CHECK POINT + CARBON BLACK
ADVANCED THREAT PROTECTION

BENEFITS

- **Prioritize Network Alerts**

  Automatically correlate Check Point Threat Prevention events with real-time endpoint data to determine which events are actionable and prioritize them based on the number of systems infected

- **Rapidly Respond to Alerts**

  Identify if a malicious file has executed and gain instant visibility into file execution events, file system modifications, registry changes and unique binary execution data; locate every instance of the suspicious file or process across your enterprise and accelerate incident response

- **Prevent Attacks**

  Check Point's SandBlast Threat Emulation Cloud Service performs real-time analysis of suspicious files and reduces the total attack surface. Based on these results, Carbon Black immediately prevents those malicious files from executing on your endpoints and spreading throughout your enterprise

- **Actionable Threat Management**

  An integrated Threat Prevention Platform including NSS-leading IPS, Antivirus, Anti-Bot, and Threat Emulation with automatic sharing of new attack information with ThreatCloud and Carbon Black

TODAY'S SECURITY CHALLENGE

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

WHAT MAKES CARBON BLACK UNIQUE?

Carbon Black helps organizations reduce their threat surface and rapidly detect and respond to incidents. Carbon Black offers real-time monitoring and recording capabilities for endpoints and servers in order to provide organizations with immediate actionable intelligence about potential threats. This enables organizations to take a policy-based approach to security. Carbon Black also leverages real-time visibility, external threat intelligence feeds, and Advanced Threat Indicators to instantly detect threats on endpoints and servers. Carbon Black's platform also supplies a real-time visual history of every execution and process that has occurred on each endpoint to provide incident responders the precise data they need to investigate and respond.

WHAT MAKES CHECK POINT UNIQUE?

Check Point provides a Next-Generation Threat Prevention Platform that blocks advanced threats and malware attacks, and enables organizations to easily and confidently control access to millions of web sites. Security features include stopping application-specific attacks, botnets, APTs, and zero-day threats. Check Point's software blade architecture includes NSS-leading IPS, Antivirus, Anti-Bot and Application Control. SandBlast Threat Emulation discovers and prevents sophisticated threats and zero-day attacks through CPU-level emulation and real-time behavioral analysis of malware code even within encrypted communications (SSL and TLS). Threat Emulation incorporates automatic sharing of new attack information with ThreatCloud and Carbon Black.

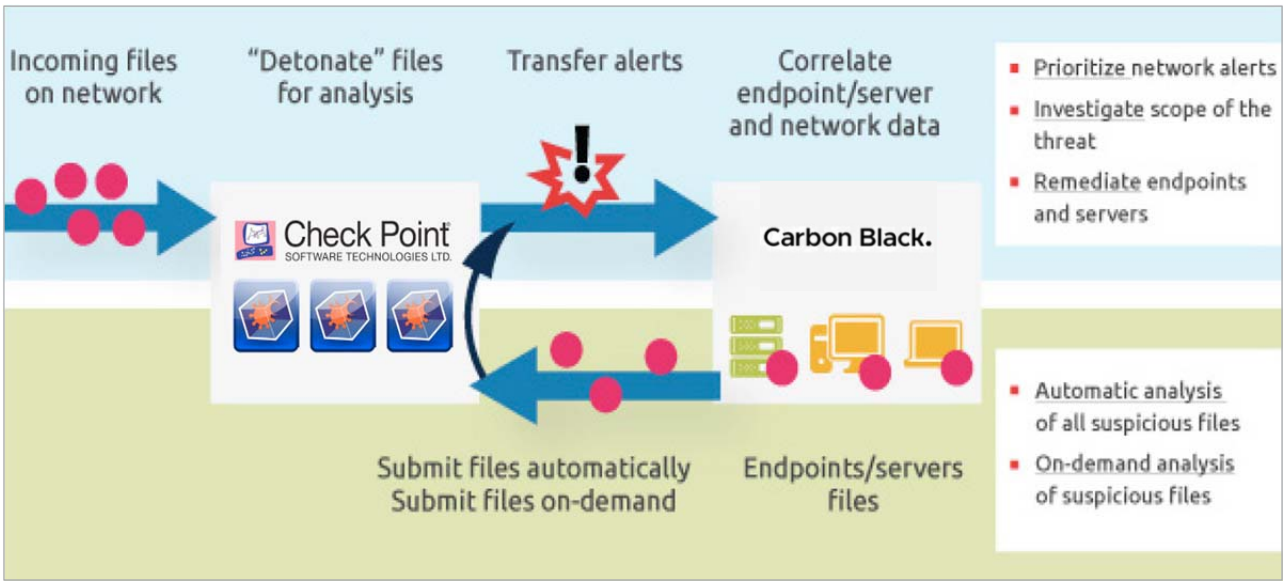
JOINT SOLUTION

The Check Point and Carbon Black integration provides users the ability to easily detect, investigate and respond to network-based events on the endpoint. When a network event is received, the data flows automatically to 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 investment in their network security solutions. Carbon Black integrates seamlessly with Check Point's Next-Generation Threat Prevention Platform to provide unique capabilities that drive rapid detection, response and remediation of potential threats.

The secret to comprehensive endpoint visibility is collecting factual and relevant sets of data. Carbon Black collects and stores this data, which incident responders utilize during an investigation: file inventory, execution events, file system modifications, registry modifications and network connections.

ADVANCED THREAT PROTECTION — INTEGRATED NETWORK AND ENDPOINT SECURITY

- The integration of Carbon Black with Check Point's Next-Generation Threat Prevention Platform gives security analysts a holistic view of their entire ecosystem. This enables organizations to strengthen their security posture, reduce their attack surface, and more rapidly respond to threats.
- The joint solution provides customers with the tools necessary to see what is running on every device, detect threats in real-time, rapidly respond to incidents and prevent future security incidents.
- When Check Point detects malware or suspicious activity, Carbon Black can validate whether the attack was able to land and execute. Carbon Black can also determine where the attack may have spread within the organization and what other files or processes were spawned.
- To prevent any further execution and propagation, Carbon Black can issue an enterprise-wide ban on the malware to immediately contain the threat.
- The unique integration of next-generation threat prevention 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 CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises — from networks to mobile devices — in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT CARBON BLACK

Carbon Black (www.carbonblack.com) offers the industry's most complete solution for advanced threat protection for endpoints and servers. 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 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.

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