Protecting information assets is the ultimate challenge for enterprises today. As IT operations are getting more complex, with cross-platforms, datacenters, identity and access management infrastructures and IT staffing, developing and maintaining a security compliant environment and mitigating risks is of utmost concern for IT managers.

Not only that, many companies need to meet compliance requirements of multiple regulations and standards such as PCI DSS, HIPAA, ISO 9001, ISO 27001; and industry specific requirements such as Graham-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), etc. This has further made it more challenging for enterprises to integrate all regulations into one security posture.

All major compliance standards, however, have certain basic requirements ensuring security within a system. No matter which regulation you are in the process of complying with, you need to authenticate every user with their unique identities and limit access to privileged roles for sensitive data. Even with the privileged roles, all logs are recorded and audited to ensure the safety of information during the course of an activity.

**Why you should audit privileged user activity?**

* To practice accountability required for compliance
* To record and be able to look for user activity in case of arising suspicions
* To be able to monitor in real time before a breach actually takes place
* To remind disgruntled employees that all malicious activities will be recorded
* To be able to put forth a clear record for evidence in case of disputes

**How Does it Apply to Payment Card Industry?**

Payment Card Industry Data Security Standard (PCI DSS) has laid down strict regulations and penalties for industries dealing with cardholder data. This is to make sure that service providers and merchants take the security and privacy of payment card data as their priority. PCI DSS 3.2 is going into effect from Oct 1, 2016 and consists of 12 requirements that need to be complied with by any enterprise that deals with storing, transmitting or processing cardholder data. All 12 requirements relate to PCI app security and protection of payment cards.

Privilege Service and Server Suite (Standard, Enterprise, Platinum) have been specifically mentioned in the 3.2 revision of PCI DSS, as they help organizations achieve overall PCI DSS compliance and PCI app security. They can help you with managing privileged user accounts, reduce PCI scope, manage access control, encryption when communicating between untrusted servers, etc.