Options surety: Case study

scmagazine.com/home/security-news/in-depth/options-surety-case-study

Greg Masters

June 1, 2016

The MIAX Options Exchange needed more than a way to appease regulators, it also required security assurance. Greg Masters reports.

Show me the money! Well, for the MIAX Options Exchange, it's all done electronically and under the supervision of a management team that includes several former top executives from Nasdaq and other exchanges.

The options trading exchange was approved by the SEC on December 3, 2012 and commenced operations four days later as the 11th U.S. equity derivatives market. But as part of the approval process to open as a national securities exchange, it had to satisfy a multitude of security criteria expected by regulators. Auditing and logging were two critical requirements. It needed a way to perform full keystroke logging of any activity on its critical systems while ensuring high availability and near-zero performance impact for the hosts.

The MIAX Options Exchange now accounts for more than eight percent of the national market share, and with a major equity rights deal early in 2015 with seven major firms, including Citadel Securities and Morgan Stanley, it is predicting to triple its market share. It now lists and trades options on more than 2,300 multi-listed classes and its system throughput is in excess of 38 million quotes per second with an average latency for a single quote being 15.89 microseconds.

The MIAX executive offices, technology development center and national operations center are all located in Princeton, N.J. Additional executive offices, as well as a multipurpose training, meeting and conference center are now being developed in a state-of-the-art facility in Miami, where it intends to locate its equities sales, membership, marketing and listing operations.

OUR EXPERTS: Password trust

John Masserini, CSO, MIAX Options Exchange

Brad Hibbert, CTO, BeyondTrust

Recent growth and expansion into other business ventures mandated that it expand its privileged access management capabilities to enterprise password management, says John

Masserini, CSO at the MIAX Options Exchange. “We needed to provide regulatory assurance of total separation of the technical and operational environments. We also saw this as an opportunity to enhance the entire privileged access management process – and enable auditability for the separation of our technical and operational various environments.”

The exchange also needed true high availability across several geographic locations, with the ability to support full disaster recovery in any of its data centers, Masserini says.

There are approximately 100 people dedicated to technology services throughout MIAX. Masserini and his team evaluated all of the leading competitors in the privileged access management space and chose a subset to perform a proof-of concept (PoC) within the environment. Several selection requirements were used – including functionality, high-availability/disaster recovery approach, user interface and cost. After selecting solutions for the PoC, the MIAX team evaluated ancillary features as part of the overall value proposition and performed detailed, technical analysis while working with the various business representatives to ensure functionality throughout the enterprise and to determine which best satisfied the requirements. At the conclusion of the PoC evaluations, the team – along with the various business representatives and security management – made the final decision on selection.

The choice, says Masserini, was to deploy PowerBroker for Unix & Linux, a privileged access management solution from BeyondTrust. “PowerBroker for Unix & Linux enables us to delegate Unix and Linux privileges and authorization without disclosing passwords for root or other accounts,” Masserini says. The solution also records all privileged sessions for audits, including keystroke information. “As a result, we’re able capture all admin activity, while gaining full forensic auditability across our critical IT infrastructure.”

The password is…

But, MIAX also had concerns about proxy-type solutions being able to keep up with the key capture requirements of its operational environment. It required a solution that could integrate with previously installed SSH applications on the local desktops. Additionally, the solution had to be a self-contained, hardened deployment – which precluded solutions that required use of the corporate SQL database. Finally, integration with the existing PowerBroker for Unix & Linux deployment was a key differentiator as was compatibility with its existing SEIM infrastructure.

After a series of PoC evaluations, Masserini’s team selected PowerBroker Password Safe, also from BeyondTrust. “With Password Safe, we provide a single login to the user and allow them to pick and choose which environment to access – and with which account.”

Deployed as a hardened physical or virtual appliance, or as software, and featuring broad support of operating systems, databases, cloud and on-prem applications, devices and directories, PowerBroker Password Safe discovers and profiles all known and unknown assets, shared accounts, user accounts, application accounts and service accounts, says Brad Hibbert, chief technology officer at BeyondTrust.

“Quickly identifying assets with common traits and automatically placing them under Password Safe management via Smart Rules reduces the number of attack surfaces,” he explains. “Password Safe ensures all passwords are randomized and rotated on a scheduled basis or upon check-in to reduce the risk of passwords leaving the organization.”

Once credentialed access has been granted, Password Safe records privileged sessions in real time via a proxy session monitoring service for SSH, RDP or Windows Applications (RemoteApp) without revealing the password – and without the need for Java, Hibbert says. “Live session management enables true dual control, allowing administrators time to investigate suspicious behavior without killing an application – or user productivity.”

Offering DVR-style playback, Password Safe provides detailed auditing of shared account access, helping to meet password protection and audit regulations for compliance mandates listed in *The Sarbanes-Oxley Act* (*SOX*), *The Health Insurance Portability and Accountability Act* (*HIPAA*), *The Gramm-Leach-Bliley Act* (*GLBA*), the PCI Data Security Standard (DSS), the Federal Desktop Core Configuration (FDCC), *The Federal Information Security Management Act* (*FISMA*) and others, he adds.

Deployment

Getting the solution operational at MIAX wasn’t as simple as flipping a switch, but with on-site assistance, the deployment went as scheduled. “Given the complexity of any environment in our business, few deployments go smoothly.” says Masserini. The onsite deployment team met with the PoC team to understand what was tested and how the entire PoC progressed, he explains. Once onsite, they were able to stand up the entire environment, including the high-availability aspect of the deployment. “Between the onsite team and the BeyondTrust support team, we resolved minor challenges and rolled out a fully functionally solution within the expected deployment time,” Masserini says.

Prior to Password Safe, the operations team would open eight to 10 SSH sessions each morning to start up and monitor the production environment, says Masserini. Each session required a one-time password resulting in wasted time and other inefficiencies. “With Password Safe, users are able to strongly authenticate a single time and have SSH sessions opened for them with one click,” he says.

Incident investigations required significant effort prior to Password Safe, requiring Masserini's security team to review logs, find the correct recorded session, and then replay that session to see if it was tied to the incident. With Password Safe, he says, the team leverages Google-like search capabilities to pinpoint suspect users and commands, replaying the sessions right from the GUI. "This is seamlessly integrated with our existing PowerBroker for Unix and Linux deployment, and it provides full visibility across all actions in all environments."

As a National Securities Exchange, MIAX has a number of regulatory compliance issues it must address on a continual basis. "Password Safe allows us to not only satisfy these requirements, but also do so in with minimal imposition to our end-users," says Masserini (*left*). "It also provides a far easier method of providing the annual user certification attestation, which ensures all users are reviewed annually for access rights."

PowerBroker Password Safe is deployed enterprise-wide, providing secure access control for every privileged user in the organization, says Masserini.

PowerBroker Password Safe features two major releases per year, two minor releases per year, and continually updates capabilities through auto-update, says Hibbert.

"Our customers are looking for strong innovative partners to reduce their internal security risks. BeyondTrust has 7 awarded and 10 pending patents spanning privilege management and advanced threat analytics," he adds." There is significant value for organizations in using a platform for privileged access management beyond the obvious benefits of lowered cost of ownership and fewer interfaces to manage. In this particular use case, integration between the products in the platform – PowerBroker Password Safe and PowerBroker for Unix & Linux – provide multi-layered security by controlling what privileged users can do with the access they've been granted."

As the MIAX business grows, Password Safe will act as an intermediary, managing privileged access across various exchange environments, adds Masserini . This foundation will provide an auditable method to prove the separation of environments, as well as the ability to log and monitor every action across all environments.

"The threats we face are, in many ways, different every day," says Masserini. "We are constantly dealing with the rapidly changing world of malware infiltration no differently than anyone else, whether it's web-based malicious ads or the spam that gets through the

majority of filters. The recent 'glibc' or 'vendor backdoor' issues just highlight the interdependency of the entire supply chain, which once again, brings focus back on user behavior, credential management and access rights.

An unexpected side benefit of Password Safe was the ability to leverage BeyondTrust's BeyondInsight platform for enhanced threat analytics and risk reporting, Masserini says. "MIAX was able to integrate BeyondInsight with feeds from various, complementary tools already in use. This provided not only a self-service reporting tool, but also a critical risk dashboard that delivered insight into the overall risk posture of the enterprise."

[sidebar]

CAPABILITIES: Differentiators

When asked what differentiates the BeyondTrust solution from competitors, Brad Hibbert, chief technology officer at BeyondTrust, offers the following reasons:

Session monitoring and management is fully integrated with password management at no extra charge, enables true dual control and doesn't require Java. Many competitors offer two separate tools for password management and session management. Not having them fully integrated causes unneeded complexity for admins and cost for the business. As well, most password and session management tools on the market offer only a binary choice – maintain a session or kill it – so sometimes perfectly good sessions are killed, ruining productivity. Password Safe enables true dual control helping teams lock, terminate or cancel a session. This balances risk-reduction with productivity.

Comprehensive discovery minimizes gaps in coverage and ensures that no accounts or assets are missed. Password Safe leverages a scanning engine built for detecting vulnerabilities, so you can scan, identify and profile all users and services, automatically onboard systems and accounts under management. This capability is all about reducing attack surfaces by closing gaps.

Application password management is included in Password Safe at no extra charge. In many cases, IT teams have to go into every application, server, and database and manually rotate application passwords. With Password Safe, those IT teams control scripts, files, code and embedded keys by eliminating hard-coded or embedded application credentials automatically. This reduces risks by closing gaps. Many other providers offer this capability separately – or not at all.

Threat analytics and vulnerability intelligence provide a risk score for privileged accounts and users. Having our own natively-built vulnerability management solution fully integrated into the password and session management solution (and importing vulnerability feeds from

competitive scanners and other sources) provides behavioral analytics and correlates privileged activity with vulnerability information. This capability is all about reducing risk by providing intelligence to help make better privilege decisions.

BeyondTrust offers all of the capability noted above in the same solution at the same price, and doesn't charge extra for additional modules, Hibbert says. "That's a lot of additional value in one price point, on one platform."

From the June 01, 2016 Issue of SC Media