Otterize

PCI

DATASHEET

PCI

Requirements

- **PCI DSS Compliance:** The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
- **Alignment with Industry Security Frameworks:**
  - **OWASP Top 10:** Address critical web application security risks identified by OWASP, including injection flaws, broken access controls, and security misconfigurations.
  - **NIST Cybersecurity Framework:** Align with the NIST framework's 5 core functions – Identify, Protect, Detect, Respond, and Recover. Protect assets, detect and respond to threats, and recover from security incidents.
- **MITRE ATT&CK Framework:** Understanding attacker tactics and techniques as outlined in MITRE ATT&CK is essential for proactively defending against threats to cardholder data.

Platform SecOps

- **Centralized Application Traffic Monitoring and Security Management:** Unified view of application traffic across multiple clusters, hyperscalers and tenants to ensure security and compliance.
- **Simple Policy Enforcement:** Manual configuration of security policies is prone to errors and can't keep pace with the dynamic nature of cloud-native environments. Automation is essential for ensuring consistent and accurate policy enforcement.
- **Granular Access Controls:** PCI DSS mandates strict access controls to protect cardholder data. Platform and SecOps teams need tools to implement and enforce granular access policies, isolating sensitive workloads and restricting traffic flow.

CISOs

- **Mitigate Reputational Risk:** A data breach can irrevocably damage brand, erode customer trust, and lead to a loss of business. Robust security is essential to maintain a trustworthy image.
- **Mitigating Evolving Threats:** The threat landscape is constantly evolving, with attackers using sophisticated techniques to target cardholder data.
- **Maintaining Continuous Compliance:** PCI DSS compliance is an ongoing process, requiring regular assessments, vulnerability scanning, and updates to security controls.
- **Demonstrating Compliance:** PCI DSS requires organizations to provide evidence of compliance to auditors.
- **Balancing Security and Business Agility:** Strict security measures can sometimes slow down business operations.
- **Enable Business Growth:** PCI DSS compliance is often a prerequisite for partnering with payment processors and expanding into new markets.
- **Avoid Costly Fines & Penalties:** Non-compliance with PCI DSS can result in hefty fines, penalties, and increased transaction fees, posing a financial risk to the business.
- **Minimize Liability in Case of Breach:** In the event of a data breach, the financial and legal repercussions can be devastating. Strong security measures can limit liability.
- **Reduce Insurance Premiums:** Implementing strong security measures can help negotiate lower cyber insurance premiums.

Drivers

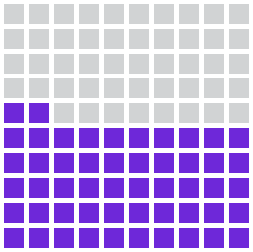
Protecting Cardholder Data:
PCI DSS mandates strict controls to prevent unauthorized access, use, or disclosure of cardholder data. This is key to maintaining customer trust and protecting brand reputation.

Mitigating Financial Risk:
Non-compliance can lead to significant financial losses due to fines, penalties, legal fees, and lost business.

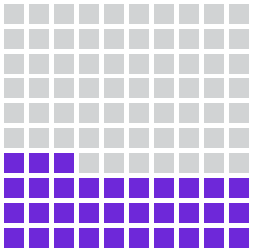
Safeguarding Business Reputation:
Data breaches involving cardholder data can severely damage brand image and erode customer trust, leading to a loss of customers and revenue.

Key Figures and Data

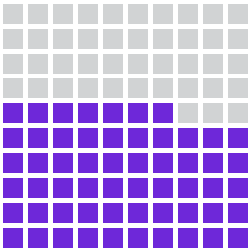
According to IBM Cost of a Data Breach Report 2023



52%
of all data breaches involved some form of customer Personally Identifiable Information (PII)

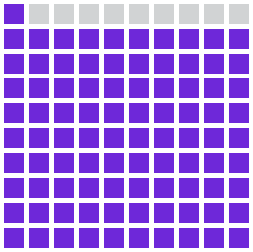


33%
of breaches were identified by the organizations' internal security teams and tools

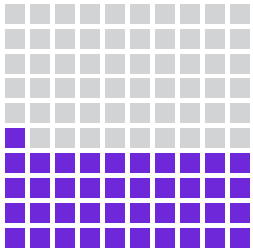


57%
of organizations that experienced a data breach had to increase the price of their business offerings and products.

Other key figures and data points



91%
of companies plan to implement continuous compliance in the next five years (Drata 2023 Compliance Trends Report)



41%
of businesses without continuous compliance report slowdowns on the sales cycle as a result (Drata 2023 Compliance Trends Report)

Average total cost of non-compliance according to Ponemon Reports

Cost of compliance

Benefits

Automated Microsegmentation for PCI Zones

- **Engineering:** Otterize automatically segments your cardholder data environment (CDE) according to PCI DSS requirements, ensuring proper isolation and access controls without additional development effort.

- **CISOs:** Simplify compliance and reduce the risk of human error by automatically generating audit reports that demonstrate adherence to PCI DSS segmentation requirements. Gain actionable insights into any violations, enabling you to proactively address them and further reduce the scope of PCI DSS audits..

- **Platform SecOps:** Reduce manual effort by automatically enforcing IAM and segmentation policies, ensuring consistent protection of cardholder data, and minimizing the operational burden on your team.

Zero-Trust Policy Enforcement for Cardholder Data

- **Engineering:** Otterize helps ensure that access to cardholder data is strictly limited to authorized users and applications, minimizing the risk of unauthorized access and aligning with secure coding practices.

  CISOs: Gain granular visibility into cardholder data access, providing the ability to detect and respond to potential threats quickly, thus reducing the impact of security incidents.

  Platform SecOps: Integrate with existing IAM systems, enabling easy access management to sensitive data in accordance with PCI DSS requirements and reducing the administrative overhead.

Automated Remediation of Security and Compliance Issues

- **Every insight and finding is actionable through Otterize.** Define global rules and let Otterize automatically remediate thousands of potential violations across your environment, ensuring continuous security and adaptive compliance without manual intervention.

Real-Time Compliance Monitoring & Alerting

- **Otterize's dashboard provides continuous visibility into security posture,** mapping your configurations to PCI DSS controls, OWASP Top 10 vulnerabilities, and NIST recommendations. This allows for proactive identification and remediation of potential risks.

- **CISOs:** Otterize streamlines compliance reporting and allows you to fix any detected gap, reducing the time and resources needed to demonstrate adherence to PCI DSS auditors. Non-compliant configurations are flagged in real-time, enabling automated remediation and minimizing the risk of costly violations.

- **Platform SecOps:** Leverage Otterize's centralized monitoring to detect and respond to security incidents promptly. The platform's alerting capabilities help identify suspicious activity, policy violations, and potential attacks, allowing for rapid investigation and containment by stopping lateral movement.

Empowering CISOs to Drive Organizational Change

- **Otterize not only provides technical solutions but also helps CISOs drive organizational change.** By clearly communicating security risks and demonstrating the business value of compliance, Otterize enables CISOs to influence development and DevOps teams to adopt security best practices and implement effective controls.

Guided Compliance Implementation

- **Otterize offers a guided compliance approach** to help organizations successfully navigate their PCI DSS compliance journey. It simplifies compliance processes by prioritizing actions, automating IAM and security policy generation and enforcement, and providing a unified view of security across multi-cluster and multi-cloud environments.

Competitive Advantage

Application-Aware Microsegmentation

- **Devs:** Otterize understands how applications work, enabling more precise and effective microsegmentation policies than traditional network-based solutions. This means less time spent on manual configurations and more focus on building secure applications.
- **CISOs:** Otterize's application-centric approach reduces the risk of over-segmentation, combining the right balance between security and functionality, while optimizing performance and minimizing disruptions to business operations.
- **Platform SecOps:** Otterize's dynamic policy generation adapts to changes within any cloud-native or on-prem environment, ensuring that microsegmentation and IAM policies remain effective even as applications evolve over time, reducing the need for constant manual intervention.

Granular Visibility and Control

- **CISOs:** Otterize provides deep visibility into application traffic and access patterns, allowing you to pinpoint weak links in the communication chain and identify unexpected traffic that doesn't comply with PCI DSS policies. This granular visibility enables you to make informed decisions about security policies and incident response.
- **Platform SecOps:** With Otterize's comprehensive monitoring and alerting capabilities, you can proactively detect anomalies, policy violations, and potential attacks. This provides faster response time to security incidents, minimizing their impact and the blast radius.

Proactive Security Posture

- **CISOs:** Otterize's proactive approach to security helps you stay ahead of the curve. By automatically generating and enforcing policies based on the latest security best practices, Otterize reduces your organization's risk profile and strengthens your defenses against emerging threats.

Actionable Insights and Automated Remediation

- **Otterize's actionable findings and automated remediation capabilities enable rapid response to security threats and compliance violations.** The platform integrates with popular ChatOps tools, allowing you to receive alerts and take action directly from your collaboration platforms. This accelerates incident response and reduces the risk of human error.

Key Features

- **IBAC:** Otterize automatically translates high-level security intent (e.g., "allow web servers to access databases") into detailed, granular access policies, abstracting away the complexities of network and application configurations. This ensures that access to cardholder data is tightly controlled and aligned with PCI DSS requirements.

- **Application Dependency Mapping:** Otterize automatically discovers and visualizes the relationships between applications and their components, including microservices, APIs, and data flows. This provides a comprehensive understanding of your cardholder data environment (CDE) and helps you identify potential security risks and dependencies.

- **Network Policy Automation:** Based on application dependency mapping, Otterize automatically generates and enforces fine-grained network policies (e.g., Kubernetes NetworkPolicies) to restrict traffic flow between application components. This ensures that only authorized communication is allowed within the CDE, reducing the attack surface and preventing lateral movement in case of a breach.

- **API & Microservices Authorization Policy Automation:** Otterize extends microsegmentation to Layer 7 by generating and enforcing authorization policies (e.g., Istio authorization policies) based on application roles and permissions. This provides more granular control over which workloads can access specific application features or cardholder data, enhancing security and compliance in both on-premises and cloud environments. Additionally, Otterize automates the configuration of cloud IAM roles and permissions directly within Kubernetes, as defined by developers, ensuring that policies align with the intended access requirements. This streamlines policy management and reduces the risk of misconfigurations.

- **PCI DSS Compliance Reporting:** Otterize generates detailed reports mapping your environment's security configurations to specific PCI DSS requirements. This simplifies audit preparation and provides evidence of compliance for internal and external audits.

- **Real-Time Threat Detection:** Otterize continuously monitors network traffic and system logs for suspicious activity, unauthorized access attempts, and potential policy violations. Early detection of threats enables faster incident response and reduces the impact of security breaches.

- **Automated Remediation & ChatOps Integration:** Otterize can automatically remediate security and compliance issues based on predefined policies. This minimizes the risk of human error and ensures consistent enforcement. Integration with ChatOps tools allows for real-time alerts and collaboration within your existing communication platforms, enabling swift action and faster resolution of security incidents.

- **Multi-Cluster Visibility:** Otterize provides a unified view of security policies and application traffic across multiple Kubernetes clusters, ensuring consistent security and compliance in complex environments.

- **Multi-Cloud Support:** Otterize works seamlessly across major cloud providers (AWS, Azure, GCP), ensuring consistent security and compliance policies for hybrid and multi-cloud deployments.

- **GitHub Integration (for DevSecOps):** Otterize continuously compares your defined security policies (ClientIntents) with actual application traffic. If discrepancies are detected, Otterize automatically creates a pull request in GitHub to update the ClientIntents, aligning them with the observed traffic patterns.

- **Agentless Deployment:** Otterize operates without requiring the installation of agents on individual workloads, simplifying deployment and minimizing performance overhead. It leverages existing Kubernetes infrastructure (e.g., service mesh) for visibility and policy enforcement.