HEALTHCARE DEFENSE:
PROTECT DATA, ENSURE COMPLIANCE AND MAINTAIN COMPLETE VISIBILITY INTO SECURITY RISK

THE HEALTHCARE CHALLENGE

Numerous recent attacks on healthcare organizations highlight the need for cyber security that extends beyond traditional anti-virus software and multiple compliance checklists. Patient health records have the highest value on the black market – even more than credit cards or other financial data. The digital age we currently live also gives us pause. Our growing dependence on connected medical devices has provided an expanded and vulnerable attack surface. For these reasons, healthcare companies are prime targets for cybercriminals.

Healthcare environments have highly demanding IT infrastructures and networks, where perimeters are no longer well defined. Threats grow more intelligent every day and we need to define the right way to protect healthcare companies in the modern and ever-evolving threat landscape. Healthcare is a profoundly complex, multifaceted ecosystem that demands advanced protection from sophisticated cyber threats. This means that integrated solutions are needed to protect against advanced persistent threats and zero-day attacks, and at the same time, help the organization uphold HIPAA and PCI DSS compliance while maintaining complete visibility into operations with centralized security management.

There is a wide proliferation of point security products available throughout the industry. However, most of these products tend to be reactive and tactical in nature rather than architecturally oriented. Today's healthcare organizations need a single architecture that combines high performance network security devices with real-time proactive protections.

> **"MANY OF THE DEVASTATING SECURITY BREACHES THAT OCCURRED IN 2018 WERE PREVENTABLE, HAD THE RIGHT TECHNOLOGY AND SOLUTIONS BEEN IN PLACE."**

AN INTEGRATED SOLUTION

Protections should automatically adapt to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections must integrate seamlessly into the larger IT environment, and the architecture must provide a defensive posture that collaboratively leverages both internal and external intelligent sources.

Check Point offers an integrated solution, built specifically for the unique cyber security needs of healthcare organizations. In essence, our healthcare solution stresses a centralized approach comprised of three components – advanced threat prevention for targeted threats and zero-day attacks, combined with compliance software blade to ensure HIPAA and PCI DSS compliance, integrated through SmartEvent to consolidate monitoring, logging, reporting and event analysis in a single console – to bring you comprehensive, easy-to-understand threat visibility.

THE FIRST COMPONENT: COMPREHENSIVE PROTECTION AGAINST KNOWN MALWARE, ADVANCED PERSISTENT THREATS AND ZERO-DAY ATTACKS

Advanced Threat Prevention

With the amount of growing attacks, Check Point offers a comprehensive solution, one that can defend against known malware, new forms of malware as well as advanced, targeted attacks, while also defending against downtime, data loss, productivity impact, and reputational risk. Working to constantly combat these emerging threats while reducing complexity and increasing operational efficiency may seem daunting, but the solution to this challenge is available in the form of a comprehensive, advanced threat prevention solution.

Check Point's multi-layered Next Generation Threat Prevention solutions protect enterprises from growing internet attacks using a single security gateway. A range of deployment options, from all-in-one appliances to add-on features and cloud-based service enable you to reduce complexity and choose the most effective means for adding advanced threat prevention to your network security infrastructure.

SandBlast Zero-Day Protection

Recent healthcare breaches have shown us the power of advanced persistent threats and zero-day attacks. These attacks are targeted and use sophisticated malware and other techniques to avoid detection. Antivirus, Next Generation Firewalls, and other core security solutions focus on signature-based threats. While these technologies are still important to protect against signature-based viruses, APTs and Zero-Day attacks will penetrate those systems with ease.

As part of Check Point's Next Generation Threat Prevention solutions, SandBlast Zero-Day Protection uses innovative Threat Emulation technology to proactively protect against evasion-resistant malware, making it a critical solution for healthcare security.

Threat Emulation detects the use of exploitation techniques by carefully examining activity in the CPU of the sandbox host, and its execution flow at the assembly code level before the malicious payload has a chance to run. As a result, it preempts most, if not all, possibilities of hackers evading detection. The speed and accuracy of detection, and the fact that the attack is detected before the malware is even downloaded to the end point device, make advanced sandboxing the best technology in detecting unknown threats.

SandBlast Threat Extraction complements this solution by promptly delivering safe content, or clean and reconstructed versions of potentially malicious files, maintaining uninterrupted business flow. By eliminating unacceptable delays created by traditional sandboxes, Threat Extraction makes real-world deployment in prevent mode possible, not just issuing alerts, but blocking malicious content from reaching users in the first place.

SANDBLAST ZERO-DAY PROTECTION

Detects and blocks new or previously undiscovered malware, taking threat defense to the next level.

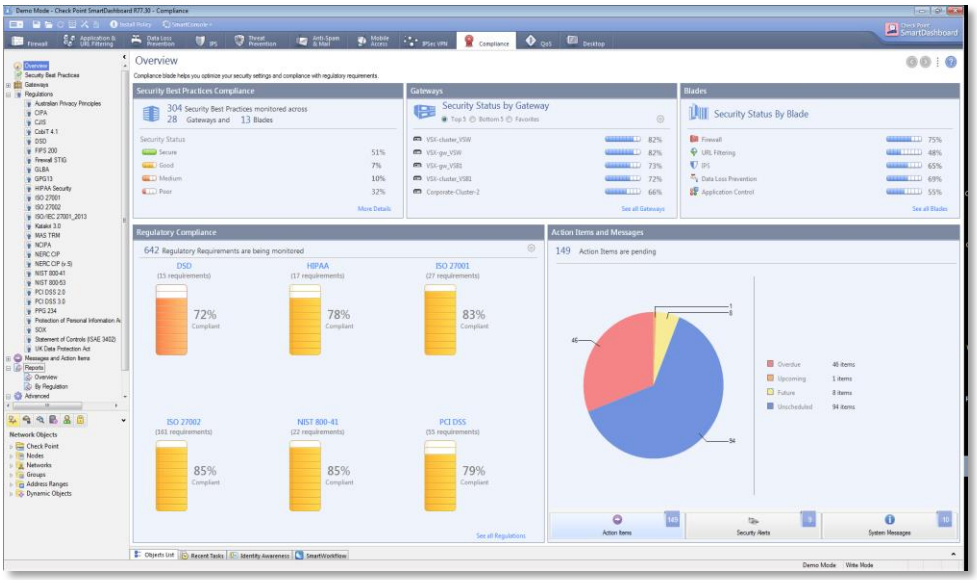
- ✓ Best catch rate of unknown malware
- ✓ Makes it virtually impossible for hackers to evade detection
- ✓ Identifies and blocks threats before it deploys
- ✓ Rapid reconstruction of files and delivery of safe content
- ✓ Reduces risk of expensive breaches or downtime
- ✓ Integrated protection maximizes operational value and minimizes TCO

Sandblast zero-day protection uses innovative threat emulation technology to proactively protect against evasion-resistant malware, making it a critical solution for healthcare security.

THE SECOND COMPONENT: PROTECT PATIENT HEALTH INFORMATION AND MAINTAIN COMPLIANCE

The Check Point Compliance Software Blade monitors your management, Software Blades and security gateways to constantly validate that your Check Point environment is configured in the best way possible. The Check Point Compliance Software Blade provides 24/7 security monitoring, security alerts on policy violations, and out-of-the-box audit reports.

The Compliance Blade validates all policy and configuration changes against best practices prior to the changes being installed, thereby enabling Security Managers to identify issues and problems in real time and before the policy is actually implemented. Companies can be continuously assured that their environment is secure and operating in line with vendor best practices. Audit and compliance reporting has never been easier, with simple HIPAA based reports that can be sent directly to managers and auditors, enabling organizations to reduce the time and costs associated with proving that each specific configuration setting is defined correctly.



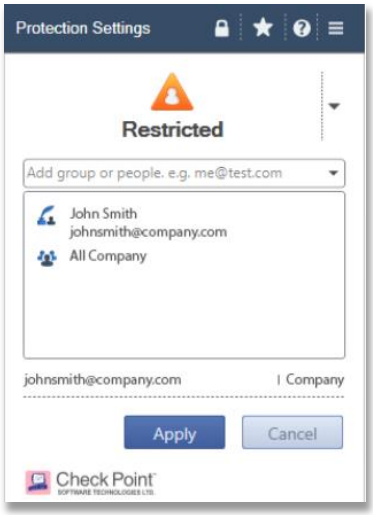
Ultimately, this frees up resources to focus on security management. The Compliance Software Blade is fully integrated into the Check Point Software Blade Architecture, providing a complete view of security status across Check Point Gateways and Software Blades. On-screen security alerts and pre-defined compliance reports enable organizations to reduce the time and costs associated with maintaining optimized security and audit preparation.

Prevent Data Loss by Ensuring Safe Sharing of Documents

Compliance Software Blade can also integrate Data Loss Prevention Software Blade and Check Point Capsule Docs to enable organizations to seamlessly protect documents, ensuring access for authorized users only. Business sensitive documents are encrypted to ensure that contents are protected wherever they go.

COMPLIANCE BLADE BENEFITS

- ✓ Improves overall security
- ✓ Identifies configuration errors and weaknesses
- ✓ Scans all changes before policy changes are implemented
- ✓ Warns of potential policy and compliance violations
- ✓ Actionable security recommendations and guidance on how to improve security
- ✓ Performs continuous monitoring, not periodic auditing
- ✓ Saves Security Managers time and reduces cost of audit
- ✓ Generates regulatory reports based on real-time security settings



CAPSULE DOCS

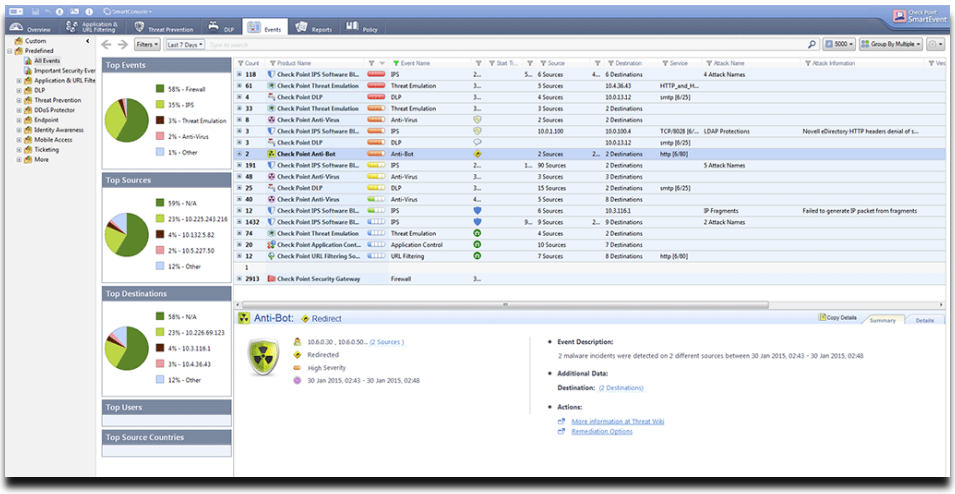
- ✓ Secure all documents by default upon creation
- ✓ Ensure only authorized individuals and groups have access to documents
- ✓ Share and upload documents without the risk of losing data
- ✓ Permissions can be set to: read, edit, print, change classification, remove protection, modify authorized users, print screen and copy/paste
- ✓ View and edit documents on personal computers, iOS and Android smartphones and tablets

THE THIRD COMPONENT: SECURITY MANAGEMENT THAT GIVES COMPLETE OPERATIONAL VISIBILITY

Today's security is complex, requiring multiple devices to cover the network. These devices generate voluminous amounts of logs. In a typical enterprise, an intrusion detection system alone can produce more than 500,000 messages a day and firewalls can generate millions of log records a day.

It is not humanly possible to scan all this data. Even with automated log analysis, it is time-consuming to identify critical security incidents and to investigate them. To add to this challenge, data collected by different devices often do not provide a complete picture of one's security posture. What appears to be normal behavior when viewed on its own may reveal evidence of abnormal activity when that data is cross-correlated and analyzed.

By automating the aggregation and correlation of raw log data, we drastically reduce the amount of data you have to review so you can quickly isolate the real security threats. Because we aggregate data from all Check Point gateways and endpoints, we detect patterns that might otherwise go un-noticed.



SmartEvent consolidates monitoring, logging, reporting and event analysis functions within the same console. This means you can easily move from tracking trends to investigating and mitigating events with just a few clicks. If you are worried about a new malware that is making the rounds, our free-text search lets you quickly see if any instance of it was discovered on your network. Need to send reports to your manager or auditor? It's very simple to set up custom reports in SmartEvent.

With SmartEvent, your security team can focus on the threats that pose the greatest risk to your business – rather than drown in data.

SMARTEVENT

Complete Threat Visibility to Better Understand, Prioritize and Respond To Critical Security Events

- ✓ Integrated security monitoring for firewall, IPS, anti-virus, anti-bot, Threat Emulation, URL filtering and Application Control
- ✓ Create rich, personalized reports for security managers, network engineers and executives
- ✓ Helps keep stakeholders abreast of security status.
- ✓ Monitor security on-the-go with new web and tablet portal
- ✓ Quickly isolate real threats in real-time
- ✓ Minimizes amount of data to be reviewed
- ✓ Enables quick action to mitigate threats
- ✓ Constant monitoring helps improve security posture

THE BOTTOM LINE

So, how do you accomplish this? You need intelligent technology that keeps up with the threat landscape – technology that can detect and block both known and unknown threats, as well as comply with regulations and give you complete visibility into the security operations of your company.

As evasion techniques evolve and get smarter, so must the technology to keep your business secure. Check Point's integrated solution for healthcare allows your company to be proactive in its approach to security, rather than reactive. When you are constantly reacting to problems after they occur, rather than preventing them, it wastes time, energy, and money that your company may not have to spend.

These threats are real. How long before it's realized that yesterday's security technology is not keeping pace with modern threats, and sophisticated hackers? How long before we take network and data security seriously? Perhaps one of the biggest lessons we can learn is that many of the devastating security breaches that occurred in 2018 and 2019 were preventable, had the right technology and solutions been in place.

To learn more about Check Point's solutions for Healthcare, please visit our website at www.checkpoint.com/products-solutions/healthcare/.

CHECK POINT OFFERS AN INTEGRATED SOLUTION, BUILT SPECIFICALLY FOR THE CYBER SECURITY CHALLENGES OF HEALTHCARE ORGANIZATIONS.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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: 650-628-2117 | www.checkpoint.com