Power trading exchange enables secure infrastructure for efficient trading for 6000+ participants with Sectona

Need

Industry
Electric Utility

Leveraging custom trading applications and critical network device applications are part of routine tasks for IT teams. Exposing such applications to external risk vectors can cause serious damages to the business. Conforming to the norms of access security, ensuring administrative credentials to such applications are not exposed and shared among multiple IT staff is of paramount importance. This is what led them to look for a Privileged Access Management (PAM) solution.
Identifying the gap, the team summarized three key objectives from PAM:

- Flexible framework for integrating with their in-house custom applications for securing access and monitoring user activities
- Secure vault for providing password-less access to applications and storing credentials in a central encrypted repository
- Scalable model to extending the access security and monitoring framework to a wide mix of IT assets, including networking devices

Solution

IEX found all three objectives being achieved with Sectona. Sectona's Privileged Access Management Suite provides an automated and robust solution that provides the Exchange with secure access to users across the IT infrastructure including network devices and custom applications. The solution has built-in framework that helps scale and extend the security framework to a wide variety of in-house or third-party applications on demand. With a robust built-in vault, the Exchange further safeguards critical passwords and helps minimize downtime. Furthermore, the solution provides increased visibility and governance over user activities with comprehensive logs, reports and threat intel.

Specific objectives met include:

- Password-Less access to third party applications such as Checkpoint Smart Dashboard
- Enhanced security and built-in replication with an embedded, unexposed and encrypted vault
- Framework for seamless integration with In-house custom applications for secure access and monitoring
- Comprehensive user session logs for forensics and audit

Benefit

Indian Energy Exchange has successfully achieved faster and seamless log-in flow to all and any applications including HPE 3PAR without exposing credentials. This enables users to connect with a single tap and optimize productivity that subsequently helps the team focus on maximizing technology for delivering efficient and transparent trading marketplace.

Background

IEX is India's premier power trading firm established in 2008 with its headquarters in New Delhi. IEX enables efficient price and counter-party risk management for customers from the electricity market and the open access industries. IEX has a consumer base of 3500 open access industries, 1000+ private generators and 4000 participants across utilities, which are leveraging the Exchange platform of IEX to manage their power portfolio competitively and reliably. IEX was looking for a solution which can manage its PAM Users, monitor their activities, provide seamless integration with in-house software and protect their IT assets along with networking devices.

Providing Built-In Plug-In Designer for In-House Solutions

IEX also has few in-house solutions like Checkpoint SmartDashboard console, which is a firewall console, HPE 3PAR which is a console for managing storage devices etc. These two consoles have login credentials to take access, which require monitoring. They wanted to on-board these consoles in for accessing and monitoring purpose.

To on board these consoles, IEX leveraged Sectona's plugin developer framework. Sectona Plugin Developer Kit allows users to redesign connectors on the go and without heavy professional services effort enabling them to integrate and onboard such consoles faster. This also ensured access to the consoles were being managed and monitored via PAM.

Embedded Database – Hardened and Unexposed

Few companies opt for using external database which will later be on-boarded on PAM Server. This approach comes with its own set of challenges viz.

- External database is easily accessible by any user.
- Organization needs to manage the backup and maintain HA as well.
- External database is exposed, and any DBA can make changes in the data.

To overcome these issues, Sectona PAM provided IEX with a built-in secure database wherein:

- Database vault is hardened and unexposed.
- Robust and easy to manage HA & DR. Reduced dependency on DBA.
- Automatic failover with no need for manual intervention.

Multiple Concurrent Privileged Sessions are taken at a time in IEX

IEX network faces multiple privileged sessions at a time. With the increase in number of sessions, it was becoming a huge task to monitor these privileged sessions. Regulatory bodies & compliance mandates also require these privileged account activities to be monitored.

To solve this issue of session monitoring, Sectona PAM leveraged:

- Real time monitoring and control of privileged session activity.
- Real time notification of any high-risk activity and gain instant control of any session from mobile device, PC or laptop.
- Deep granular level visibility of these sessions with video playback capabilities and log review with metadata viz. commands.
- Composite risk scoring mechanism to help with improved session review and governance