CASE STUDY

PCI DSS Compliance at Leading Financial Services Provider

Safeguard for Privileged Sessions

EMP
EMERGING MARKETS PAYMENTS

The Emerging Markets Payments (EMP) Group was established to deliver world-class electronic payments services to banks, retailers, governments and consumer finance institutions across the Middle East and Africa. EMP is committed to remaining at the forefront of this revolution by creating a payments platform that drives card penetration and other payment types in these emerging markets. EMP is the leading merchant acquirer, with over 14,000 merchants on its network. The company is headquartered in South Africa and has offices in Jordan, Egypt and Nigeria.

The Challenge

The Payment Card Industry Data Security Standard (PCI DSS) is mandatory for EMP. Among others, PCI DSS requires strong control over and deep visibility of third-party access. EMP also works with third-party IT vendors – among others, they operate EMP's Card Management System and provide hosting services for the Online Payment Gateway. Consequently, EMP needed to find a solution to control the remote access of these vendors. Though they had Cisco VPN in use, this solution couldn't completely fulfill this requirement: "Cisco VPN is a good and secure solution with two-factor authentication but it doesn't provide sufficient monitoring capability in respect to what the vendor is exactly doing." – adds Mr. Mohammad Ashkaibi, IT Security Engineer of EMP.

EMP specified comprehensive technical expectations against a possible solution – they required complete audit trails on vendors' working sessions and they wanted to enforce strict security measures on these connections. These security measures included:

- limiting accessible target servers,
- enforcing strong authentication,
- recording remote sessions,
- time policy-based access and
- long-term archiving of audit trails.

Learn more

- Safeguard homepage
- Request callback

"SAFEGUARD FOR PRIVILEGED SESSIONS GAVE US COMPREHENSIVE CONTROL AND MONITORING MECHANISMS, WHILE BEING COMPLETELY TRANSPARENT FOR OUR VENDORS. IN ADDITION, WE GET GREAT SUPPORT FROM ONE IDENTITY'S FRIENDLY AND HELPFUL TEAM."

– Mr. Mohammad Ashkaibi, IT Security Engineer, Emerging Markets Payments.

The Solution

EMP experts started to search for a secure remote access solution. “Actually, One Identity’s Safeguard for Privileged Sessions and SecureLink were considered, but SecureLink had high recurring costs and no support for two-factor authentication. In contrast, One Identity was the most flexible vendor to conduct a Proof of Concept with, which was an extremely important starting point to us. During the PoC, we discovered the powerful control functions of Safeguard for Privileged Sessions, while receiving solid support to configure the device. Furthermore One Identity offered the most competitive price among the suppliers.” – explains Mr. Ashkaibi.

The PoC and testing phase took two months and finally, EMP decided to purchase the Safeguard for Privileged Sessions. They purchased the virtual appliance version of Safeguard for Privileged Sessions, because the VMware-based appliance gave them greater flexibility in deployment. The implementation of the product was fast - the transition from testing to production took only 3-4 days.

Now Safeguard for Privileged Sessions is in production environment and remote administrators are transparently going through it to reach the core application servers. Safeguard for Privileged Sessions controls and monitors all SSH and Citrix ICA sessions initiated by the vendors. SSH connections are used for managing UNIX servers whilst the Citrix (XenApp) environment is used to support remote database management.

Benefits

Safeguard for Privileged Sessions provided all the required benefits for EMP. These include:

- Granular controls over remote accesses (e.g., channels)
- Secure recording of sessions
- Fast search in recorded sessions and
- Comprehensive reporting.

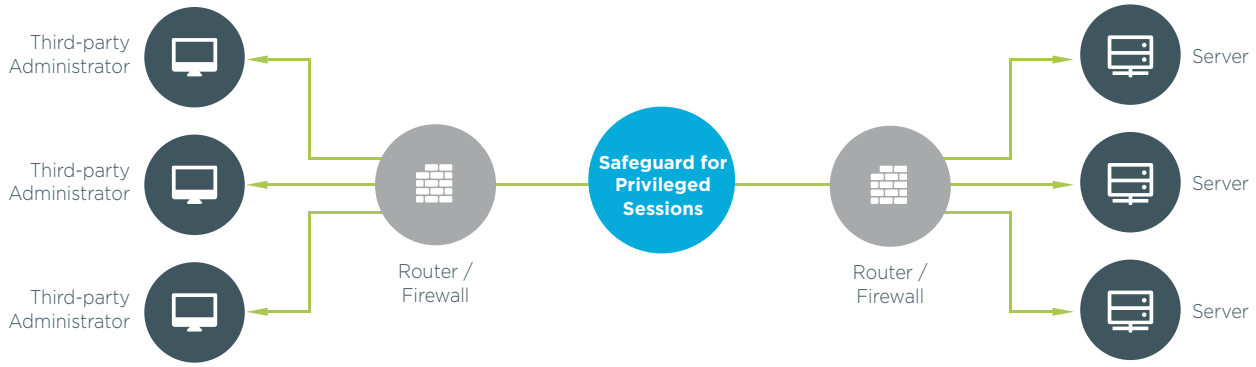
“By using One Identity Safeguard for Privileged Sessions we can better monitor our vendors’ actions, as opposed to digging into OS and application logs done previously. In addition, we have more granular control options as we can allow the required access but restrict it to a preferred level.” – concludes Mr. Ashkaibi.

Future plan

As for the future, EMP plans to utilize further Safeguard for Privileged Sessions benefits, such as:

- The ability to detect credit card content and intervene if necessary
- The flexible authentication options
- The key/certificate-based authentication for SSH sessions (two-factor authentication).

In addition, EMP intends to extend the same control and monitoring functions to sessions conducted by EMP’s internal administrators as well. The company wants to control internal access not just to core application servers but infrastructure servers as well.



Control of third-party IT vendors with Safeguard for Privileged Sessions

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com