DATA SHEET

PCI Compliance Made Easy with Fugue

Organizations that handle credit card information must be compliant with PCI Data Security Standards (PCI), a compliance standard for protecting payment cardholder data. If your organization accepts or processes payment cards, PCI applies to you.

PCI is categorized into 6 high-level goals mapped to 12 requirements based on security best practices that address technical and operational components connected to cardholder data. While all six goals are important for overall PCI compliance, not all of them are of direct concern for assessing cloud infrastructure compliance.

KEY PCI GOALS MOST RELEVANT FOR CLOUD ORGANIZATIONS:

Build and Maintain a Secure Network

Protect Cardholder Data

Implement Strong Access Control Measures

Regularly Monitor and Test Networks

Fugue helps to address the following 4 goals which are the most relevant for organizations in the cloud:

Build and Maintain a Secure Network

If a payment system network is not secured, malicious individuals can access it and steal cardholder data and sensitive authentication data. Fugue helps ensure that network security controls are in place to prevent unauthorized incoming and outgoing traffic. Fugue also identifies security parameters that have not been changed from insecure default settings.

For example, Fugue detects VPC security groups that violate PCI control 1.2.1, "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." If a security group rule permits ingress from 0.0.0.0/0 to all ports, for example, Fugue identifies the violation. And if the ingress rule drifts from a known-good baseline while enforcement is enabled, Fugue auto-remediates the rule back to its compliant state.

Protect Cardholder Data

Preventing malicious individuals from accessing sensitive payment information is one of the most important parts of PCI compliance. Not only does a compromised payment card hurt the customer, it hurts your business. Fugue helps ensure that an organization protects data through encryption and not storing cardholder data unless truly necessary.

For example, PCI 3.1 states that organizations should limit cardholder data storage and retention times to what is required for business and regulatory needs. Fugue helps organizations maintain compliance with PCI 3.1 by detecting whether automated RDS backups specify a retention period. Backups should not be retained longer than is strictly necessary.

Implement Strong Access Control Measures

The more people who have access to cardholder data, the higher the risk of a breach is. Access should be granted on a need-to-know basis to ensure the data can only be accessed by authorized personnel. By ensuring access control systems are implemented, Fugue helps prevent data from being mishandled through accident or malice, limiting the potential scope of damage.

A well-known best practice for security is the principle of least privilege. PCI 7.1.2 states "Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities." For example, Fugue detects IAM policies that grant full "*:*" administrative privileges and marks them as non-compliant, which helps ensure non-sysadmin users don't have sysadmin permissions.

Regularly Monitor and Test Networks

The PCI Quick Reference Guide points out that "networks are the glue connecting all endpoints and servers in the payment infrastructure." Malicious actors can exploit holes in a network to access payment card applications and cardholder data. Fugue combats this by ensuring networks are monitored and log files are protected.

For instance, PCI 10.5 states "Secure audit trails so they cannot be altered." Fugue promotes compliance with PCI 10.5 by identifying CloudTrail log files that have not enabled log file integrity validation and marking them as non-compliant. This helps ensure that malicious users are unable to cover their tracks by editing audit logs.

Ensuring PCI Compliance with Fugue

The PCI compliance standards applies to all organizations involved in storing, processing, or transmitting cardholder data or sensitive authentication data. Fugue ensures that cloud infrastructure stays in continuous compliance with enterprise security policies. Our solution provides insights into your PCI compliance posture by detecting cloud misconfigurations and compliance violations, enforcing baselines with codeless auto-remediation, and offering audit reporting with dynamic reports, dashboards and visualizations.

Sign up for a free compliance audit: https://resources.fugue.co/free-infrastructure-compliance-audit

About Fugue

Fugue ensures that cloud infrastructure stays in continuous compliance with enterprise security policies. Our product identifies security risks and automates compliance with out-of-the-box frameworks for the CIS AWS Foundations Benchmark, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. Fugue enforces infrastructure baselines with codeless auto-remediation to self-heal and provide visibility into unwanted changes. Organizations such as PBS, SAP NS2, and TrueCar trust Fugue to protect their cloud environments.