February 2, 2009

Case Study: Reliant Security Innovates With Open Source Software

by Jeffrey S. Hammond
with John R. Rymer and Justinas Sileikis

EXECUTIVE SUMMARY

Retailers that want to accept credit cards need to demonstrate that their systems are Payment-Card-Industry- (PCI-) compliant. The problem is that implementing PCI compliance can be expensive, and retailers really don't get much additional revenue from their PCI investments. Reliant Security offers a PCI compliance solution that makes substantial use of open source software (OSS) to help drive out cost while raising flexibility. Reliant Security's managing partners made sure that they developed a concise, developer-friendly OSS policy that focused on cost avoidance. They also worked with external legal counsel to make sure that their commercial licenses, software acquisition policies, and ALM processes allowed them to exploit OSS components while fulfilling licensing obligations and providing full transparency to customers. As a result, Reliant Security has helped customers achieve PCI compliance with substantial cost savings. Although Reliant Security is an independent software vendor (ISV), its tactics for avoiding software capital expenses are equally appropriate for IT shops with systems made up of large numbers of geographically distributed system nodes.

SITUATION: RETAIL CHAINS NEED SECURE SYSTEMS THAT DON'T BUST THEIR BUDGETS

How many times per week do you use your credit or debit card at a local store? Do you think twice about the in-store security that prevents hackers from taking your card data and assuming your financial identity? Brick-and-mortar stores think about this scenario a lot, because they need to demonstrate Payment Card Industry Data Security Standard (PCI DSS) compliance as a requirement for accepting credit card transactions.[1] About 65% of global enterprises are still working on their PCI compliance initiatives, and implementing them can be expensive, with some companies spending up to 10% of their IT budgets on compliance remediation.[2] The combined hardware and software costs of achieving PCI compliance can severely tax the IT budgets of retailers with hundreds of in-store networks to secure.[3]

Reliant Security provides data security products and services that assist retailers in meeting PCI compliance requirements. Reliant Security decided to make open source software a key part of its solution because every dollar that it can wring out of an in-store PCI-compliant deployment is one more dollar that its customers can allocate to other areas they need to fund to survive in a recessionary economy. Reliant Security also takes on the role of a prime contractor by evaluating multiple OSS and commercial components and integrating the results. While there's nothing stopping its clients from taking that exact same approach, Reliant Security's hard won experience with OSS and subsequent development of best adoption practices allow it to offer its clients a packaged solution that mitigates the risk of working in an unfamiliar, highly customized OSS environment.

BEST PRACTICE: RELIANT SECURITY SET A CLEAR POLICY FOR OSS USAGE

When Reliant Software developed its Managed PCI System (MPS) for Merchant Environments, it focused on cutting costs, as most retailers simply can't justify the high costs associated with commercial PCI solutions. If retail businesses do not comply with PCI data security standards, the participating credit card providers can subject those businesses to significant fines; however, retailers really don't get much additional revenue from their PCI investments. As a result, Reliant Security adopted OSS software within its solution to keep costs low. Reliant security:

- **Clearly defined cost avoidance as a major goal guiding OSS adoption.** Enhanced security is an unavoidable cost of doing business for retailers, but the lower the cost of a PCI solution, the better its chance to win requests for proposal (RFPs) from cost-conscious retailers. When Reliant Security Managing Partners Richard Newman and Mark Weiner compared the cost of ownership of a PCI solution using OSS with the cost of a PCI solution using commercial software alternatives, the OSS solution won because it does not require license and support fees. The result is the Reliant Security MPS, which packages commodity hardware and OSS components including FTimes, Nessus, OpenVPN, OpenSolaris, Snort, and syslog-ng into a low-cost virtual appliance (see Figure 1).[4] Retail customers drop an MPS into each brick-and-mortar store, where it performs core network, firewall, and security-monitoring functions.

- **Drew up a comprehensive license acknowledging GPL usage.** Once Reliant Security decided to use OSS components covered by the GNU Public License, the managing partners knew that they would need to make sure that the company proceeded within both the spirit and letter of the law. To ensure compliance with the viral provisions of the GPL, the company worked with an independent lawyer with software IP experience to draft a commercial license that acknowledges the portions of its solutions that rely on OSS and that creates a clear understanding with its customers that the package solution they are acquiring contains open source. Furthermore, the license also gives customers the right to download and modify that source themselves should they choose to do so. Reliant Security also includes the source files for the OSS components that it uses as part of its installation media and provides links to the original source locations.

- **Uses a concise OSS policy document to keep developers on track.** Reliant Security keeps its developers on track with a 15-page policy document that it updates regularly. The policy lays out how developers should account for open source provenance as well as how they can make sure that they have adequately updated the license declarations for any code that they write that is dependent on an OSS component.

Figure 1 Open Source Software Components That Reliant Security Uses

OSS component	What it's used for
OpenSolaris	Base operating system used in MPS appliance
Open VPN	Secures communication traffic for different user communities/zones over the underlying network
FTimes	System baselining and evidence collection tool for intrusion detection and forensic analysis
syslog-ng	Reliably transfers log messages using TCP; provides content filtering and message reformatting
Nessus (v 2.2.11)	Scans network and identifies potential vulnerabilities
Snort	Provides network intrusion detection and prevention
Puppet	Manages and configures geographically dispersed nodes at individual stores
StrongKey	Manages the generation, escrow, recovery, and issuance of symmetric encryption keys
MySQL	Stores persistent data for central portal and administration console
Spring	Used as the base framework for component integration and custom development

48204 Source: Forrester Research, Inc.

BEST PRACTICE: RELIANT SECURITY TUNED ITS ACQUISITION PROCESSES FOR FLEXIBILITY

While Reliant Security uses significant amounts of OSS to keep licensing costs low, it also focuses on flexibility as a key component of its overall solution. While some components of a PCI solution are straightforward to set up and configure, others require significant customization. A common example is integration of the PCI solution into sales process and network access policies, which vary widely from retailer to retailer. The need to provide both low cost and flexibility has pushed Reliant Security to focus its software acquisition processes on:

- **An evaluation process that puts OSS options first but also includes commercial alternatives.** The per-unit cost advantages for in-store components make it desirable to use OSS wherever possible, but other solution attributes such as overall total costs, integration capabilities, and component performance are also prime considerations. Developers evaluate commercial components and build-from-scratch options in parallel with OSS components, basing their assessments on how well each option will fulfill customer requirements. Mr. Newman sums it up nicely: "We download whatever we can, buy what we have to, and build where we must." In practice, this acquisition flexibility results in a mix of OSS, packaged, and custom code. Examples of Reliant Security's buy-versus-download decisions include the use of Atlassian JIRA for change management and Splunk for searching log files generated by other system components.

- **Rapid replacement of software components as customer needs and component costs evolve.** Reliant Security compliments its best-of-breed integration approach that prioritizes open source with an architectural design that allows developers to quickly replace components in the MPS software stack. For example, when developers found that using OpenBSD as the operating

system didn't adequately support some customers' security requirements, they replaced it with OpenSolaris and implemented a virtualized environment in which each network zone has its own IP stack and network resources. In another situation, a customer already had a commercial alternative in place but still needed a more cost-effective log capture capability. Reliant Security's modular architectural strategy also insures against lock-in from commercial products: If a particular commercial component were to increase its per-processor cost, developers would work to replace it from a list of previously identified alternatives.

- **Prioritization of specific performance "ilities."** When evaluating their options, Reliant Security's developers prioritize a component's security, extensibility, and quality characteristics above other "ilities" such as accessibility, simplicity, usability, and manageability. In practice, this means that documentation and features such as automated setup and configuration utilities take a back seat to other considerations such as the number of open defects a component has and how quickly community developers are fixing them. One reason that this tradeoff is practical is because Reliant Security employs experienced developers used to using alternative sources such as community forums or third-party books that replace technical reference manuals.

BEST PRACTICE: RELIANT SECURITY ADJUSTED ITS DEVELOPMENT PROCESSES

Reliant Security uses Agile development practices to minimize delivery times and maximize customer responsiveness. That said, the company found that it did need to make a few minor process adjustments to application life-cycle management processes to ensure the proper documentation of developers' use of OSS components. These process tweaks are:

- **Developers must capture OSS dependencies in their design documents.** Reliant Security developers use design documents that require them to identify their software's OSS dependencies. The company uses the resulting documentation to demonstrate compliance with licenses such as the GPL and provides this information to customers in the interest of full transparency.

- **Developers must check OSS components to ensure provenance.** As part of Reliant Security's OSS dependency declaration process, developers must identify the origin of downloaded code. Wherever possible, developers use standardized repository locations such as SourceForge to assure the integrity of the source code they are using. Checksums verify either that no one has modified files during the development process or that source that is packaged into the product does not differ from known good versions of OSS components.

Next Steps: Reliant Security Plans For Greater Coordination And Richer Features

Reliant Security plans to use more open source wherever practical to support more features in its solution. Its next steps include:

- **Centralizing OSS component information in a trusted repository.** Reliant Security provides full disclosure of the OSS components that its developers use in its software and points clients to project locations, but today clients must verify and download source code if they want to modify the out-of-the-box solution. Reliant Security is working to create a single source repository of all the software that is in active use. Once development is complete, customers will have a single, validated location from which they can download the exact versions and configurations of any OSS component source they wish to modify or review.

- **Improving remote management with emerging OSS components.** As potentially hundreds of remote appliances are geographically distributed in stores, on-site administration really isn't a cost-effective solution for retailers. Providing effective remote configuration management with an OSS configuration management tool such as Puppet allows Reliant Security's clients to avoid the cost of an expensive commercial configuration management tool while still securely managing their in-store networks.[5] Reliant Security has successfully deployed an initial version of Puppet-based administration into production environments for two customers and is now in the process of rolling it out to other clients.

BEST PRACTICE RESULTS: RELIANT SECURITY'S CLIENTS ACHIEVE PCI COMPLIANCE

The bottom line for Reliant Security's customers is that they need a repeatable implementation of a secured in-store network that can successfully pass a compliance audit. At this point, multiple customers have done exactly that, demonstrating successful PCI compliance in the process. And the icing on the cake is that achieving compliance has come at substantial cost savings. In one case, a customer saved over $1 million in deployment costs across 700 retail installations compared with the cost of deploying alternative solutions based on commercial technologies — a net project cost reduction of over 50%.

Lastly, the benefits of Reliant Security adopting open source don't just accrue to its customers. Even though the retail sector is challenged by the recession, Reliant Security is entering 2009 with a healthy backlog of implementation projects and is attracting attention from larger retailers that prior to the recession would have purchased more-expensive solutions from larger commercial ISVs without much concern over the added cost.

RECOMMENDATIONS

HOW TO APPLY RELIANT SECURITY'S BEST PRACTICES IN OSS ADOPTION

Reliant Security proves that even small companies can benefit from adoption of open source software, especially in situations where a company must pass the costs of its development efforts along to clients. To apply the lessons learned from Reliant Security's successful use of OSS, organizations should:

- **Start by looking at system components that aren't industry-specific.** Repeated OSS assessments have led Reliant Security's application development professionals to conclude that the more "horizontal" an architectural component is, the greater the likelihood that multiple OSS options for that component exist that might very well meet an organization's needs. Since security components have wide horizontal appeal, they've found many options to choose from. Start your own adoption efforts by separating industry-neutral architecture layers from industry-specific ones, and concentrate early efforts on the industry-neutral ones.
- **Identify spots where changing the total cost of ownership (TCO) profile pays big benefits.** Reliant Security's model works because the TCO of a PCI solution is highly sensitive to the unit costs of the hardware and software that retailers deploy to each brick-and-mortar store. By lowering the capital expense of each per-unit deployment, Reliant Security frees up substantial capital that can be deployed to operational expenses — for example, hiring more-experienced developers or administrators to customize the solution and further integrate it into retailers' other systems. Start your own OSS adoption plans by looking for situations where trading off capital expenses for operational expenses would return similar results.

ENDNOTES

[1] Forrester published a report detailing the demands of PCI compliance. See the September 11, 2008, "Confessions Of A QSA: The Inside Story Of PCI Compliance" report.

[2] Forrester published a report listing the top 10 things companies should know when working toward compliance. See the March 23, 2007, "The Top 10 Things You Should Know About PCI Compliance" report.

[3] Almost any store you shop in has an in-store network connecting point-of-sale terminals and in-store servers. Some stores may even provide customer-accessible hotspots as customer convenience features.

[4] As an example of costs differential, one client recently implemented Reliant Security's logging functionality, based on syslog-ng, for a total implementation cost that was under $50,000. This compares favorably with other commercial security log capture solutions from companies such as ArcSight, Cisco Systems, and LogLogic, where enterprise solutions start at an entry price of $60,000 and quickly grow into the $500,000+ range.

[5] For more information about Puppet, see "What Is Puppet?" (http://reductivelabs.com/trac/puppet/).