COMPLIANCE BEST PRACTICES FOR FINANCE

INSIGHTS

It will come as no surprise to most financial services executives that information security incidents are continuing to rise, as are the costs of these intrusions. In 2014, JPMorgan Chase revealed it was the victim of a data breach of unknown size and origin, spotlighting once again the perils of safeguarding information at financial institutions in an era of pervasive cyber threats. Banks, payment card providers, payment processors, and other financial services firms are attractive targets for cyber attacks, an estimated 80% of which are thought to be linked to organized crime. Despite these attacks, many global financial services companies have not implemented the right processes and technologies to prevent, detect, and respond to security risks. Similarly, in the UK, the Information Commissioner's Office (ICO) expressed concern with banks such as Barclays and Santander for potentially repeated violations with non-compliance of the Data Protection Act.

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.

As regulators around the world move to tighten compliance requirements for financial services organizations, improvements in these practices will become increasingly essential to safeguard data as well as ensure compliance with global regulatory bodies.

SOLUTION

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

By validating policy and configuration changes according to best practices and internal policies in real-time, the Compliance Software Blade enables security managers to identify issues before policies are implemented. In addition, it addresses the needs of Basel, Sarbanes Oxley, and National Institue of Standards (NIST) requirements.

COMPLIANCE BLADE BEST PRACTICES MEETS THE NEEDS OF BASEL, SOX, AND NIST

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 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.

RISK MANAGEMENT

All organizations should conduct regular security risk assessments, giving management a clear picture of the risk landscape and of security and reputational exposures. Either the risks should be accepted by the business or they should be treated with security controls such as firewalls, IPS, Anti-Bot, and Threat Emulation (sandboxing). The Compliance Software Blade monitors these security controls and validates that they are working as expected and as intended.

FINANCIAL COMPLIANCE AND AUDIT

The Compliance Software Blade is a critical component of any Check Point security architecture for the finance sector. Not only does it allow firms to audit security policies in real time, but also it ensures correct configuration and functioning of security controls such as firewall, Antivirus, IPS, and DLP. Any regulation or audit requiring a business to understand what security is working and what is not working, a critical component of any Risk Management framework, will benefit from the Compliance Software Blade.

Compliance Requirements in the Finance Sector	
NIST 800-53	Assessing security controls as part of a comprehensive continuous monitoring process
SOX/CobiT	Establish a platform to share best practices and to capture information on defects and mistakes to enable learning from them
Basel	The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures
Dodd-Frank/GLBA	Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures

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