CASE STUDY

SILVERFORT

GLOBAL ONLINE PAYMENTS COMPANY BLUESNAP IMPLEMENTS SILVERFORT TO ENABLE MFA FOR SENSITIVE SYSTEMS

BlueSnap® As a payment processor, BlueSnap needed to comply with the Payment Card Industry Data Security Standard (PCI DSS) information security standard. PCI DSS v3.2 Req 8.3 requires firms to incorporate multi-factor authentication (MFA) for all non-console access to the cardholder data environment (CDE) for personnel with administrative access, as well as any remote network access originating from outside the entity's network. This includes both users and administrators, as well as third-party access for support or maintenance.

Complying with these requirements is a challenge for organizations, due to the difficulty of implementing MFA for various systems that are part of the CDE. With regular MFA solutions, this typically requires deployment of software agents on relevant servers, performing local configurations and segmenting the network. For some types of servers and components, implementing MFA is not possible, because deploying 3rd party software agents on them is not technically feasible or not allowed.

Silverfort provides BlueSnap with an easy-to-install, easy-to-use, centrally managed platform that delivers MFA for all user access to all sensitive systems and resources, without the need to modify those production-critical systems in any way.

QUICK FACTS

ORGANIZATION

A global payments company headquartered in the USA, with offices in United Kingdom and Israel. The company provides an All-in-One Payment Platform designed to increase sales and reduce costs for B2B and B2C businesses.

CHALLENGE

- Comply with PCI DSS requirements to enforce MFA for remote and privileged user access to the cardholder data environment
- Find an MFA solution that could support BlueSnap's VPN and VMware systems as well as various Windows and Linux servers without undue complexity and without deploying software agents
- Meet PCI DSS user access audit

SOLUTION

- Silverfort MFA was incorporated to protect non-console access to all CDE systems
- The solution was extended to secure remote VPN access of all users
- A consolidated audit trail was provided for monitoring user access to all systems and resources

RESULTS

- PCI DSS requirements for secure access and a comprehensive audit trail easily addressed
- MFA incorporated for all sensitive use cases within hours, including VPN, VMware systems and sensitive Windows and Linux servers,
- A consolidated audit trail helps track and monitor user access to all systems and resources, including granular detail and real-time risk assessment
- Visibility into shared service accounts allowed the organization to bring those accounts back into compliance with security best practices
- No changes were made to existing systems, no software agents were required

PROTECTING PRIVILEGED USERS ACCESS TO THE CDE

> *"Silverfort enabled us to address PCI DSS requirements and easily incorporate MFA to secure privileged access to systems we couldn't previously protect"*
>
> **Michael Rubenchuk,** VP of IT Operations and Infrastructure at ***BlueSnap***

To address PCI DSS requirement 8.3, BlueSnap looked into incorporating MFA for privileged users accessing the Cardholder Data Environment. These users included administrators, DevOps engineers, support personnel and BI developers, who access internal production systems. BlueSnap's production systems run on a variety of platforms including VMWare, Windows-based servers and Linux based servers. Privileged users often use non-console access, including SSH and RDP, to connect and work on those systems.

The first system to be addressed was the VMware vCenter Server. The VMware vCenter Server is the centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts and all dependent components from a single centralized location.

Since most MFA solutions do not support an integration with VMWare, BlueSnap was struggling to protect this sensitive system. However, since Silverfort's MFA solution does not require any integration or software installation, it was easily applied to secure privileged access to vCenter.

The implementation was quick and easy. A proof of concept was set up in just a couple of hours, and within a month BlueSnap extended the solution to secure privileged access in all offices across the globe.

Additional policies were quickly added to secure privileged access to other servers, including hypervisors, Window and Linux servers. Silverfort's MFA was applied on all privileged users access including non-console RDP and SSH access, ensuring all access to these systems was properly secured and PCI DSS requirements were met.

SECURING REMOTE VPN ACCESS

With the MFA system in place to secure privileged access to the CDE, BlueSnap wanted to incorporate Silverfort's MFA solution to secure remote VPN access of all employees. BlueSnap had recently replaced its VPN but the new product was not supported by the existing MFA solution. Incorporating a new MFA solution is not only expensive, but is also painful to implement, as most MFA solutions require custom integrations and configurations.

BlueSnap was looking for a cost-effective MFA solution that could support the VPN as well as its sensitive internal systems from a single platform. Silverfort's agentless technology allowed the company to incorporate MFA for secure VPN access using the same Silverfort platform that was deployed to secure privileged access to the CDE. Silverfort's unique architecture enabled holistic protection without the need to make any change to the VPN or undertake any custom integrations or additional software installations.

User enrollment to the Silverfort mobile MFA app, that receives the push notifications for required authentication, was completed within a few days, and provided a frictionless user experience.

TRACKING AND MONITORING ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

To comply with PCI DSS, BlueSnap not only required MFA, it also needed to address requirement 10 to track and monitor all access to network resources and cardholder data. Before implementing Silverfort, the company used several tools to audit user access to systems – each tool providing limited coverage and generating a standalone audit trail in its own format.

With Silverfort's Authentication Platform, BlueSnap has a consolidated audit trail for all user access across the entire organization, including on-premise and cloud systems. Since Silverfort monitors and analyzes all authentication activity, it provides unparalleled visibility into user activities across the different systems and resources in a single audit trail. This enables BlueSnap to easily track and trace back suspicious activity to a specific user.

Silverfort's unparalleled network-wide visibility is also leveraged by its Risk-Engine to analyze the user's behavior and calculate a risk score. The user's risk score combined with the organization's over-all risk level is utilized by Silverfort to apply risk-based adaptive authentication policies.

DETECTING USAGE OF SHARED ACCOUNTS

As a byproduct of this visibility, BlueSnap was able to detect the use of privileged shared accounts from various endpoints for accessing different resources. Shared accounts are considered a bad practice because they create insufficient audit trail, don't allow accountability of a specific person/system in the case of unauthorized or malicious use, and often lead to bad password management habits.

Once detected, these accounts were replaced with more suitable personal accounts.

"Other solutions were difficult to implement. Silverfort saved us a lot of resources and time by avoiding any modifications to our systems."

Michael Rubenchuk,
VP of IT Operations and Infrastructure at ***BlueSnap***

CONCLUSION

With Silverfort, BlueSnap can now comply with the PCI DSS standard by securing remote and privileged access with MFA and auditing all user access across the organization.

Silverfort's Authentication Platform enabled BlueSnap to meet PCI DSS requirements for all its systems, including systems it couldn't previously protect, without installing software agents, without complex architecture changes, and without custom and expensive integrations.

BlueSnap was able to easily extend MFA for all the organization's users and to any system or resource and gain unparalleled visibility with a consolidated audit trail.

CONTACT US

US: (+1) 646.893.7857
43 Westland Avenue, Boston, Massachusetts

Israel: (+972) 54.660.0161
30 Ha'arbaa St, Floor 26, Tel Aviv, Israel

info@silverfort.io