

**\*\*\*EMBARGOED UNTIL THURSDAY, FEBRUARY 21, 2013 AT 8:30 AM EST\*\*\***

**Media Contact**

Juanita Mo  
Check Point Software Technologies  
+1 650.628.2138  
[press@us.checkpoint.com](mailto:press@us.checkpoint.com)

**Investor Contact**

Kip E. Meintzer  
Check Point Software Technologies  
+1 650.628.2040  
[ir@us.checkpoint.com](mailto:ir@us.checkpoint.com)

**CHECK POINT UNCOVERS HIDDEN SECURITY RISKS ON ENTERPRISE NETWORKS**

*2013 Security Report Defines Security Priorities for Organizations Worldwide*

**SAN CARLOS, CA – Feb. 21, 2013** – [Check Point® Software Technologies Ltd.](http://www.checkpoint.com) (Nasdaq: CHKP), the worldwide leader in securing the Internet, today issued its 2013 Security Report, uncovering major security risks that impact organizations worldwide. The new report examines top security threats, risky web applications that compromise network security, and loss of data caused by unintentional employees. Most importantly, the report provides security recommendations on how to protect against these threats.

For a full copy of the Check Point 2013 Security Report, please visit:  
[www.checkpoint.com/campaigns/security-report/index.html](http://www.checkpoint.com/campaigns/security-report/index.html)

As the arms race between attackers and IT professionals unfolded in 2012, it has become clear that many of the most serious threats stayed hidden from network administrators. These threats come from ever-changing techniques deployed by criminal hackers in addition to risky online activities by employees, which unintentionally create vulnerabilities on the corporate network. In order to develop a strong security blueprint, organizations must first be aware of and fully understand the activities occurring on their networks.

Based on research of nearly 900 companies, the Check Point 2013 Security Report sheds light on what is hiding on corporate networks, and the major security risks exposed to organizations on a daily basis:

**Hidden Security Threats**

From crimeware to hacktivism, cyberattacks will continue to evolve this year, impacting organizations of all sizes. The research revealed that 63% of organizations were infected with bots, and more than half were infected with new malware at least once a day. The report reveals a list of top threats, including the most infamous botnets, top malware location by country, top vendor vulnerabilities and exposures, and SQL injection events by source country, among other surprising findings.

**Risky Web 2.0 Applications**

The surge in web 2.0 applications has given criminal hackers unprecedented options to penetrate corporate networks. The research found 91% of organizations used applications with potential security risks. These risky web applications are brought to light in the report, including frequency and usage of anonymizers, P2P applications, file storage and sharing applications, and top social networks – all of which can potentially open a backdoor to enterprise networks.

**Data Loss Incidents**

Corporate information is more accessible and transferable today than ever before, leading to higher risk of data loss or leakage. More than half of the organizations studied had at least one potential data loss incident. The report exposes the different types of sensitive data leaked and lost, including PCI related information as well as HIPAA-protected health information. It also sheds light on the industries with the highest tendency toward data loss.

“Our research uncovered many alarming vulnerabilities and security threats on networks that most organizations were not aware of,” said Amnon Bar-Lev, president of Check Point Software Technologies. “With clearer visibility, IT professionals can now better define a security blueprint to protect their organizations from the constant stream of evolving security threats, ranging from botnets, to employees using risky web



applications like anonymizers, to data loss.”

“Check Point’s 2013 Security Report is a resounding call-to-action, providing unique insight into the magnitude and breadth of the current and emerging threat landscape,” said Alberto Dosal, chairman of the board of Compuquip Technologies, one of South Florida’s largest, fully integrated IT service providers. “It is truly an impressive and comprehensive must-read for any C-level executive.”

As a trusted security leader, Check Point helps organizations of all sizes implement a security blueprint and architecture that aligns with business needs. The company’s award winning portfolio of products provides organizations with multi-layered security to combat all types of threats identified in the report. Check Point Security Gateways running Check Point Software Blades, such as IPS, Application Control, URL Filtering, Antivirus and Anti-Bot, can detect and prevent the latest threats. Check Point ThreatCloud™ feeds software blades with real-time intelligence and signatures. Additionally, Check Point Secure Web Gateway blocks access to malware infested websites and usage of high risk applications like anonymizers. And Check Point DLP Software Blade helps organizations pre-emptively protect sensitive information from unintentional loss and leakage.

To read the full report, please click here:

<http://www.checkpoint.com/campaigns/security-report/index.html>

For more information on conducting an onsite security analysis of your infrastructure, please click here:

<http://www.checkpoint.com/campaigns/3d-analysis-tool/index.html>

#### **About the Report:**

The Check Point 2013 Security Report provides insight into network security events that occurred in organizations worldwide and recommendations on how to protect against them. The report is based on research and analysis of nearly 900 companies gathered from Check Point 3D security reports, Check Point ThreatCloud™, and Check Point network of sensors.

#### **About Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point’s award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

©2013 Check Point Software Technologies Ltd. All rights reserved.

