



Payment Card Industry (PCI)

Compliance with Sawmill

An Executive White Paper

September 2007



Regularly Monitor and Test Your Secure Networks

Whether you're a merchant or in the banking industry, credit card and identity theft are continuing to increase. You must protect your consumer data and as part of an internal solution, Sawmill can play a major role.

Since 2005, all merchants that store, process, or transmit credit card data are required to abide by the Payment Card Industry (PCI) Standard. All forms of payment, paper or electronic are covered by this compliance. The PCI standard is endorsed by all credit card brands, including Visa, MasterCard, American Express, Discover Card and JBC.

The risk of non-compliance can be a loss of your reputation, large fines and increased fees from credit card programs.

The benefits of compliance for the consumer are many, including limited risk, more confidence in the industry and identify theft prevention. For you, as the merchant or Payment Service Provider (PSP), you keep your competitive edge, gain trust from consumers, your data is safeguarded and your reputation is protected.

How Can Sawmill Play a Role in Compliance?

Sawmill will monitor all incoming and outgoing traffic to your network, 24/7, which is section 10 of the PCI DSS compliance list. At any time you can run a report and get the precise information about who is accessing your data. You can also schedule Sawmill to run a new report at any time of day, to check for any vulnerability. Any unauthorized access to your network will be reported. You can configure Sawmill to alert you when an exceptional event occurs, as determined by the highly configurable rules that you define. You define your own alert rules, but once this is done, Sawmill will be the watchdog.

With Sawmill's robust reporting tools, you can create an internal audit whenever it's needed. Before you reach a compliance deadline, you can run Sawmill and verify that you are meeting all of the compliance requirements.

What if Security is Breached?

The PCI Council makes it very clear that once your data is compromised, you must notify them and stop your customers' data from being exposed. Sawmill can help you with this breach as well. Once you have run your internal review and ascertained that you have a breach, you can block any outsiders from accessing your data. You can block access by any visitor, via their IP address. You can also set up passwords and reports, to allow only need-to-know employees, access to secure data.

Cost Effectiveness

With Sawmill, you can install it on your existing hardware and monitor your current network. You can run reports immediately for your onsite assessment of compliance. We offer standard support and also premium support. Our premium support engineers can help you refine your reports and optimize Sawmill's performance, so that you can keep ahead of any security problems. Before you pay for a costly security solution or audit, you will want to see for yourself how your data is being accessed.

Sawmill combines the internal controls and reporting that you need to help keep your customer's data protected. In order to keep your customer's trust, you can use Sawmill as part of your internal infrastructure to keep compliant on a day-to-day basis.