COMPLIANCE BEST PRACTICES FOR RETAIL

INSIGHTS

In recent years, sophisticated cyber criminals infected large retail companies such as Home Depot and Target, raising questions about the effectiveness of the retail sector's information security. A recent survey by the Ponemon Institute showed the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014. This appears to be a global phenomenon. Research among British retailers show that 72 percent have not implemented fundamental security required to safeguard both business and customer data.

Organizations require that their security environments operate according to established standards and security best practices. This isn't easy, when often what needs to be checked is unknown, or the process is time-consuming and manual. With configuration and policy settings in a constant state of flux, IT departments must apply hundreds of changes each year.

This is further complicated by compliance challenges inherent within frameworks such as PCI DSS 3.0 that are mandatory for the retail sector. PCI in its latest version requires businesses to implement security controls on a "business as usual" basis, highlighting the expectation that security compliance is no longer a once a year checkbox exercise, but must be fully integrated into traditional business processes.

SOLUTION

Our Compliance Software Blade automatically and continuously monitors your network environment with a library of over 300 security best practices, identifying configuration errors and security weaknesses.

By validating policy and configuration changes in real-time according to best practices and internal policies, the Compliance Software Blade enables security managers to identify issues before policies are implemented. In addition, it addresses the needs of PCI's DSS 3.0 requirements.

72 PERCENT OF RETAILERS HAVE NOT IMPLEMENTED FUNDAMENTAL SECURITY REQUIRED TO SAFEGUARD BOTH BUSINESS AND CUSTOMER DATA[1]

[1] Source: Ponemon 2014 Cost of Data Breach Study

SECURITY BEST PRACTICES

Compliance Blade Best Practices reviews all Check Point management and enforcement points, comparing them to a library of over 300 security best practices. This provides a rich and extensive knowledgebase on how to best configure your environment. Defined by engineers and security experts, each best practice ensures maximum utilization of our security deployments.

AUTOMATED ALERTS

With the network environment constantly in flux, security policy and configuration setting changes are frequent. Security best practices validate each saved configuration change. If it detects a violation that negatively affects the overall security status, it generates an automatic alert. All this happens before policy installation, reducing time associated with manual change management.

PCI-DSS "BUSINESS AS USUAL"

To ensure security controls continue to be properly implemented, PCI-DSS should be implemented into business-as-usual activities as part of an overall security strategy. This can occur by actively monitoring the security controls, ensuring effective and proper operation.

RETAIL COMPLIANCE

The Compliance Software Blade is a critical component of any Check Point security architecture for the retail sector. Not only does it allow firms to audit security policies in real time, but guarantees correct configuration and operation of security controls such as Firewall, Antivirus, IPS (Intrusion Prevention Systems) and DLP (Data Loss Prevention). PCI-DSS specifically refers to these security controls as shown in the following table:

PCI DSS Requirements
1: Install and maintain a firewall configuration to protect cardholder data
5: Protect all systems against malware and regularly update anti-virus software or programs
7: Restrict access to cardholder data by business need to know
8: Identify and authenticate access to system components
11: Regularly test security systems and processes

ASSESS YOUR COMPLIANCE STATUS TODAY

Save time and significantly reduce costs by leveraging your existing security infrastructure to automatically implement the Check Point Compliance Software Blade. Get started with a trial today and learn more about the Compliance Software Blade.

Over 300 Best Practices

"THE CHECK POINT COMPLIANCE SOFTWARE BLADE HAS MADE ALL OF OUR AUDITS AN ORDER OF MAGNITUDE EASIER. IT NOT ONLY MAKES THE AUDITING PROCESS FASTER, BUT INSTILLS CONFIDENCE IN OUR CLIENTS THAT WE TRULY KNOW WHAT WE ARE DOING.

IN THE COMPLIANCE WORLD, CONFIDENCE IS EVERYTHING."

- Customer Testimonial

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com