# CHECK POINT AND SONPO

## A SECURE FILE EXCHANGE SOLUTION

## SAFE FILE EXCHANGE

### Solution Components

- Check Point SandBlast (sandboxing)
- SOFiE – Safe Online File Exchange

### Solution Benefits

- Integrated file protection using Check Point SandBlast Zero-Day Protection
- Clientless solution - no plugins or other software required for clients; a web browser is sufficient
- SOFiE leverages APIs to fully integrate with the SandBlast Appliance and SandBlast Cloud

### Solution Features

- Identify new malware hidden in over 40 files types, including: Adobe PDF, Microsoft Office, Java, Flash, executables, and archives
- Configurable inspection of files
- Option to set granular access rights
- Flexible deployment options; on-premises or cloud
- Option to export logs to remote syslog for external processing (SIEM support)
- Threat Emulation detailed report generated for each file emulation

Attacks from unknown and zero-day threats pose a critical risk to businesses. Often these come in the form of malicious files attached to emails or downloaded from the web. Businesses rely on a detection strategy where their help desk or Security Operations Center (SOC) staff isolate and "clean" infected hosts after the attack has breached their protections and infected an employee computer, but this is a time consuming and ineffective strategy.

## A SECURE FILE EXCHANGE SOLUTION

Check Point and Sonpo are partnering to protect businesses from unknown and zero-day threats without compromising business productivity. With our prevent-first, secure file exchange solution, businesses can reduce the risk of unknown attacks while reducing security overhead and ensuring productivity.

The SONPO's application SOFiE (Safe Online File Exchange) offers a secure solution to receiving and sending files of any size and type both inside a company and outside for communicating with other entities. It significantly increases the protection to a level very difficult to achieve when using other file exchange solutions, such as email or FTP server for example. The integration of SONPO's application SOFiE with Check Point SandBlast Zero-Day Protection provides customers with unparalleled security protection against ransomware, malware, and advanced unknown threats.

SOFiE is a clientless solution which doesn't require plugins or other software, and it can replace emails and other legacy services for file exchange, which could have many issues in customer environments, including the following:

- Attachment size:
  Most email servers limit email size to less than 50 MB. E-mail communication is therefore not suitable for large documents.
- Attachment blocking:
  Security nowadays often requires using highly restrictive policies to block executable files, documents containing macros, and archives containing such files.
- Using public online services and cloud systems is often needlessly complicated for exchanging files, and also problematic in terms of security of company data, or in terms of the protection of personal data in relation to the General Data Protection Regulation (GDPR).

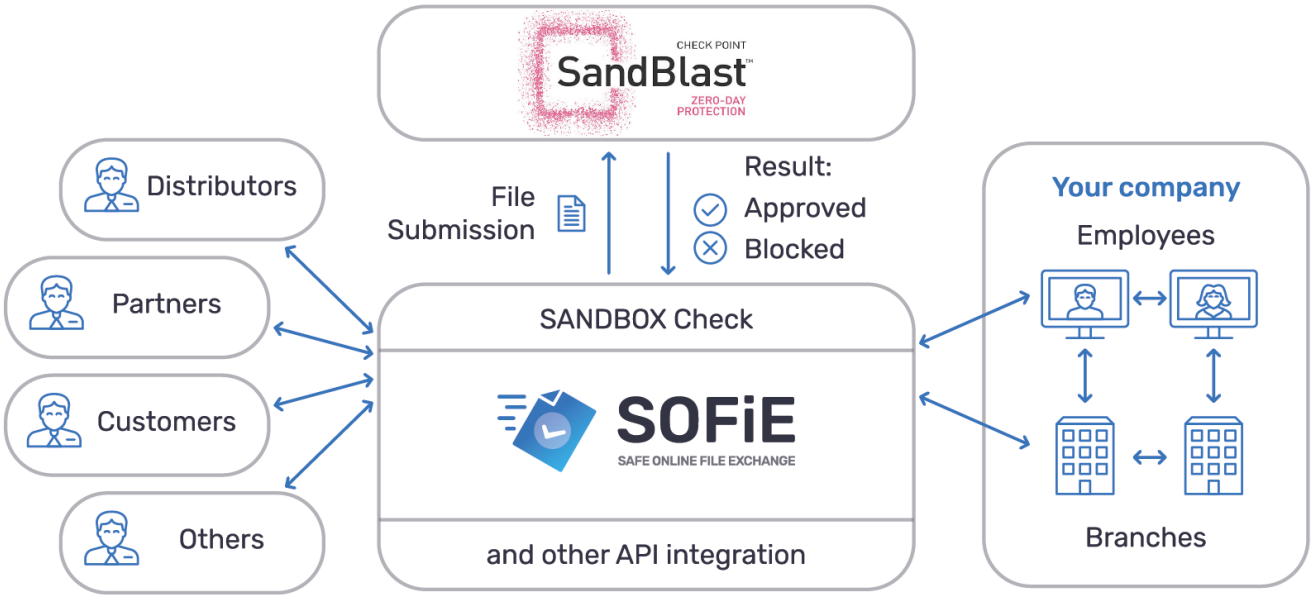
Using SOFiE with integrated SandBlast protection provides a unique security level for each organization who decides to be protected against ransomware, malware, and

zero-day attacks. You can easily receive files even from anonymous users (customers, partners, distributors etc.) by sending them an invite with URL for file upload.

## EFFECTIVE ZERO-DAY THREAT PREVENTION

The SandBlast Threat Emulation technology employs the fastest and most accurate sandboxing engine available to pre-screen files, protecting your organization from attackers before they enter your network. Every file emulation generates a detailed report including forensic information about any malicious attempts originated by running this file. The report provides actual screenshots of the simulated environments while running the file.

Inspecting files and emails for which no threat intelligence exists, SandBlast performs deep CPU-level emulation that is resistant to the most evasive attacks. It also employs OS-level inspection to examine a broad range of file types, including executables and documents, and emulates threats across PC and Mac devices, ensuring the best zero-day protection for all enterprise users. SandBlast leverages the power of data science to detect the newest threats with exhaustive AI engines and rich rule-based engines that process millions of parameters collected from runtime behaviors—reaching a single conclusive AI-generated verdict. AI heuristics are continually optimized against the latest threats unleashed to the wild.




## ABOUT SONPO

Sonpo specializes in ICT services with focus on security. Sonpo has its own team of experienced developers who take a comprehensive view of ICT security that encompasses all its complexity, analyze the weaknesses of customer's environments, systems, processes and, together with the customer, find optimal solutions that not only help increase their safety and security, but also fit into their existing environment as an integral part of it. For more information, visit www.sonpo.eu.

## ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

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 | www.checkpoint.com