Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point and Bit9 + Carbon Black Advanced Threat Protection

TODAY'S SECURITY CHALLENGE

Security-conscious organizations are adopting next-generation solutions to protect against advanced threats that evade traditional security tools. As well-funded cybercriminals launch increasingly sophisticated and targeted attacks, a defense-in-depth strategy including solutions for next-generation endpoint security and incident response are required.

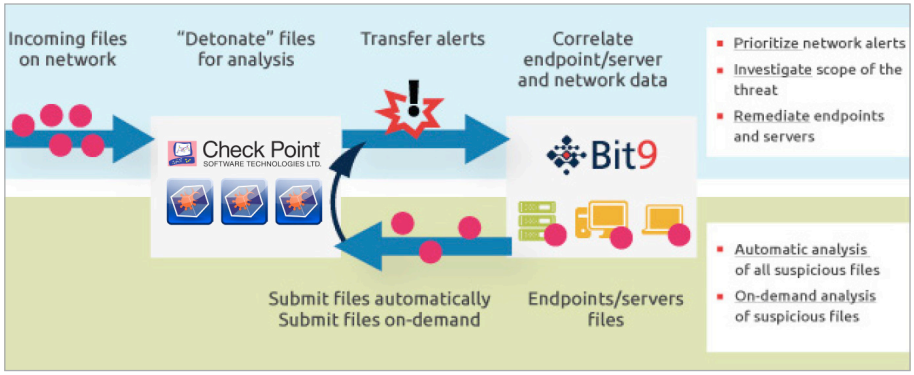
SOLUTION OVERVIEW

Integrating with Check Point gives Bit9 + Carbon Black users the ability to easily detect, investigate and respond to network-based alerts on the endpoint. When a network alert is received, the data flows automatically to Bit9 + Carbon Black, which validates whether the attack has landed or executed on any endpoint or server across the enterprise. This layer of endpoint visibility helps security analysts prioritize alerts, dramatically reduces the time required by security analysts to investigate alerts, increases response speed and immediately enhances an organization's investments in their network security solutions.

Bit9 + Carbon Black makes verifying network-based alerts easier than ever. Bit9 + Carbon Black integrates seamlessly with Check Point's next-generation firewall and Threat Emulation services to provide unique capabilities that drive rapid detection, response and remediation of potential threats.

The secret to such comprehensive endpoint visibility is collecting the right kinds of data. Bit9 + Carbon Black collects and stores the data that incidents responders need most during an investigation: file inventory, execution events, file system modifications, registry modifications, Network Connections.

Bit9 + Carbon Black provides customers with the tools needed to see what is running on every device, detect threats in real-time, rapidly respond to incidents and prevent future security incidents.



- **Prioritize network alerts**
  Automatically correlate Check Point Threat Prevention network alerts with real-time endpoint data to determine which alerts are actionable and prioritize them based on the number of systems infected.
- **Rapidly respond to alerts**
  Gain instant visibility into file execution events, file system modifications, registry changes and unique binary execution data to understand if a malicious file executed, locate every instance of the suspicious file or process across your enterprise, and accelerate incident response.
- **Prevent attacks**
  Reduce the total threat surface by using the Check Point Threat Emulation Cloud Service to perform real-time analysis of suspicious files. Based on the results, Bit9 can immediately prevent those malicious files from executing on your endpoints and spreading throughout your enterprise.
- **Actionable threat management**
  An integrated Threat Prevention solution including NSS-leading IPS, Antivirus, Anti-Bot, and Threat Emulation with automatic sharing of new attack information with ThreatCloud and Carbon Black.

Bit9 + CARBON BLACK
ADVANCED THREAT PROTECTION FOR ENDPOINTS AND SERVERS
Contact Bit9 + Carbon Black

GET NETWORK PREVENTION OF ADVANCED THREATS AND MALWARE
Request a Free Trial

softwareblades™

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

WHAT MAKES BIT9 + CARBON BLACK UNIQUE?

Bit9 + Carbon Black helps organizations reduce their threat surface and rapidly detect and respond to incidents.

- Bit9 + Carbon Black offers the only real-time monitoring and recording capabilities for endpoints and servers to provide organizations with immediate actionable intelligence about potential threats.
- Bit9 + Carbon Black enables organizations to take a policy-based approach to security. Security teams can decide which files, applications and processes are trusted and then set policies to block or further analyze everything else. This enables organizations to be offensive in their security policies to reduce the threat surface.
- Bit9 + Carbon Black enables organizations to rapidly detect and respond to threats. Bit9 + Carbon Black leverages real-time visibility, external threat intelligence feeds and Advanced Threat Indicators to instantly detect threats on endpoints and servers and arm security teamswith the data needed to rapidly respond.
- Bit9 + Carbon Black provides a real-time visual history of every execution and process that has occurred on each endpoint to provide incident responders with the precise data they need to investigate and respond. Whereas traditional incident response has been tedious, time-consuming and imperfect, Bit9 + Carbon Black helps incident responders reduce investigation time from days or weeks to minutes or hours.

WHAT MAKES CHECK POINT UNIQUE?

Check Point offers a unified next generation solution that prevents advanced threats and malware attacks and enables an organization to easily and confidently control access to millions of web sites. Protections include stopping application-specific attacks, botnets, targeted attacks, APTs, and zero-day threats.

- ThreatCloud Emulation Service discovers AND prevents sophisticated threats and zero-day attacks with real-time behavioral analysis of malware code even within encrypted communication (SSL and TLS).
- ThreatCloud Emulation works with your existing infrastructure. There is no need to install any new equipment.
- Reduce operational overhead with a low monthly price for the entire organization, based on incoming file volume.
- A unique agent for exchange server monitors email attachments, even without Check Point infrastructure in the organization.
- Zero false-positives means you can secure the network without stopping the flow of business.
- An integrated Threat Prevention solution including NSS-leading IPS, Antivirus, Anti-Bot, and Threat Emulation with automatic sharing of new attack information with ThreatCloud and Bit9.

WHAT MAKES THE JOINT SOLUTION UNIQUE?

The integration of Bit9 + Carbon Black with Check Point Next Generation Threat Prevention gives security analysts a holistic view of their entire ecosystem, which enables organizations to strengthen their security posture, reducing their surface of attack, and more rapidly respond to threats. When Check Point detects malware or suspicious activity, Bit9 + Carbon Black can validate if the attack was able to land and execute, where it may have spread and what other files or processes were spawned as a result. To prevent any further execution and propagation, Bit9 + Carbon Black can issue an enterprise-wide ban on the malware to immediately contain the threat. This unique integration of next-generation network and endpoint security can help you improve your security posture by adding greater levels of protection and response while simultaneously increasing the efficiency of your security operations team.

ABOUT BIT9 + CARBON BLACK

Bit9 + Carbon Black offers the industry's most complete solution for advanced threat protection for endpoints and servers. Bit9 + Carbon Black helps companies reduce their attack surface and rapidly detect and respond to threats. Carbon Black technology delivers "incident response in seconds," and Bit9's industry-leading prevention technology continuously monitors and records all activity on endpoints and servers and stops cyber threats that evade traditional security defenses. Organizations are able to gain immediate visibility into everything running on their endpoints and servers; real-time signature-less detection of and protection against advanced threats; a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents; and real-time integration with network security solutions. More information is available at https://www.bit9.com/.

Bit9 + Cb CARBON BLACK
ADVANCED THREAT PROTECTION FOR ENDPOINTS AND SERVERS
Contact Bit9 + Carbon Black

ABOUT CHECK POINT

Check Point Software Technologies Ltd., the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats. 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. The Software Blade Architecture provides flexible simple, and easy to deploy security modules that enable customers to select the security they need to build a custom Check Point security gateway solution. More information is available at http://www.checkpoint.com.

GET NETWORK PREVENTION OF ADVANCED THREATS AND MALWARE
Request a Free Trial

CONTACT CHECK POINT

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

May 15, 2014