PROFICIO

SURVEY ON PCI DSS 3.0 READINESS

Introduction

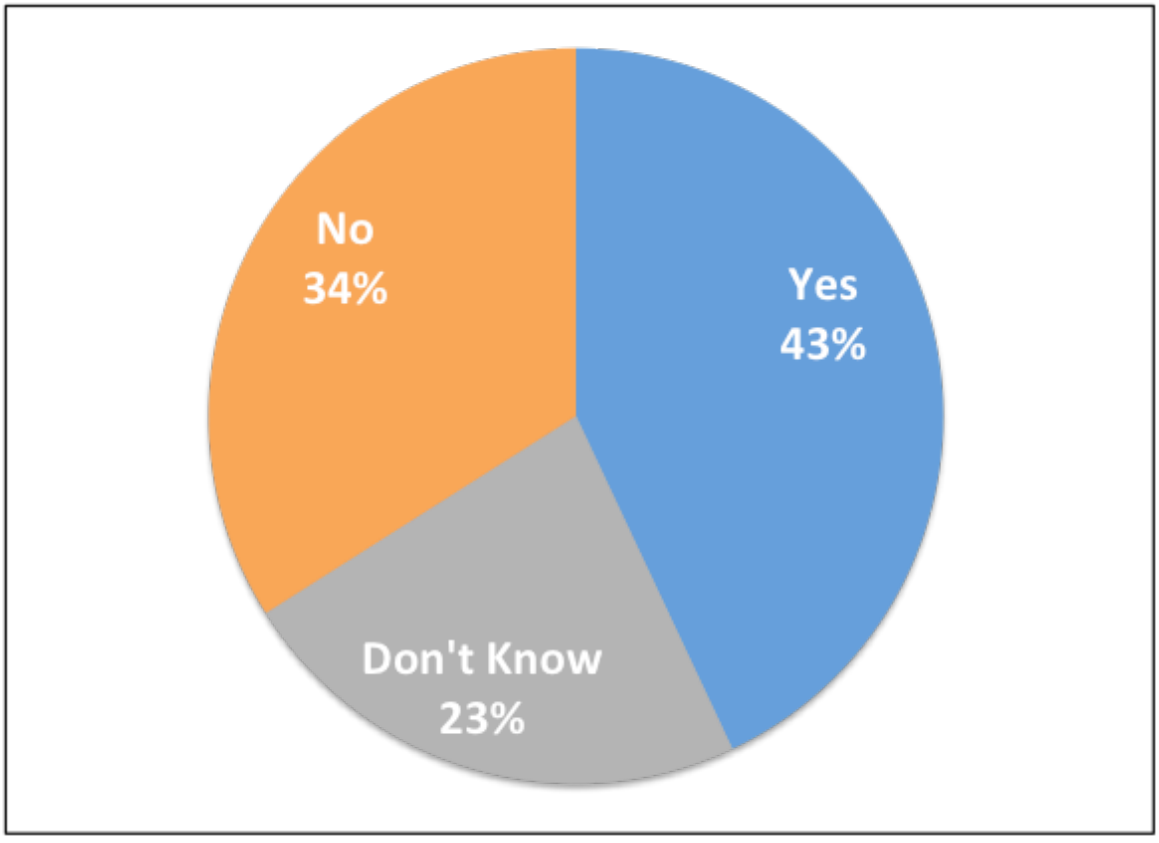
PCI DSS 3.0 was announced in November 2013 and went into effect on January 1, 2014. PCI DSS 2.0 compliant merchants have until January 1, 2015 to transition to the new standard. Certain requirements are treated as best practices and must be met by June 30, 2015.

The purpose of this survey was to take a snapshot of enterprises at the end of 2014 to assess the progress in meeting PCI 3.0 requirements and identify the challenges associated with this transition.

The following is a summary of the responses from 129 security and compliance professionals from retail, financial services, healthcare, education, government, and other sectors.

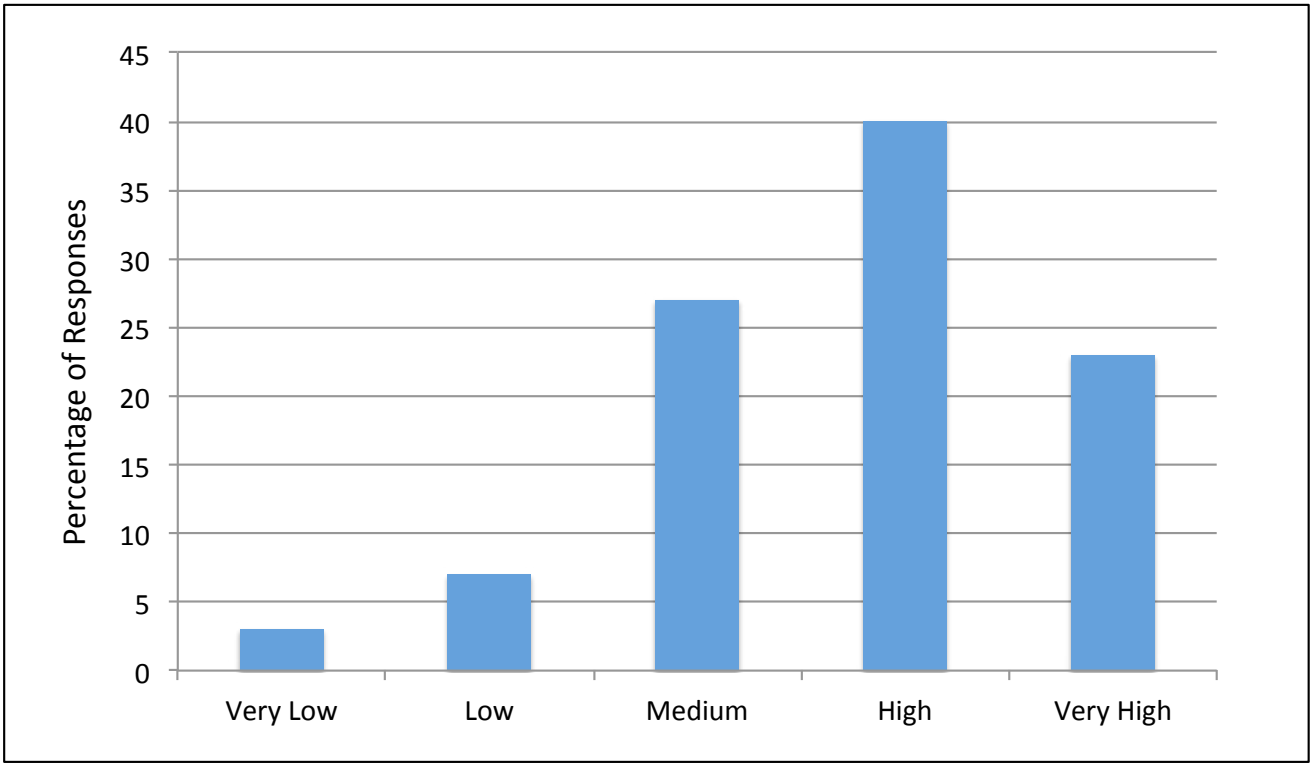
Response Summary

1. Do you meet PCI 3.0 requirements today?

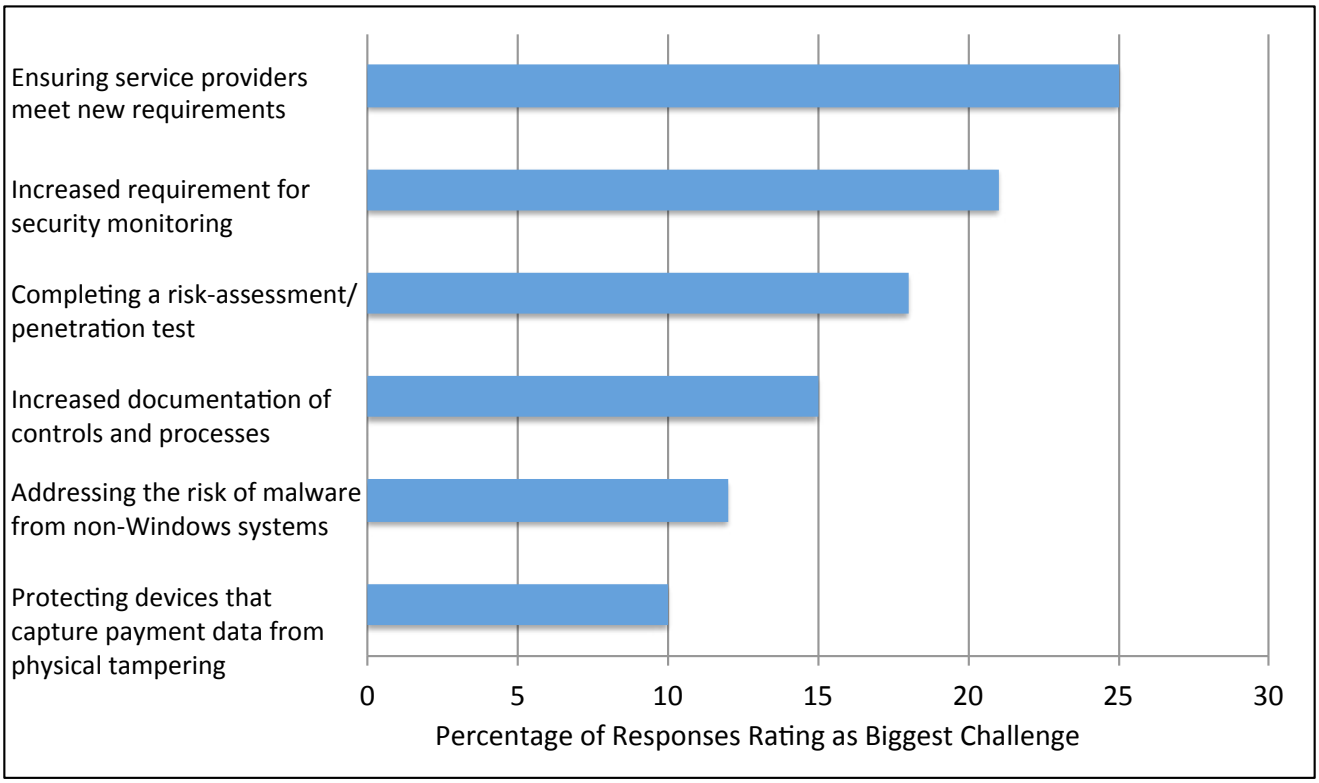


Overall, less than half of the respondents indicated they meet PCI 3.0 requirements at the time of the survey (December, 2014). However, more than 60% of respondents from the retail and financial services industries indicated they are currently in compliance – higher than other industries and reflecting the importance of credit card data to their operations.

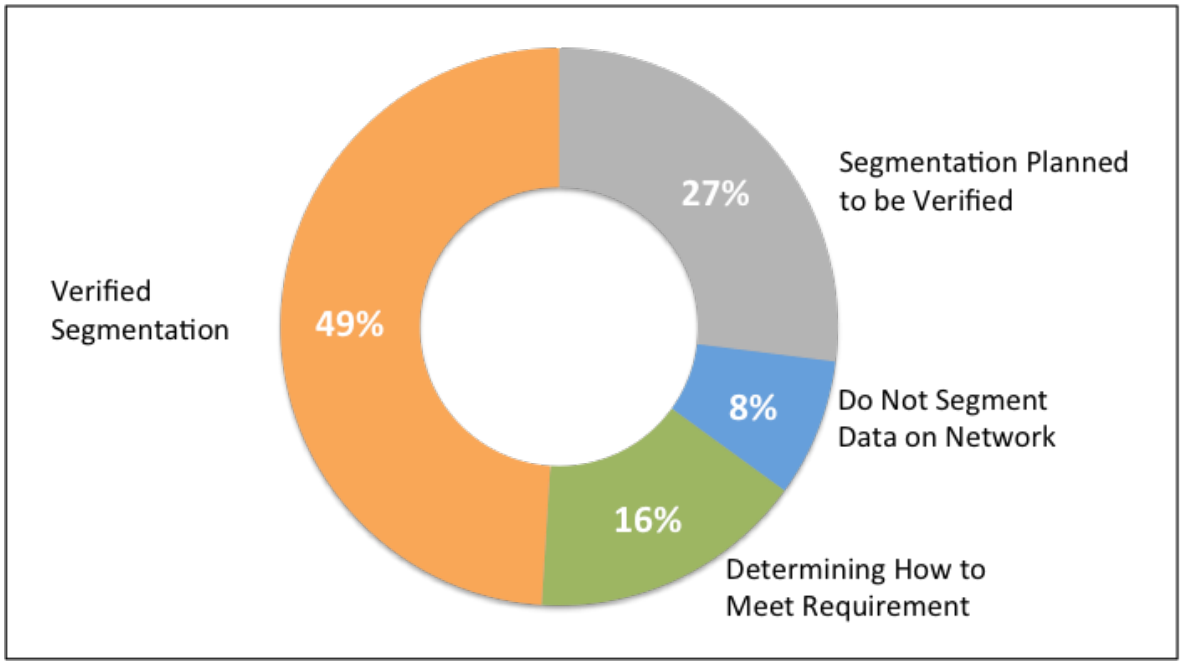
2. How confident are you that you will be in full compliance with PCI 3.0 by June 30, 2015?



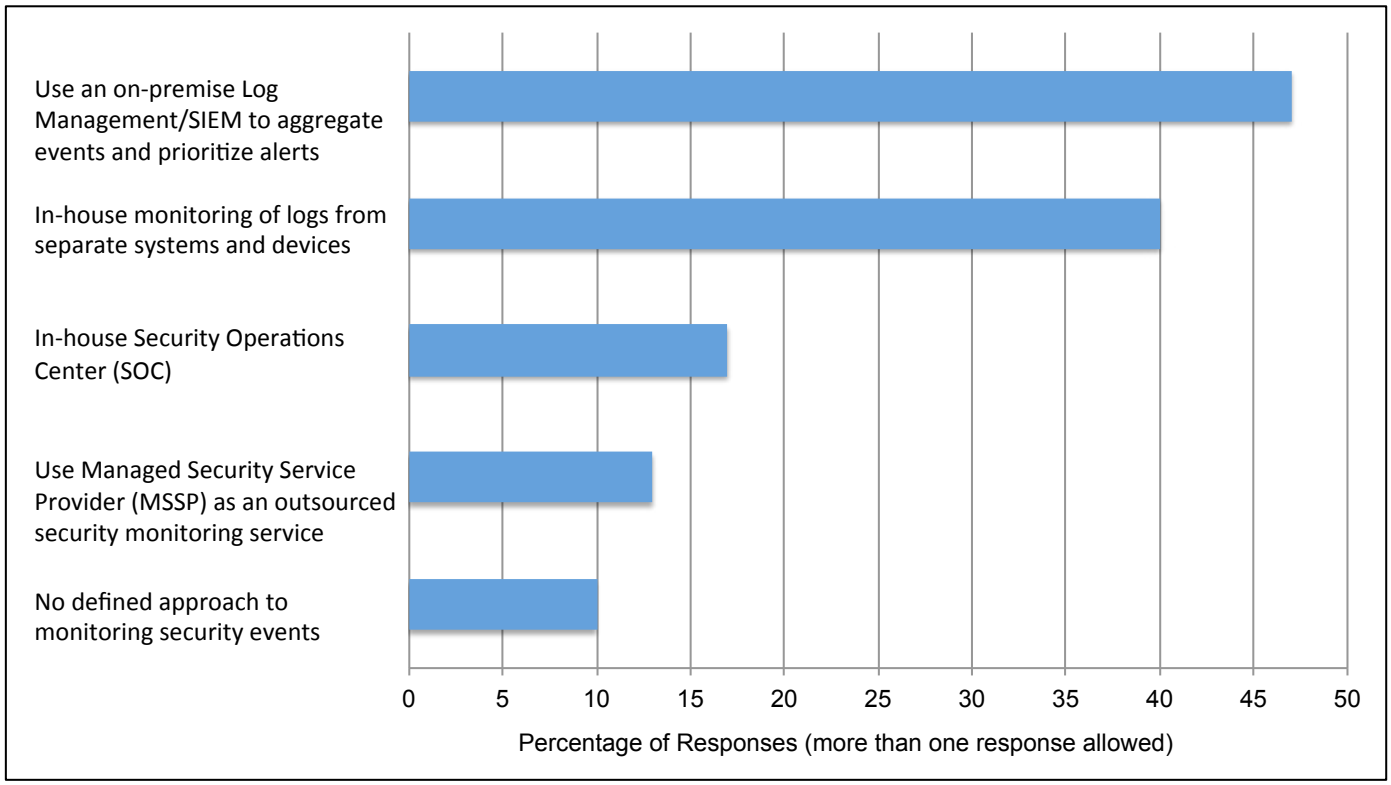
3. What are the biggest challenges for your organization to achieve PCI 3.0 compliance?



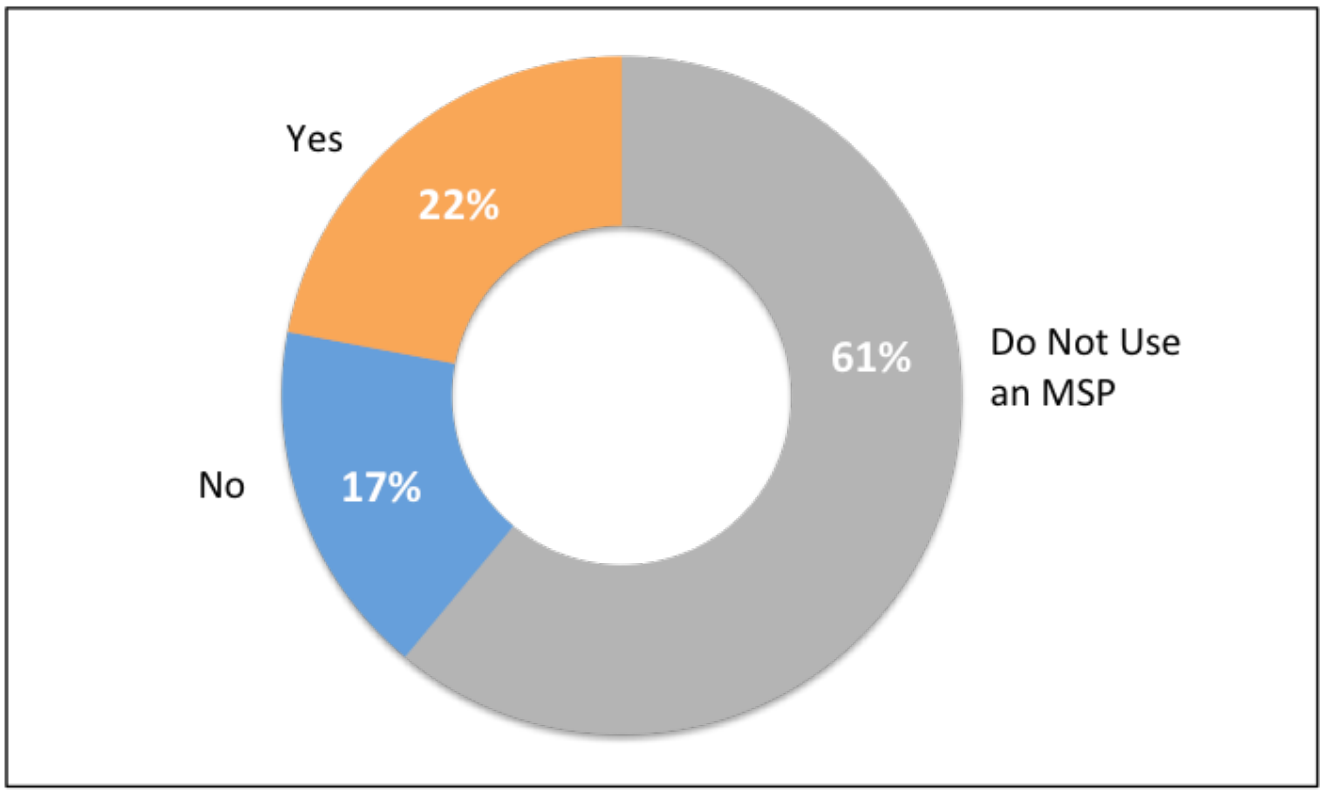
4. If segmentation is used to isolate the Cardholder Data Environment (CDE) from other networks, PCI 3.0 requires you to perform penetration tests to verify the segmentation methods used are operational and effective. Which of the following best describes your progress in meeting this requirement?



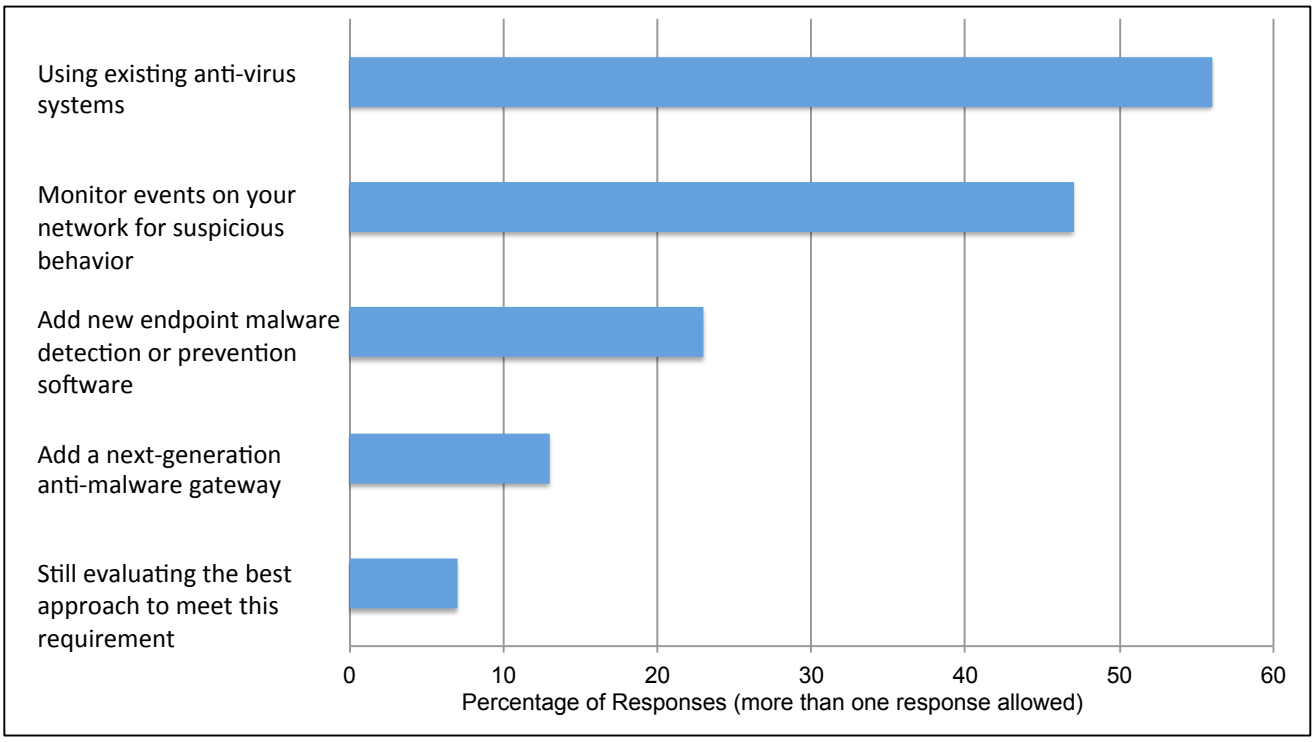
5. PCI 3.0 now requires periodic review of logs from system components outside the PCI Cardholder Data Environment. Which of the following best describes your organization's approach to addressing this requirement for increased security monitoring?



6. If you outsource any of your security functions to a managed service provider (MSP), have you formally documented which PCI DSS requirements are managed by your service provider(s) and which are managed in-house?



7. PCI 3.0 requires organizations to evaluate evolving malware threats from any systems not considered to be commonly affected by malicious software. How do you plan to address this?



Conclusions

With less than half of respondents meeting PCI DSS 3.0 requirements, there is still work to be done for many organizations. However, respondents were confident that their organizations will achieve full compliance by June 30, 2015.

When asked what are the biggest challenges facing organizations in achieving PCI 3.0, the three most frequent responses were:

- Ensuring service providers meet new requirements
- Increased requirement for security monitoring
- Completing a risk-assessment/penetration test

New PCI 3.0 guidance and requirements related to these challenges include:

- 8.5.1: New requirement for service providers with remote access to customer premises, to use unique authentication credentials for each customer
- 10.6.2: New requirement to periodically review logs of system components outside the PCI Cardholder Data Environment based on the organization's policies and risk
- 12.2: Clarification that risk-assessments should be performed at least annually and after significant changes to the environment

Proficio's PCI Compliance Services

Proficio helps our customers meet PCI 3.0 requirements through the following services:

- 24x7 real-time security event collection, analysis and review
- Free 12 month log retention
- Monitoring policies and controls associated with PCI DSS requirements
- Advanced data breach prevention services
- Active Defense that blocks targeted attacks in real-time
- PCI compliance reporting and dashboards
- Vulnerability management including quarterly managed vulnerability scans
- Risk-assessments and penetration testing services

About Proficio

Proficio is a leading provider of Next-Generation Managed Security Services. We are changing the way organizations meet their IT security and compliance goals by providing the most advanced cloud-based solutions to monitor and scan critical assets without the need for added headcount or costly software or hardware systems. Proficio's ProSOC™ service logs, monitors and analyzes organizations' security events. Staffed 24×7 by security experts and using industry leading SIEM technology, ProSOC helps organizations address critical security and compliance needs, prevent data breaches, and reduce operations costs. Our customers value our insight, experience and unrelenting passion for defending their networks and applications from cyber attacks. For more information see: www.proficio.com.

Free Pilot

Try Proficio's SOC-as-a-Service for free for 30 days and receive actionable information and security alerts within 48 hours. Email us at freepilot@proficio.com.

Proficio Headquarters:
3264 Grey Hawk Court
Carlsbad, CA 92010
+1-800-779-5042
info@proficio.com

Proficio Asia:
73 Ubi Road 1
#08-62 Oxley Bizhub
Singapore 408733
+65-6726-2950

Proficio Australia and New Zealand:
264 George Street
Sydney, NSW 2000
Australia
+61(0)2-9258-1153

PROFICIO