

# CHECK POINT + OPSWAT SECURE DEVICE ACCESS

## Benefits

- Automatically quarantine or block non-compliant or compromised remote laptops and mobile devices
- Build custom comprehensive compliance and security policies for specific regulatory or corporate needs on Windows, Mac, Android, and iOS
- Provide clear instructions to blocked devices for self-remediation or configure automatic remediation
- Determine true state of antivirus, disk encryption, password protection, personal firewall, and more
- Proprietary interrogation methods provide industry leading accuracy and reliability of security software state and configuration
- 3 ways to find compromised devices:
  - 1) Scan any antivirus software's log files for un-remediated threats
  - 2) Identify infection patterns in antivirus scan logs
  - 3) Perform supplementary anti-malware scan with up to 43 antivirus engines

## INSIGHTS

Lack of control and visibility into the security state of devices complicates today's security mobility challenges. Existing solutions either provide too little information about the device, or require full management. The Gears platform is different. Gears provides accurate, detailed information about the security configuration, regulatory compliance, and infection state of all devices – managed and unmanaged.

OPSWAT Gears uniquely provides enhanced posture checking for remote devices, without corporate active directory membership or managed endpoint security software. Your users are enabled to use their own laptop or device and choose their own mobile security software – Gears allows you to monitor their antivirus, firewall, disk encryption, and more. Powered by industry-leading technology used in over ten million endpoints around the world, Gears represents the latest generation of device posture checking technology, provided as a service.

## JOINT SOLUTION

The Check Point Mobile Access Software Blade is the safe and easy solution to connect to corporate applications over the internet with your Smartphone, tablet or PC. The solution provides enterprise-grade remote access via both Layer-3 VPN and SSL VPN, allowing you simple, safe and secure connectivity to your email, calendar, contacts and corporate applications.

OPSWAT Gears performs continuous or on-demand monitoring of the security configuration, risk, and infection state of remote laptops and mobile devices. When these devices attempt to connect to a Check Point gateway with the Mobile Access Software Blade enabled (MAB), MAB queries Gears for the compliance state and in turn grants or denies access. Patent-pending technologies between Check Point MAB and OPSWAT Gears provide the smoothest user experience in an advanced remote access security solution. A small persistent or dissolvable agent on the endpoint collects data and reports it to the Gears cloud for monitoring. Use for ad hoc security assessments of guest devices, as well as persistent monitoring of managed devices. Optional remediation features and clear compliance messages assist users in self-remediation.

By integrating Gears with Check Point Mobile Access, administrators centrally define security baselines for their entire organization, and provide automatic access control of noncompliant, risky or compromised devices via enforcement by the Mobile Access Gateway. Use this for security as well as regulatory compliance with HIPAA, FINRA/SEC and more.

## A BETTER APPROACH TO SECURE ACCESS FOR MOBILE DEVICES

Work anytime, anywhere, with the combination of OPSWAT's Gears and Check Point's Mobile Access Gateway. Ensure corporate security policies by providing Security Administrators the ability to monitor, manage, and restrict access.

- OPSWAT Gears provides the most comprehensive posture checking of laptops and mobile devices in the industry
- Check Point Mobile Access simply, safely and securely connects you to email, calendar, contacts and corporate applications

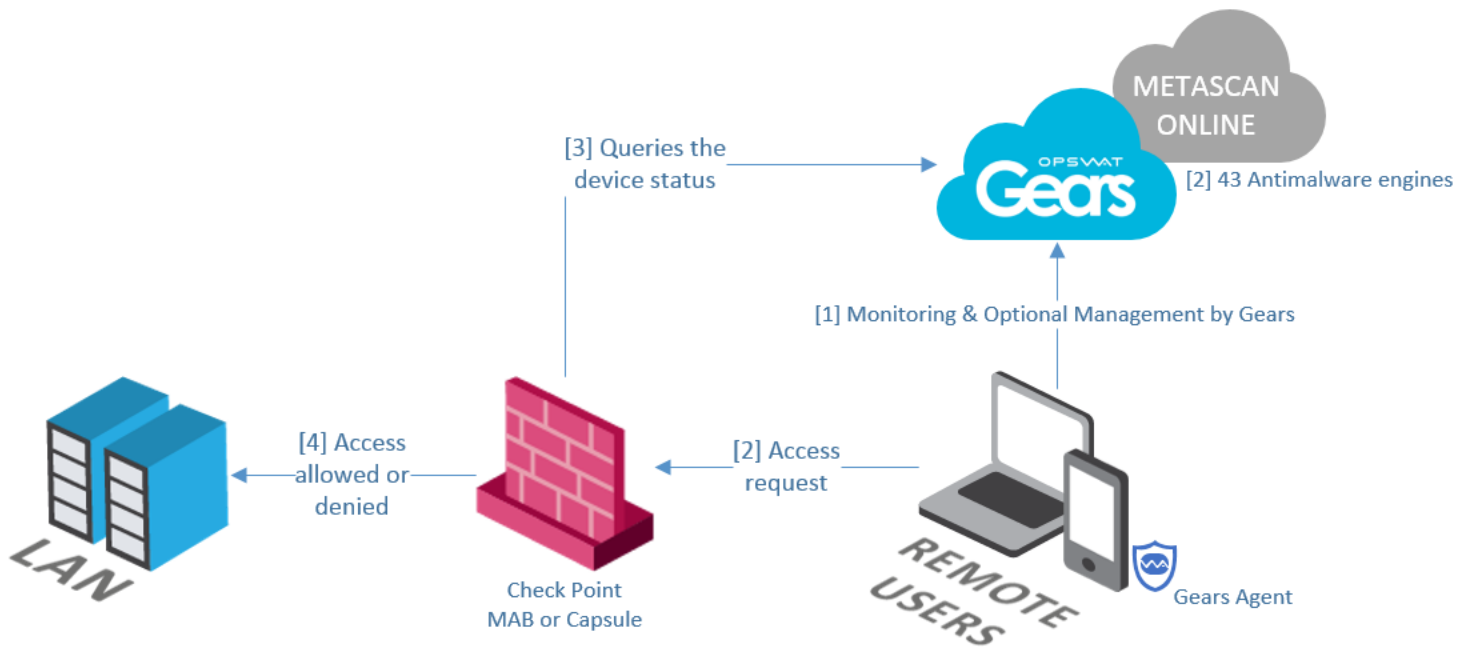


Figure 1: Integration Diagram

## ABOUT CHECK POINT

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects 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' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

## ABOUT OPSWAT

OPSWAT is a San Francisco-based software company that provides solutions to secure and manage IT infrastructure. Founded in 2002, OPSWAT delivers solutions that provide manageability of endpoints and networks, and that help organizations protect against zero-day attacks by using multiple antivirus engines scanning and document sanitization. OPSWAT's intuitive applications and comprehensive development kits are deployed by SMB, enterprise and OEM customers to more than 100 million endpoints worldwide. To learn more about OPSWAT's innovative and unique solutions, please visit [www.opswat.com](http://www.opswat.com).

### 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](mailto: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](http://www.checkpoint.com)