VALTIX

CUSTOMER SPOTLIGHT:

PAYBYPHONE ACHIEVES SECURITY & PCI-DSS COMPLIANCE WITHIN AWS

paybyphone®

paybyphone®

Industry:
Mobile Payments

Headquarters:
Vancouver, BC, Canada

Employees:
250

Challenges:
Cloud Migration, Multi-Account Security, PCI-DSS Compliance

Outcomes:
Continuous Discovery, Intrusion Detection, Identity-Based Segmentation, Zero Management of Firewalls, Security Automation with Infrastructure as Code (IaC)

Security & PCI-DSS Compliance Within AWS

PayByPhone is one of the fastest-growing mobile payment companies in the world, processing more than 135 million transactions totaling more than $550 million USD in payments annually. Through the company's mobile web, smartphone, and smartwatch applications, PayByPhone, owned by Volkswagen Financial Services AG, helps millions of consumers easily and securely pay for parking without the hassles of waiting in line, having to carry change, or risking costly fines.

As PayByPhone transitioned to a cloud-first approach, a key initiative became to consolidate and modernize their approach to cloud security and compliance.

Senior Manager of Platform Infrastructure, Andrew Malady, and Senior Cloud Developer, Kevin Neufield, were tasked with building PayByPhone's go-forward cloud security architecture. One of their key responsibilities was to ensure that PayByPhone complied with PCI DSS (Payment Card Industry Data Security Standard) requirements. PCI DSS is a key payments industry requirement to meet minimum levels of security to store, process, and transmit cardholder data.

Architecturally, PayByPhone, like many in the retail industry, separates PCI data (cardholder) from non-PCI data (non-cardholder). Andrew and Kevin had nearly finalized their design based on AWS Security Groups when their auditor provided a new interpretation. Explained Kevin, "AWS Security Groups, while providing some basic network segmentation and east-west traffic control between PCI and non-PCI workloads, were not sufficient to meet our security requirements. Security Groups are simple, stateful firewalls that don't provide protection from malware-based attacks or stop exfiltration."

PCI also requires that outbound traffic be limited to approved destinations. Almost all modern applications connect outbound using the domain name or URLs of the destinations. But Security Groups and ACLs only support IP addresses, which is inadequate to meet PCI requirements.

To meet PayByPhone's needs, Andrew and Kevin would have to implement more robust cloud network security through a next-generation firewall (NGFW) plus intrusion prevention (IPS) to enable more granular segmentation. These security controls are coupled with an 'allow' list of approved domains for outbound traffic. Using FQDN and URL filtering allowed connections to be made based on the workload context (dev, test, prod, or cardholder). This best practice enables the prevention of lateral movement of threat actors and ultimately protects sensitive data from exfiltration to unknown sites.

Beyond enabling PayByPhone to meet these critical compliance requirements, the team prioritized finding a capability that didn't negatively impact agility. Andrew and Kevin needed to be able to leverage Terraform to automate security and compliance through Infrastructure as Code (IaC).

Explained Andrew, "Time was of the essence. We needed a solution that could handle our needs in a cloud-first way."

Legacy NGFW Proves Immature and Cumbersome For AWS Security

The PayByPhone team, Andrew and Kevin, began their search with their on-premises firewall vendor, who provided a virtual appliance (VA). While the VA NGFW seemed to check the boxes in terms of the compliance requirements, what they quickly learned was that implementation in the cloud was untenable.

Explained Kevin, "Our NGFW vendor provided an open-source Terraform provider for IaC (Infrastructure as Code), but it proved to be immature - capabilities were limited and support from the vendor was minimal. The legacy NGFW really lacked strong centralized cloud management as well."

Inevitably, these issues could result in costly and cumbersome maintenance as well as compromising security.

"Time was of the essence. We needed a solution that could handle our needs in a cloud-first way."

Andrew Malady, Senior Manager of Platform Infrastructure

The Valtix Solution: Cloud-first Approach to Network Segmentation and Intrusion Monitoring

Andrew and Kevin were connected to Valtix through their cloud architect. Explained Andrew, "Immediately we saw the promise of a cloud-first approach to network security, but what impressed us above all else was Valtix's ability to provide customer support as well as their attention to working with us to fully satisfy our PCI requirements." The Valtix team dove in to ensure the PayByPhone team could meet their project needs.

Continuous Discovery

Enables identification of cloud endpoints in order to better define segmentation.

Identity-Based Workload Segmentation

The primary requirement for Andrew and Kevin was to address PCI DSS and the need to segment cardholder from non-cardholder data.

FQDN Filtering With Forward Proxy

FQDN Filtering enables PayByPhone to block malicious or unauthorized activity from touching their cardholder environment. By implementing a whitelist approach, PayByPhone can lock their environment down to restrict connections to just what's allowed.

Intrusion Detection With SIEM Connector

By deploying Valtix Gateways, the PaybyPhone team is able to send a feed of network security activity through Valtix to a centralized security datastore for monitoring, alerting, analysis, and investigation.

Zero Management for Patching of Firewalls

One of the most exciting benefits of the Valtix solution, the PayByPhone team sees huge potential in terms of eliminating the need to maintain cloud firewalls. This will enable the team to stay focused on more important items and to continually respond to new business requirements and security threats versus just maintaining the security infrastructure.

Security Automation with Terraform-based Infrastructure as Code (IaC)

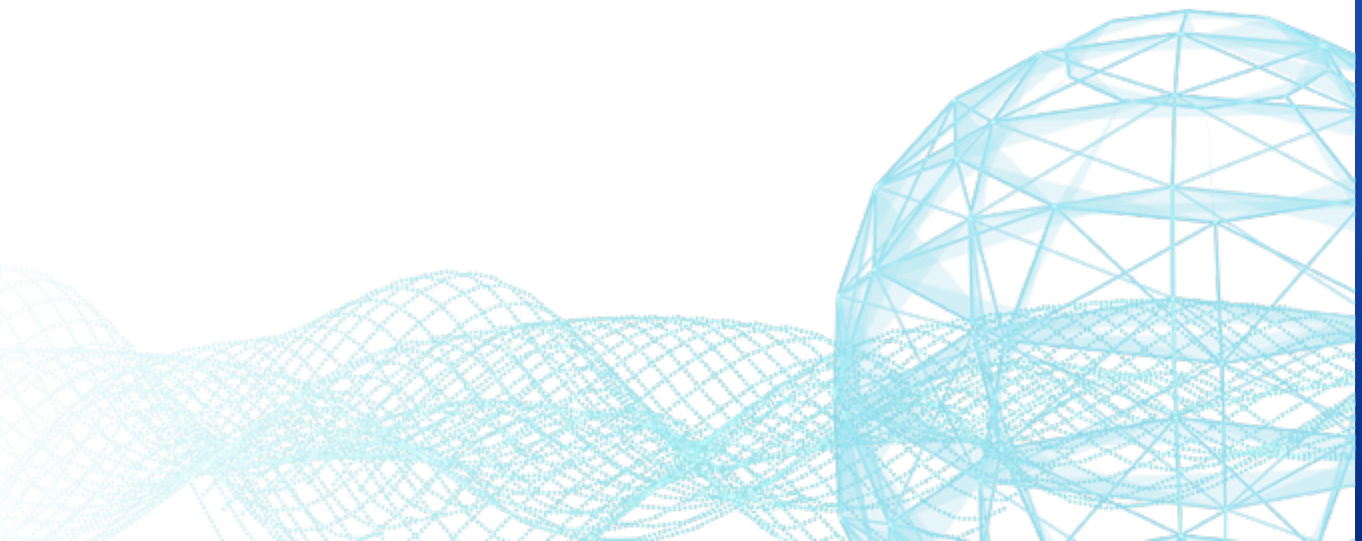
With Valtix, PayByPhone has fully automated cloud security through deployment, maintenance and policy management, orchestrated using Terraform.

For the Future: Extending Security and Prevention

Beyond their current focus and use cases, the team is actively considering opportunities to leverage additional Valtix platform capabilities that can unlock new possibilities.

Said Kevin, “Using Valtix we were able to meet our PCI DSS requirements for network segmentation, while at the same time enabling alerting, analysis, and detection of security related incidents. Having a cloud-first approach enables velocity for our security operations through Terraform and the simplicity of a SaaS model. We’re excited about the partnership and look forward to future opportunities to expand usage of Valtix platform capabilities.”

paybyphone®



VALTIX

CUSTOMER SPOTLIGHT:

PAYBYPHONE ACHIEVES SECURITY & PCI-DSS COMPLIANCE WITHIN AWS

Valtix is on a mission *to enable organizations with security at the speed of the cloud. Deployable in just 5 minutes, Valtix was built to combine robust multi-cloud security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to cloud network security called Dynamic Multi-Cloud Policy™, which links continuous visibility with advanced security controls.*

The result: *security that is more effective, adaptable to change, and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business. Valtix has been recognized as an innovator in numerous industry awards including 2021 top honors in the "Next-Gen in Cloud Security" from Cyber Defense Magazine, SINET-16 Innovator recognition, and inclusion in Gartner's Cool Vendors in Cloud Networking report.*

Get started with a free trial and a cloud visibility report at **Valtix.com**.

HQ - Santa Clara, USA
2350 Mission College Blvd #800 Santa Clara, CA 95054
650.420.6014 info@valtix.com