proofpoint.

SOLUTION BRIEF

Proofpoint Cloud App Security Broker IaaS Protection

Identify Misconfigured Cloud Services and Protect Sensitive Data in IaaS Storage

CHALLENGES

- Misconfigurations
- Unknown resources and IaaS accounts
- Data loss and compliance
- Cloud account takeover

KEY CAPABILITIES

- Simplify multi-cloud security and compliance with centralised governance for all IaaS resources across vendors, accounts and regions
- Identify misconfigured security settings that deviate from published baselines
- Monitor and analyse user behaviour to detect and stop unauthorised logins and administrative activity
- Protect sensitive data in IaaS storage
- Discover and govern unsanctioned IaaS accounts
- Deploy quickly in the cloud

PRODUCTS

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint CASB IaaS Protection

Cloud adoption is accelerating. Just as business and IT teams opt to deploy SaaS apps to improve agility, elasticity and scale, so do DevOps teams. They are developing new applications and services on cloud infrastructure.

Your organisation may have tens or hundreds of IaaS accounts with workloads deployed on a single or multiple cloud services. Due to data privacy regulations, you may have to store your data on cloud repositories located in different regions of the world. The lack of visibility into the gaps in your cloud security posture can make it difficult to maintain IaaS security and ensure compliance and cloud threats such as compromised accounts and lack of well-trained staff can add to the complexity.

Customer misconfiguration, mismanagement and mistakes can lead to large-scale breaches. Attacks on cloud services such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud (GCP) can result from such oversight. Security and risk management leaders must identify and mitigate these risks. IaaS accounts, resources and sensitive data in cloud storage such as customer or patient records should be secured.

To protect your IaaS environments and ensure compliance, Proofpoint CASB IaaS Protection (IaaS Protection) provides

- IaaS discovery
- Cloud Security Posture Management (CSPM)
- Data security
- Threat protection
- Adaptive access controls

IaaS Protection is an add-on feature of Proofpoint CASB.

Identify misconfigurations in IaaS environments

IaaS Protection helps you govern security posture in your multi-cloud environment. This feature of Proofpoint CASB discovers configurations and settings that deviate from published baselines in IaaS services. That includes settings such as a "root" user account that is not enforcing multi-factor authentication. IaaS Protection evaluates your virtual machine, storage, network and access controls settings against the following four security baselines.

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

And when it identifies misconfigurations that present a security risk, it recommends the best practices for fixing them.

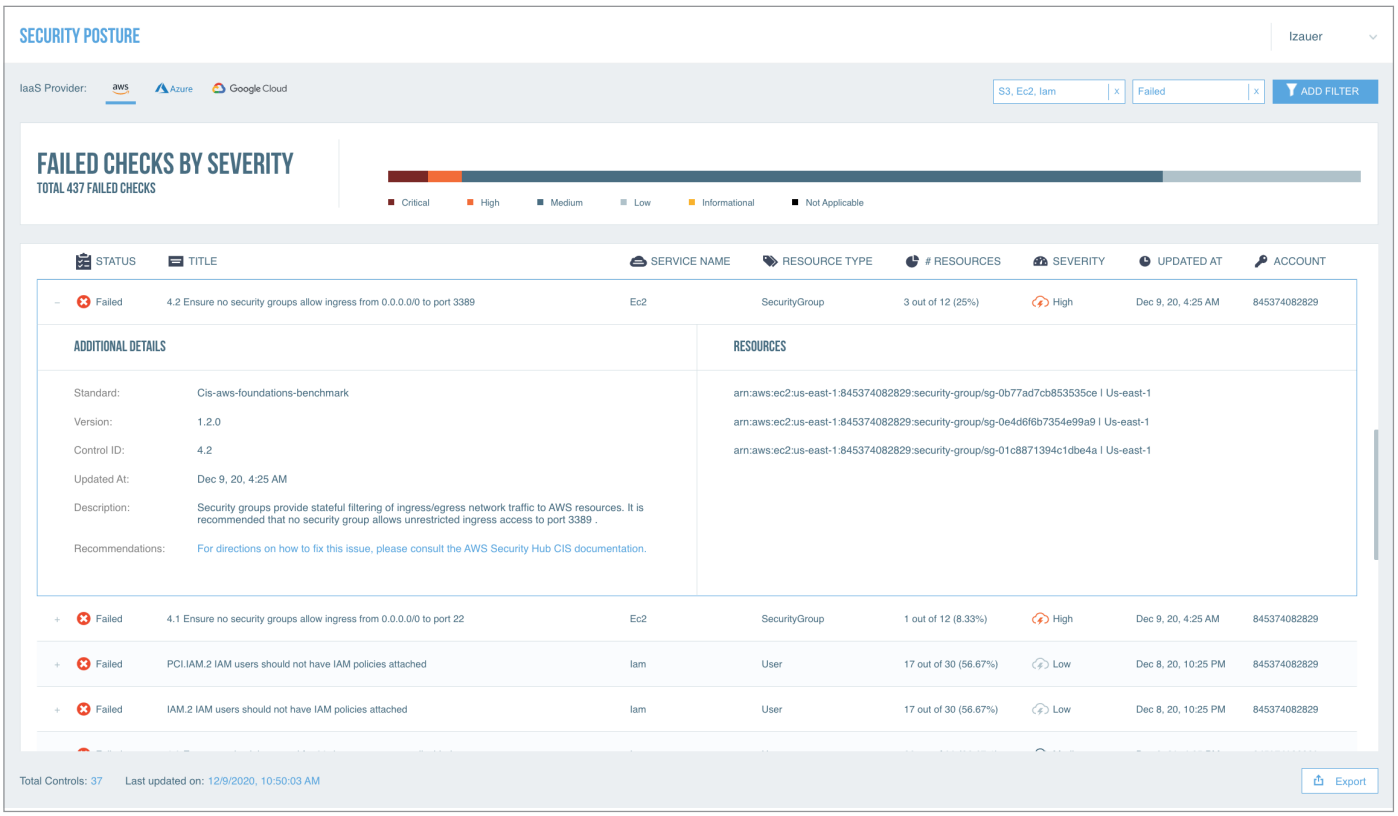

Figure 1: Security posture dashboard showing a misconfiguration, the instructions on how to meet the security baselines and a list of resources that failed to meet the standard.

Monitor and control privileged users activity

Unlike SaaS applications, most IaaS users are privileged users such as DevOps engineers or software developers. They can deploy, delete and configure IaaS resources such as virtual machines and cloud storage. And they can assign admin privileges. Monitoring privileged user activities is critical.

Proofpoint CASB with IaaS Protection enables you to set people-centric policies (Figure 2). Such policies are based on rich context and output alerts in the event of unauthorised privileged user activities. The context includes user risk, location, device and network, as well as any cloud app the user is trying to access. For example, you can prevent admin activities such as changes to bucket permissions from block-listed countries.

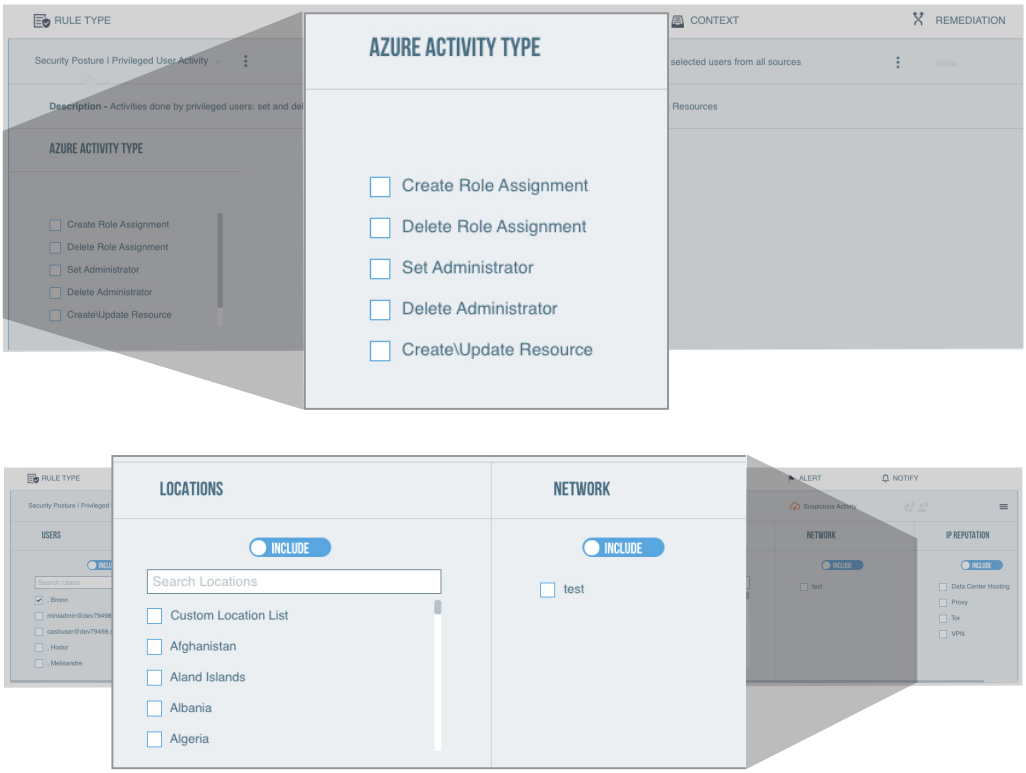

Figure 2: Policy rule template for privileged user activities.

Discover all IaaS resources

With Proofpoint CASB, you can simplify multi-cloud and multi-region IaaS security and compliance with centralised management. And you get visibility of all your SaaS apps and IaaS resources across IaaS vendors, accounts and regions (Figure 3).

You can visualise resource creation trends and look for anomalies such as excessive resource creation or deletion. You can also drill down into discovered resources by type and region and ensure that accounts are provisioned according to regulations and best practices—for example, if you are a multi-national or European organisation, you can monitor for buckets deployed outside of the EU to prevent GDPR violations.

Discover unprovisioned IaaS accounts

Proofpoint CASB gives you visibility into shadow IT across your organisation. This includes IaaS accounts that are not approved or documented by IT (Figure 4). We help you audit network traffic logs. You can discover cloud apps and IaaS accounts accessed on your network. These can include IT approved, undocumented and possibly private IaaS accounts. As you audit unapproved accounts, you can track their status in the CASB console. For example, after discovering undocumented accounts acquired during a merger, you can provision them according to security benchmarks to ensure compliance.

Figure 3: IaaS discovery dashboard showing resource trends, locations and types.

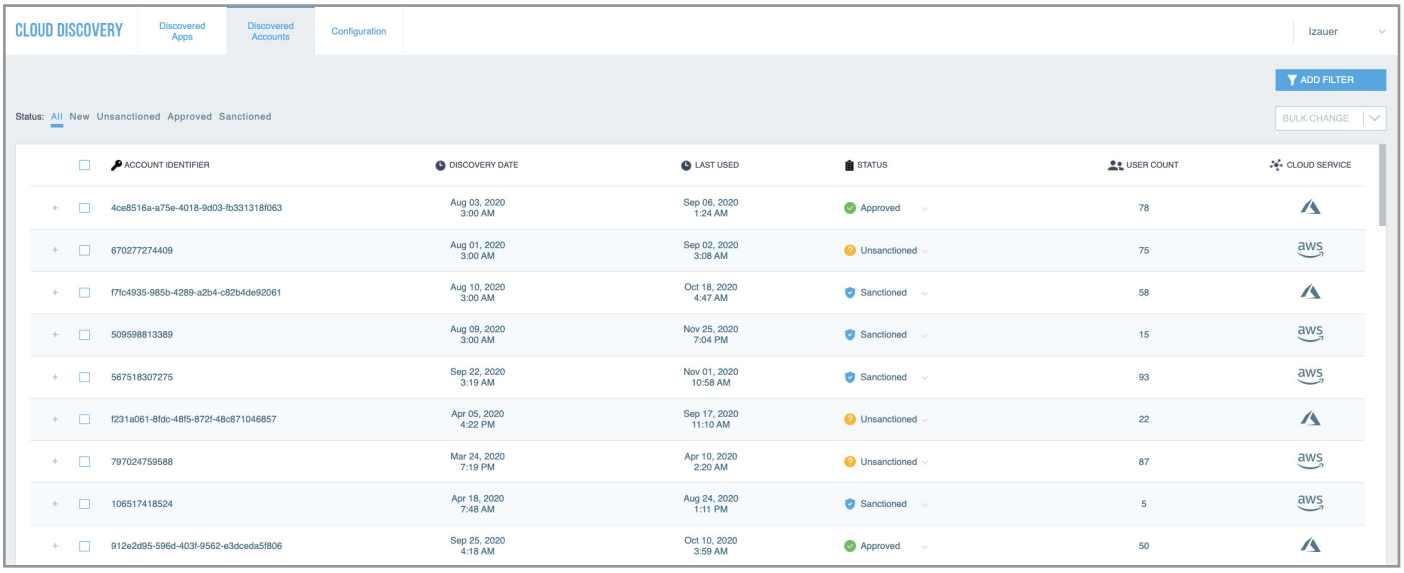

Figure 4: Dashboard showing status of IaaS accounts discovered on the corporate network.

Protect sensitive data in cloud storage

Proofpoint CASB with IaaS Protection helps you identify and classify sensitive data in your cloud storage repositories, such as AWS S3 buckets and Azure Storage Blob containers. It also helps you:

- Monitor file activities for DLP violations
- Monitor buckets and containers for excessive sharing
- Build data security policies using DLP classifiers—including built-in smart identifiers, dictionaries, rules and templates that are shared with other Proofpoint DLP products

Our out-of-box classifiers help you shorten the time needed to discover and protect regulated data in cloud storage and it helps you remain compliant. As part of Proofpoint Enterprise DLP, our CASB enables you to deploy consistent DLP policies across your SaaS apps, IaaS buckets, email and endpoint. And it lets you centralise DLP incident management for these channels on a single console. Combining content, behaviour and threat telemetry across multiple channels helps you determine whether the user that triggered the DLP alert is compromised, malicious or negligent.

Proofpoint CASB DLP capabilities include:

- 240 built-in classifiers covering PCI, PII, PHI and GDPR regulations
- Dictionaries and proximity matching to improve DLP detection
- Exact data matching to automate the upload of custom dictionaries or identifiers to detect information unique to your organisation—including account numbers and other structured data from databases
- Document fingerprinting to detect sensitive data within unstructured content—including formulas, source code, forms, contracts and other intellectual property
- Support for 300 file types and a file-type profiler to support new, custom or proprietary file types

Flexible rule templates allow you to build content, user behaviour and threat-aware policies (Figure 5). It lets you control how your data is shared, uploaded and downloaded. You can automatically reduce sharing permissions for buckets to ensure compliance. For example, you can monitor for and remove excessive sharing of buckets from block-listed countries.

Investigating DLP incidents is also easier. You can correlate suspicious logins or misconfigured buckets with DLP incidents. And you can filter events and alerts for reporting and closely monitor compliance by subscribing to alerts.

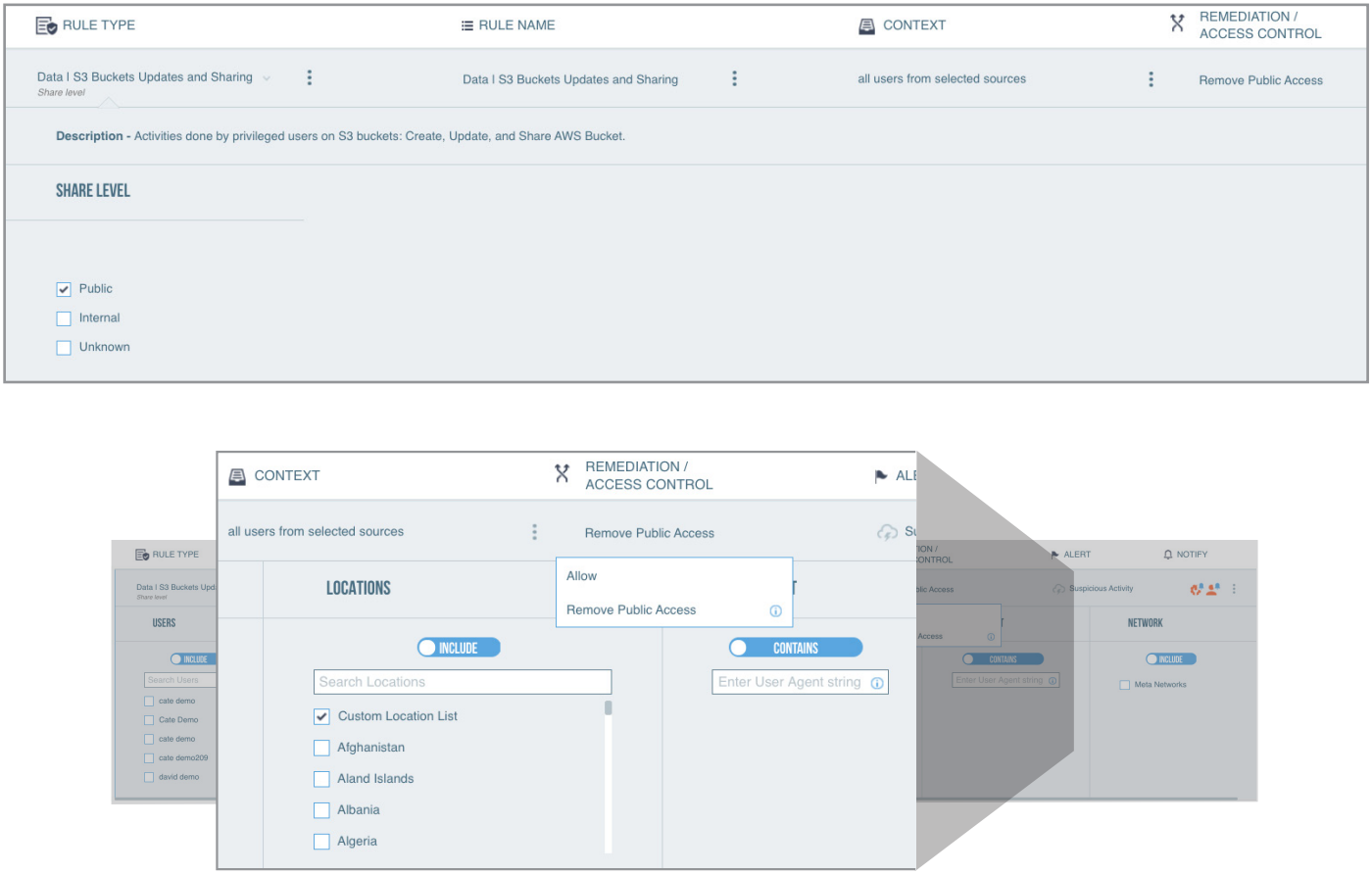

Figure 5: Policy rule template to monitor bucket/container sharing permissions.

Adaptive access controls and threat protection

IaaS management console is a web-based application used to create and manage cloud resources. Organisations need to monitor and control access to this powerful tool. CASB's adaptive access controls enable real-time security measures based on risk, context and role. It lets you:

- Protect your IaaS environment by setting up policies to block access from risky locations and networks and by known threat actors.
- Apply risk-based controls to high-risk and high-privilege users including step-up authentication, managed-device policy rules and VPN enforcement

Proofpoint CASB combines rich cross-vector (cloud, email and more) threat intelligence from Proofpoint Nexus Threat Graph with user-specific contextual data. We apply machine learning to this data to analyse user behaviour and detect anomalies across cloud services and tenants. We help you:

- Detect when a cloud account is compromised
- Investigate past activity and alerts, including any suspicious access to your federated IaaS services.

LEARN MORE

For more information, visit **proofpoint.com**.