EventTracker
Actionable Security Intelligence

Meeting PCI-DSS Compliance at Autoscribe

Introduction

Autoscribe's rich history of innovation in the electronic payment processing business dates back to 1992, with the release of their first desktop software application. Over the years they have expanded their platform to include a variety of payment collection methods, verification systems, and settlement services to support the cash management process. Today, Autoscribe has over 800 clients processing payments through their systems. Autoscribe is a member of NACHA's Electronic Check Council (ECC) and works closely with ECC and other industry leaders to deliver products that exceed government security and compliance requirements.

Business Drivers

- Enable compliance with PCI-DSS
- Protect information systems from internal, external and emerging attacks.

Business Requirements

Processing over $4 billion in credit card transactions annually for over 800 clients, ensuring the security of cardholder data is fundamental for Autoscribe and compliance with the Payment Card Industry (PCI) Data Security Standard essential. Donald J. Patti, VP of Technology and Product Development faced two challenges:

- Compliance with the complex and numerous requirements of the PCI standard that govern the safeguard of consumer credit card information throughout the information lifecycle.
- The need to protect information systems from security breaches. These could be internal (employees with malicious intent), external (hackers) or emerging (Zero-day).

After deciding on Security Information and Event Management (SIEM) to extend Autoscribe's security and PCI compliance objectives, Patti conducted a requirements analysis and came up with the following criteria that the selected SIEM solution needed to meet:

- Real-time correlation and alerting
- Ease of configuration and use
- Preconfigured reports mapped to PCI requirements

After evaluating several options, Patti and his team decided that EventTracker was not only optimal in meeting their requirements but offered an additional benefit in the form of an integrated change management module. "Selecting EventTracker was an obvious choice. It came with a number of pre-built reports specifically mapped to PCI requirements and as an added bonus, provided us with both Event Management and Change Management capabilities. This allowed us to not only comply with section 10, which describes log data monitoring and reporting requirements, but also section 11, which details requirements relating to monitoring changes on critical systems," says Patti.

Complying with PCI-DSS

EventTracker helps Patti meet the following requirements of the PCI standard:

- Section 10: Track and monitor access to network resources and cardholder data.
- Section 11.5: Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

In addition, EventTracker has a widespread applicability to monitor compliance with other areas of the standard as well, such as Section 12 that calls for maintaining and documenting a policy that addresses information security. With EventTracker, Patti and his team can now link all access to system components containing critical data to individual users and get alerted in real-time to unauthorized access and/or modifications.

> *The alerts are particularly helpful in ensuring that we are constantly in compliance with PCI requirements" says Patti. "Plus, we regularly use the scheduled and ad-hoc reporting to demonstrate adherence.*

Another advantage is the automatic back-up of logs to a central warehouse. This is secured with a MD-5 checksum to prevent tampering and ensure that audit trails are always secure. EventTracker is the only SIEM solution that comes integrated with a change management module, which provides configurable change monitoring capability for Windows files, dlls, executables and registry entries. This is specifically helpful with section 11.5.

"None of the other solutions that we evaluated were able to provide us with such a broad coverage of PCI requirements" adds Patti. Defense in-depth like most mid-size companies, Autoscribe does not have the luxury of a dedicated security operations center. With EventTracker's real-time log monitoring, correlation and analysis, however, Patti has 100% security visibility across his entire

EventTracker
Actionable Security Intelligence

information architecture without having to hire expensive security experts or build a large team to track threats.

"Although our primary objective for choosing EventTracker was to help us with PCI, we quickly realized that we could leverage the solution to continuously manage risk" says Patti. He now uses EventTracker to help protect Autoscribe's IT assets from a variety of attacks including:

- The readily identifiable attacks – For example, 100 login failures in a short time from a single IP address
- The known but not easily recognized threats – For example, a legitimate administrator activity but at odd hours
- Emerging attack vectors – These include inside attempts at data theft and zero-day attacks (Nugache, Storm) that are so new that threat profiles have not been created.

EventTracker offers a blend of white-list and traditional approaches for defense in depth, necessary for emerging attack vectors. With its change management module, it can quickly detect attacks that breach traditional defenses and manifest themselves as subtle configuration changes.

Bottom-line

EventTracker provides Autoscribe with real-time event log monitoring, correlation and alerting; canned and customizable reports; secure audit trails and built-in compliance workflows – all these capabilities along with an integrated change management module help the company address a large number of PCI requirements and implement a defense-in-depth security program.