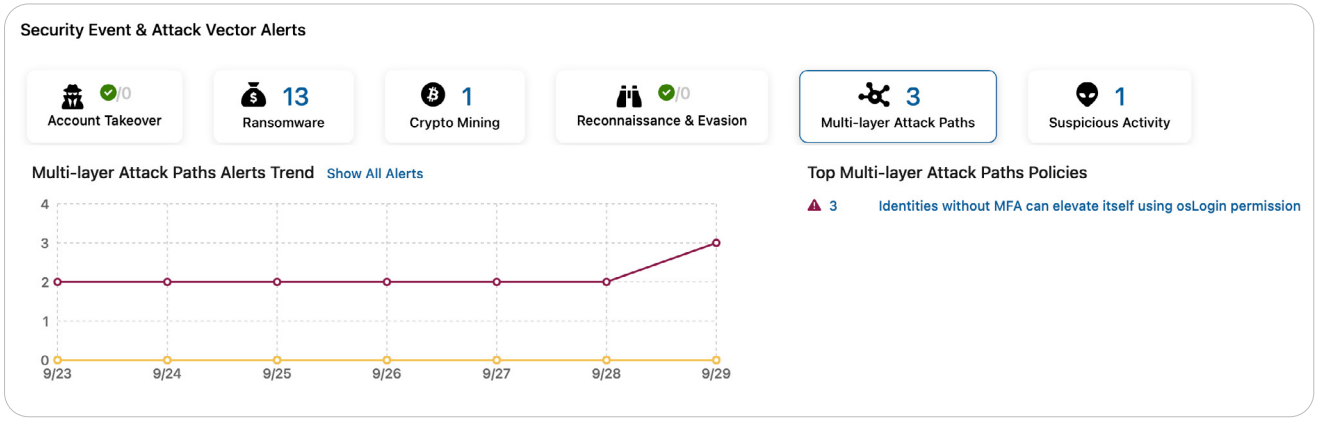


Figure 7: Ability to classify multiple paths to potential identity misuse

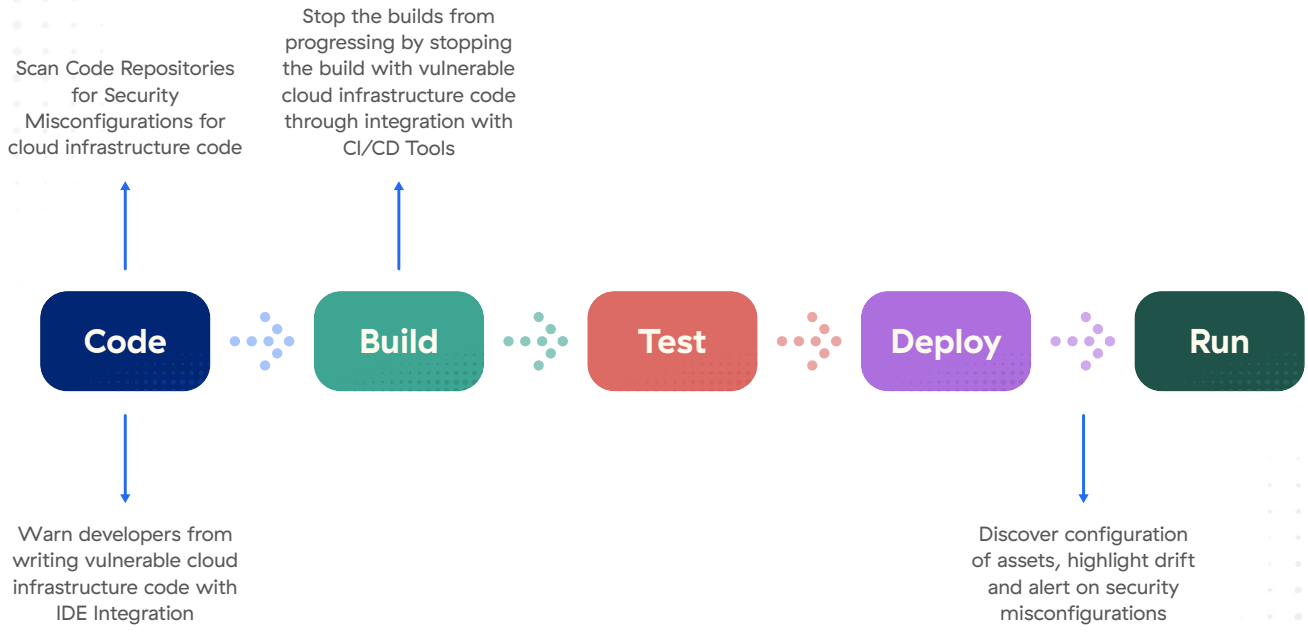
Configuration Management

Effective configuration management (CM) is critical to ensure consistency in security controls and verification that the system remains secure throughout its lifecycle of changes.

In the context of the cloud, this creates an effective conflict of interest because, by nature, the cloud was born to be agile and developer–oriented so applications can be built, deployed, and delivered faster. However, this scale is achieved through high levels of automation and continuous updates, along with changes through the adoption of DevOps.

Enforcing cloud security policies that ensure immutability can stop policy drift. This critical capability is required for effective cloud security governance and to provide security oversight for cloud configuration changes.

Posture Control has multiple ways of providing insights into security policy drift with respect to changes in cloud configuration. First, the platform continuously tracks changes to cloud resources. Second, it enforces safety governance by integrating security policies directly into the DevOps lifecycle. This has a multipronged effect. It ensures the defined cloud security guardrails are consistently applied over the lifecycle of the application, and it drastically reduces the overhead of having to fix configuration drift or misconfigurations in production that was introduced due to application changes.



Posture Control makes it easy to integrate with the developer's native tools such as integrated development environments (IDE) and continuous integration/continuous delivery (CI/CD) tools. Examples are VsCode for IDE, GitHub, and Bitbucket for source code and Jenkins/Azure DevOps for CI/CD tools.

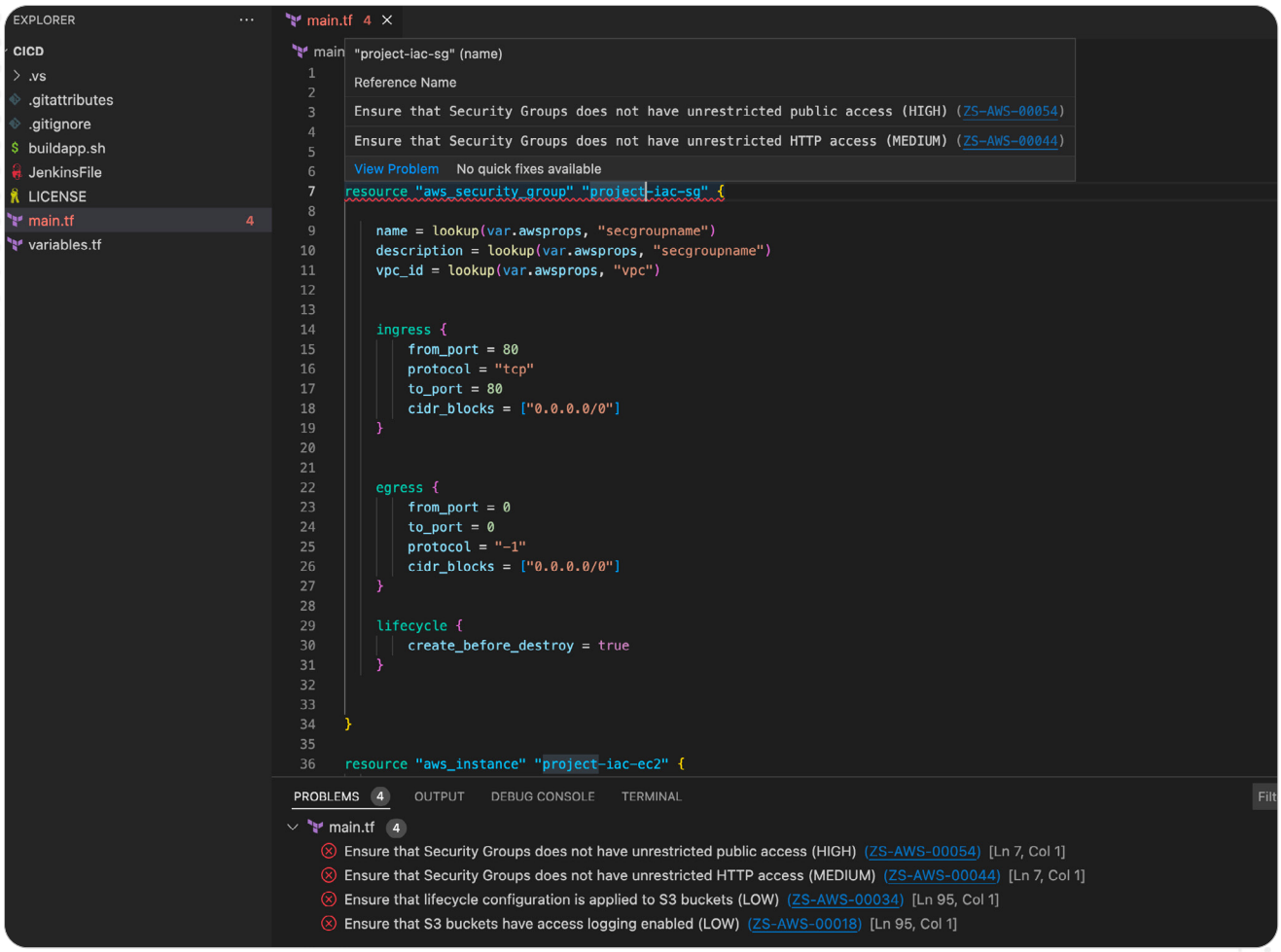


Figure 8: Integration with developer IDE

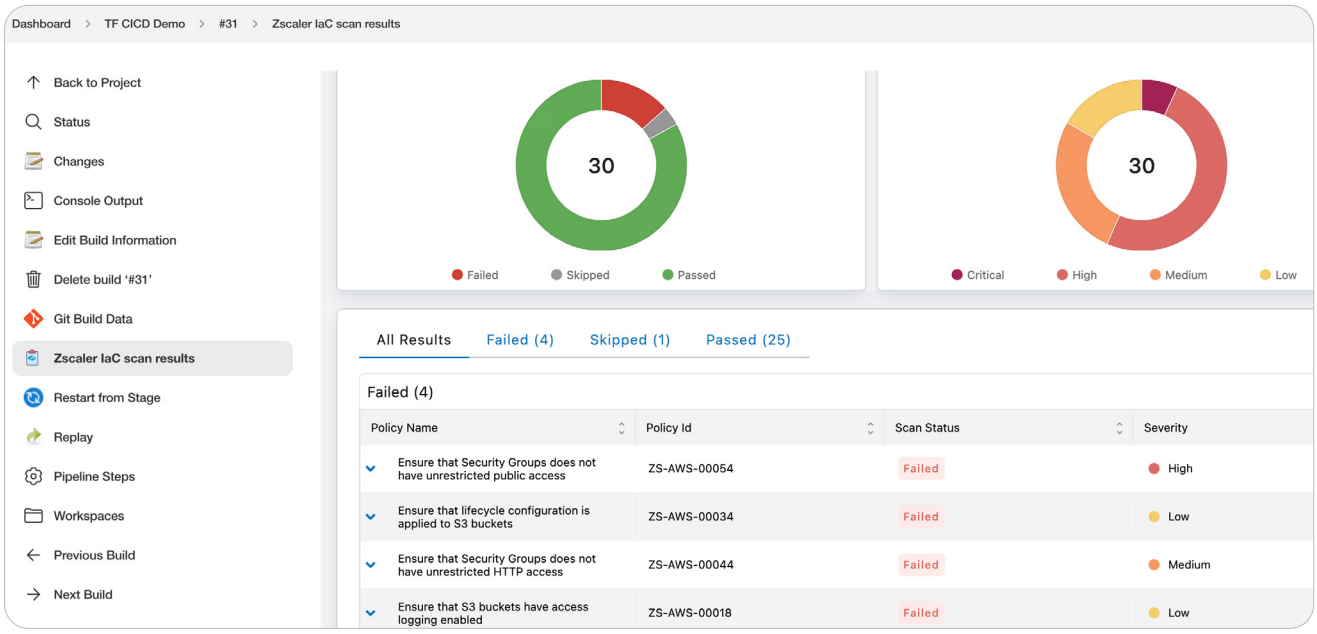


Figure 9: Using Jenkins integration to prevent security baseline configuration drift

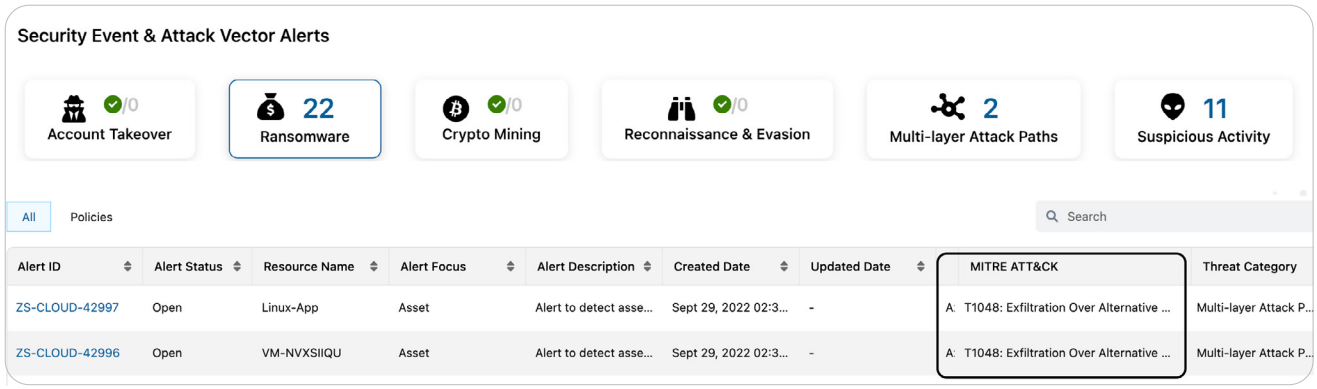
Incident Response

Incident response (IR) is a critical control category and a core function of any security practice. An effective incident response capability that manages the risks of an enterprise attack surface and detects as well as responds to threats quickly is core to every organization's cyber resilience.

Incident response remains a critical function of a cloud security/SecOps team, as cloud incidents generally have a higher potential for business impact due to extensive levels of exposure. However, incident responders may lack cloud architecture, asset context, and exposure information that would help them build an effective investigation for their cloud environments. There is also a problem with multiple security tools generating alerts that are isolated from each other, which results in alert fatigue.

Zscaler Posture Control helps cloud IR teams with the following capabilities:

1. **Alert prioritization:** Any alerts that are generated on an asset are cross-correlated for threat context and potential impact. Threats are categorized based on policies that are mapped to the MITRE ATT&CK® Framework.



2. **Incident timelines:** Most security incidents are a chain of events that ultimately lead to a vulnerability being exploited and an organization being impacted. The first task in an IR scenario is to establish the attack timeline. Posture Control combines configuration change timelines with exposure, vulnerability, and threat intelligence information to provide a comprehensive view of the attack timeline, drastically reducing the mean time to respond (MTTR).

Figure 10: Incident timeline

3. **Custom cloud investigations:** A key part of the incident triage process is to gather additional information on the impacted asset or to gain insight on finding all VMs with exposed ports to the internet, as these may have further access via IAM to supplementary services. This type of capability is vital for SOC analysts because it allows deeper scope into their incident investigation.

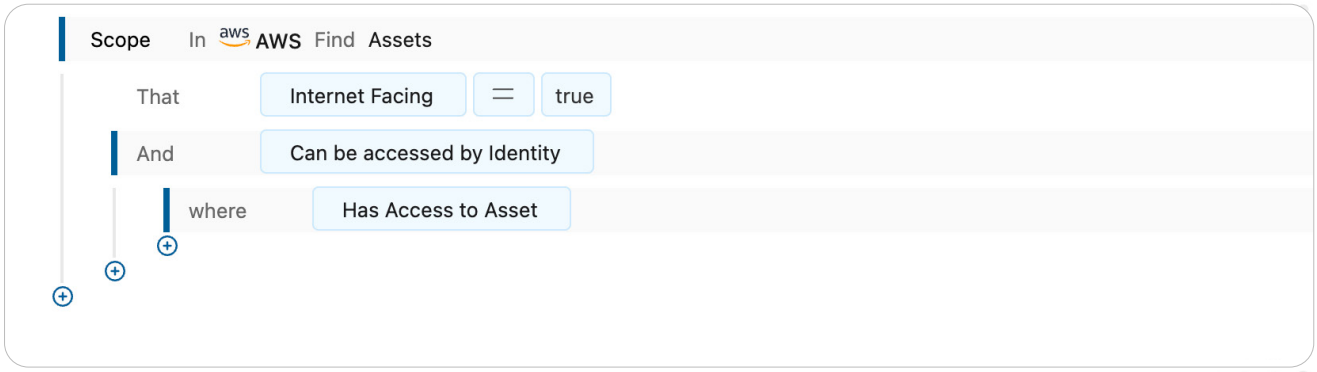


Figure 11: Quick query to gain cloud asset exposure and context

4. **Closing the IR loop of detection to remediation:** One of the final steps of IR is to remediate the risk and set up guardrails to detect future activity. This is easily achieved by converting the above query into a custom alert policy that gets triggered upon matching the same criteria. The solution also provides guided remediation and risk mitigation steps, helping organizations that lack specific cloud service knowledge to effectively remediate.

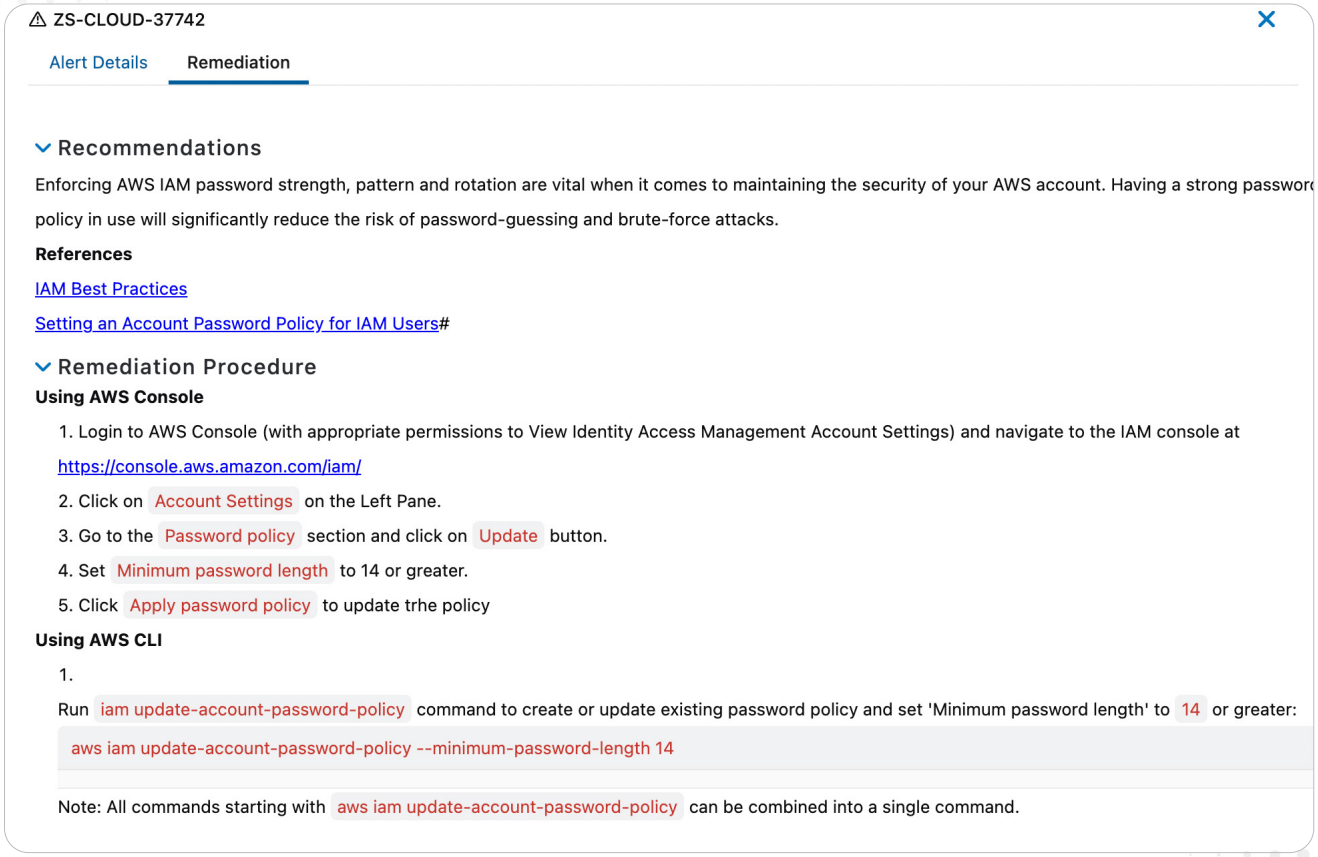


Figure 12: Guided remediation

PII Processing and Transparency

The PII processing and transparency (PT) control group's primary aim is to ensure the identification of sensitive data and the application of adequate security controls to that information. The Zscaler platform provides comprehensive capabilities to cover these requirements.

Zscaler Cloud DLP scans cloud storage locations such as Amazon Web Services S3 (AWS S3) and finds sensitive data. Posture Control then assesses the security controls of cloud data stores and ensures application of adequate access controls, code settings, and correct setup of data encryption keys, as well as data lifecycle policies. Finally, Workload Communications enforces network/web DLP capabilities for outbound traffic, blocking exfiltration of sensitive information.

Risk Assessment

Risk assessment (RA) is a critical component of an effective security program. It allows organizations to measure and establish metrics around the effectiveness of their security strategy and controls.

Posture Control performs deep cloud risk assessment by comparing the configuration state of the cloud environments to the best practices recommended by Cloud Service Providers (CSP) and well-architected security frameworks. The solution performs risk assessment in two key stages:

1. **Prioritized risk assessments:** This is driven by identifying the key risk indicators (KRIs) that have maximum potential to impact confidentiality, integrity, and availability of the cloud environment. A prioritized list of potential cloud threats is displayed on the dashboard to allow for quicker surfacing of critical infrastructure weaknesses so that they can be remediated before becoming a potential breach.

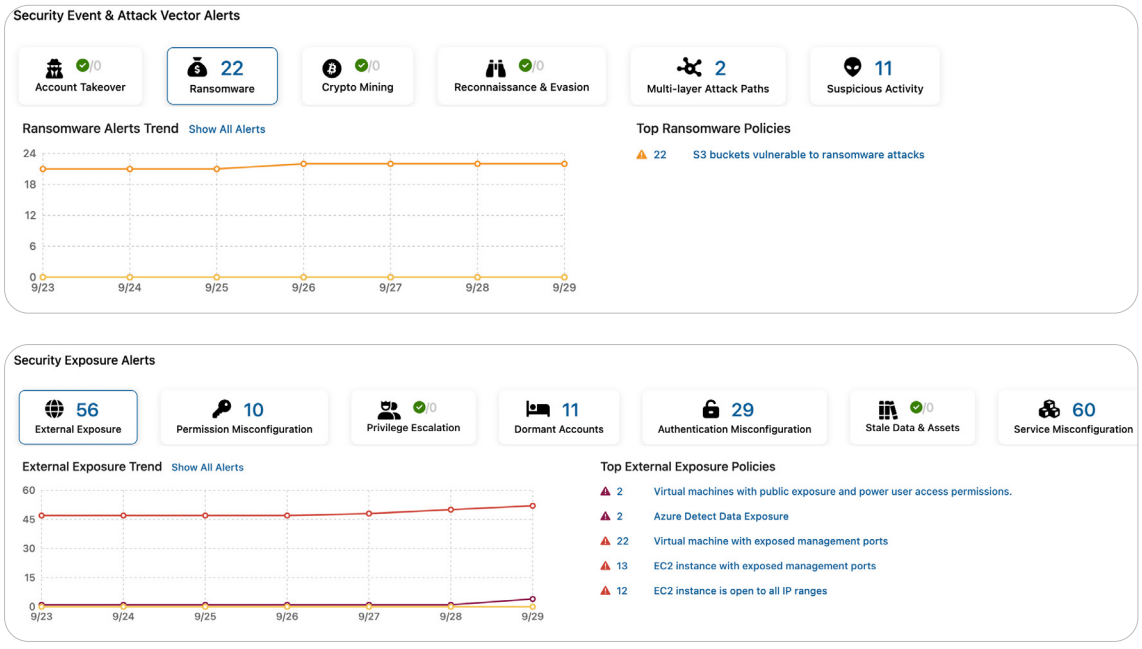


Figure 13: Prioritized risk assessment

2. **Policy-driven risk assessments:** The solution offers thousands of pre-built risk assessments based on a number of control frameworks such as PCI DSS, SOC2, NIST 800-53 rev 5 (including sub controls), CIS, and more.

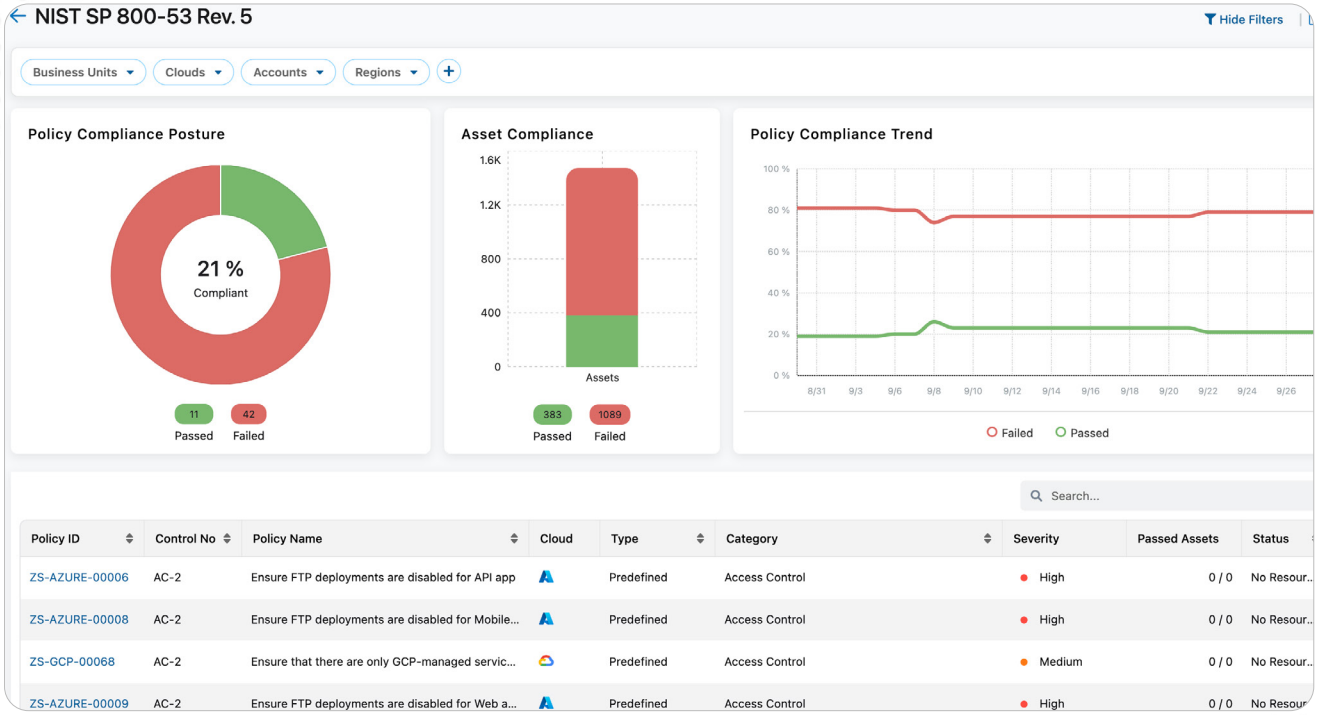


Figure 14: Policy-based risk assessment

The solution also allows for the creation of tailored risk assessments based on existing frameworks by allowing the creation of custom benchmarks.

Systems and Communications Protection

The systems and communications protection (SC) category of controls ensures that the Zscaler zero trust platform provides comprehensive protection for cloud workloads. This includes defense from network-borne cyberthreats and data protection via a simple model that unifies policies across multicloud environments. Zscaler provides secure workload-to-internet and workload-to-workload communications built on a zero trust foundation.

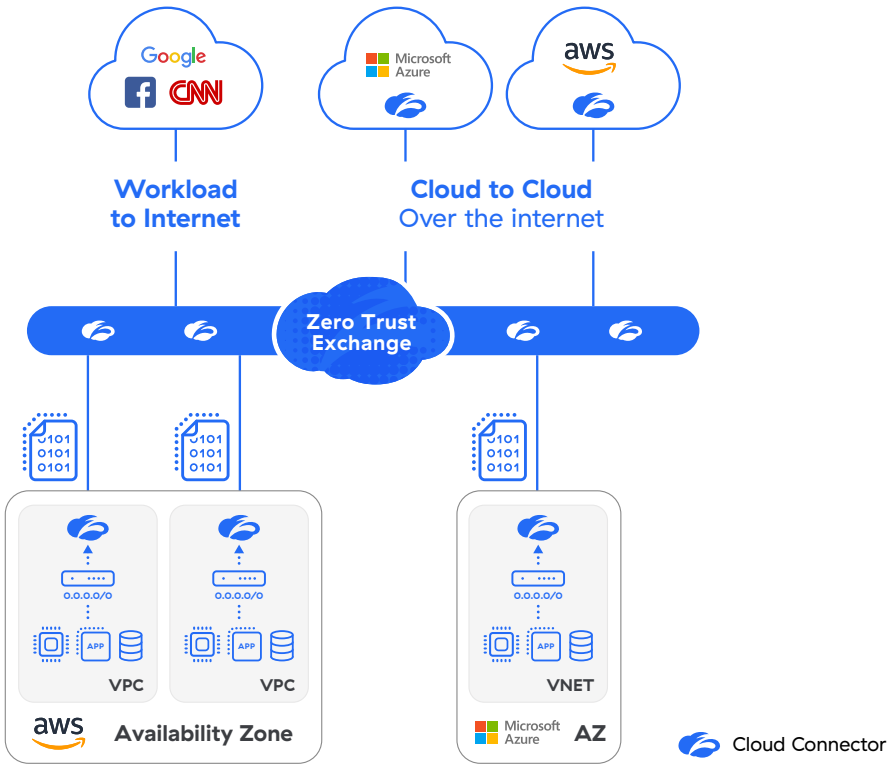


Figure 15: Zscaler zero trust for workload communications

Posture Control also detects misconfigurations related to network setup, such as security groups and encryption on data that could result in unwanted exposure, as well as data breaches.

System and Information Integrity

The aim of the system and information integrity (SI) control group is to have effective visibility and processes around vulnerability management of security controls that affect the integrity of the system and sensitive data. In the public cloud, this boils down to addressing vulnerabilities in the cloud software supply chain, such as VM or container images, as well as ensuring the proper policies are applied against tampering with data and workloads.

Posture Control provides agentless vulnerability scanning of cloud workloads and container images.

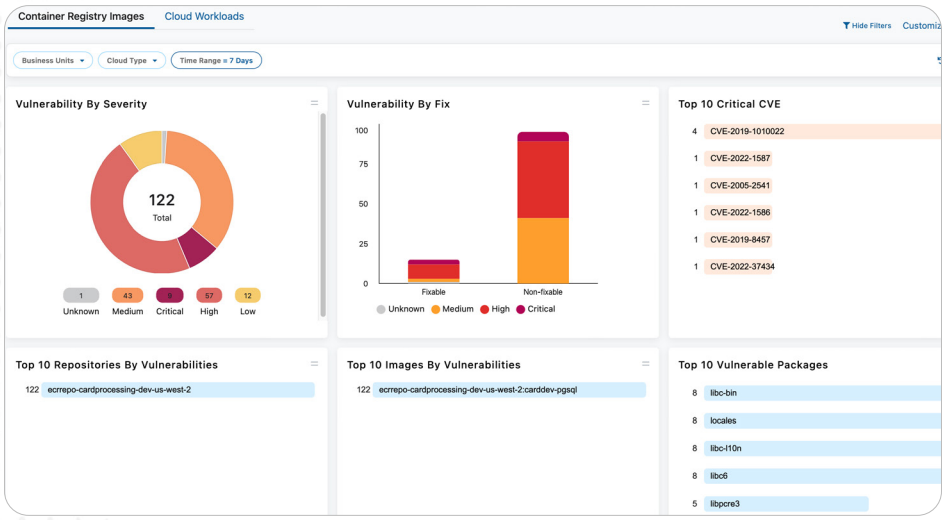


Figure 16: Agentless vulnerability scanning

In addition, the platform provides policies to assess weaknesses in cloud logging, as well as authentication weaknesses that might result in denial of validity.

Supply Chain Risk Management

Supply chain risk management (SR) is a critical control in the context of the cloud. The agile development cycle of cloud applications is predicated on the reusability of code, which means that any kind of vulnerability in the reused code can spread rapidly across hundreds of workloads.

Posture Control creates a centralized inventory of cloud vulnerabilities, making it easy to search and group associated impacted images or workloads.

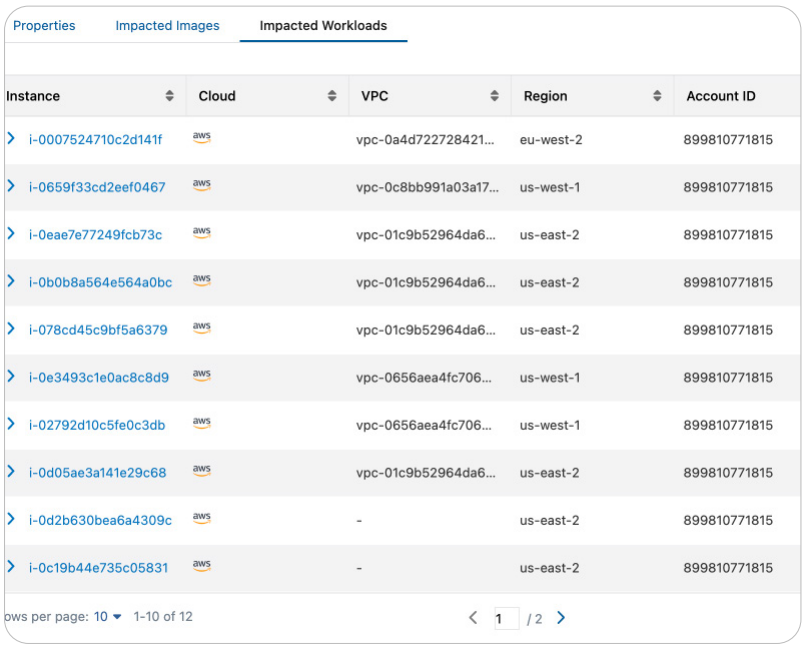


Figure 17: Quick scoping of all impacted workloads against a vulnerability

Summary

Zscaler for Workloads provides comprehensive capabilities to allow organizations to rapidly adopt compliance frameworks such as NIST 800-53. Zscaler for Workloads allows organizations to garner holistic cloud security capabilities that are developer-first, threat-informed, and operationally efficient. This ultimately helps businesses securely accelerate their cloud adoption journey, while helping security teams focus on strategic goals.

So, what's next? Give us an opportunity to be your mission partner in delivering a secure cloud infrastructure. Zscaler Posture Control provides an assessment of your cloud infrastructure today and helps you build security processes for tomorrow.

Learn more about Zscaler Posture Control: zscaler.com/posture-control

Schedule a demo or try out our platform:
zscaler.com/products/posture-control#contact-us, or reach out to your Zscaler account manager.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com