Check Point SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

Accellion

Check Point + Accellion

kiteworks Secure File Sharing Platform

Accellion kiteworks and Check Point SandBlast Threat Prevention provide organizations security and continuity in their data transfer efforts to prevent the risk of infiltration by malicious software.

Product Benefits

- Flexibility to integrate security into a variety of business processes where data transfer is involved.
- Enables organizations to send and receive information securely and in compliance with internal policies and government regulations.
- Provides unified access to all content in the enterprise, whether on-prem or in the cloud.
- Enhances the utilization of secured data sources when dealing with untrusted sources.
- Simplified threat prevention over encrypted protocols such as HTTPS and SFTP.

Product Features

- Granular controls aligned with existing policies on threat reporting and quarantine.
- Detailed reporting around the source of threats and violations.
- Centralized auditing around violations.
- SSL / TLS secure communications.
- Multi-tiered on-premise and hybrid cloud secure deployment options.

INSIGHTS

As technology advancements generate more data and organizations increasingly rely on external partners to increase operational efficiencies, enterprise data transfer becomes more critical to business success. However, as more data is shared beyond enterprise borders, the risk of a data breach or other form of unauthorized access to sensitive information increases. The infiltration of ransomware or other forms of malicious software can lead to data loss, regulatory penalties, brand erosion, litigation, and other far-reaching, long-term ramifications. Therefore, the ability to transfer data securely outside the organization, while at the same time ensuring any data that enters the organization is free of malicious software, is critical to business viability.

JOINT SOLUTION

Accellion kiteworks and Check Point SandBlast work together to prevent the spread of malicious software. Leveraging an integration with Check Point SandBlast, kiteworks provides organizations an integrated governance framework over all of the content entering and leaving the organization to prevent the risk of malware infiltrating an organization's network. Granular visibility and control of content going through the kiteworks platform enables organizations to analyze and either block or simply report on any threats of malicious data.

Accellion's legacy is in securely connecting an organization's content to the people and systems that are part of critical business processes. The kiteworks secure file sharing governance platform ensures this content is shared securely and provides a detailed and centralized audit trail that demonstrates compliance with internal policies and government regulations.

Check Point SandBlast delivers advanced protection against Zero-Day attacks, implementing a set of unique technologies which detect and prevent the use of the most sophisticated evasion techniques. These include CPU-Level inspection, a Threat Extraction engine, and others.

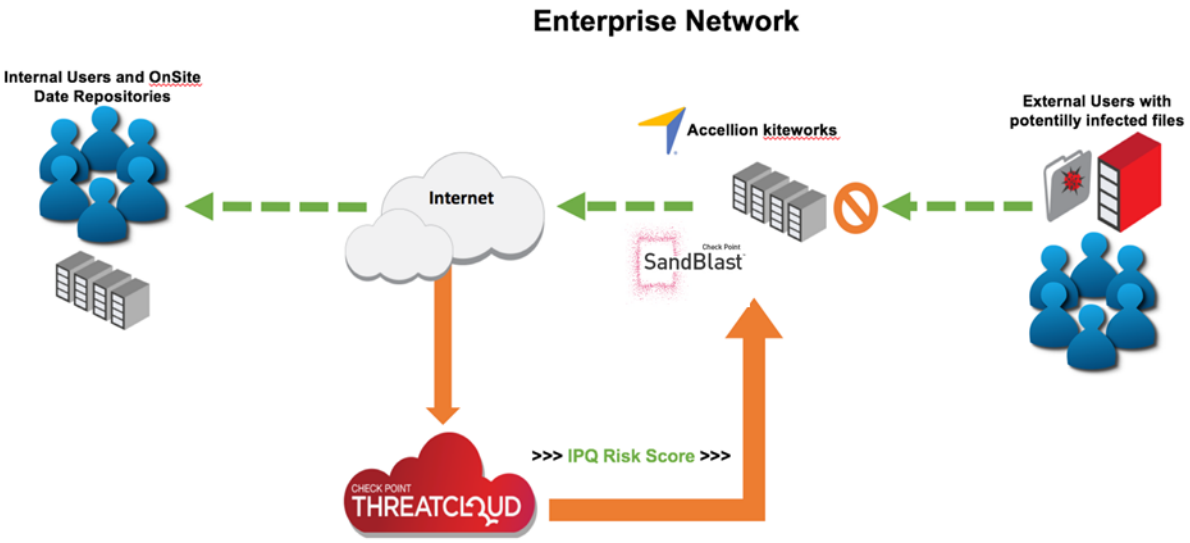
With Accellion and Check Point, all content is analyzed for malicious software, before advancing into any business operation. The joint solution stops hackers from evading detection and infiltrating an organization's network, reducing the risk of expensive breaches or downtime.

Through a simple web-based administration interface, kiteworks can be configured with minimal administrator effort to send all files into the SandBlast system for a complete security scan. All violations will be visible in both Check Point and kiteworks' logging and reporting solutions, with the ability to integrate with an organization's existing SIEM infrastructure.

In summary, kiteworks provides a secure channel for data transferred across enterprise boundaries, utilizing a variety of common protocols like SFTP, HTTPS, and simplified automation. By integrating SandBlast Threat Emulation, organizations now have the power and confidence to share content securely and mitigate the risk of a malware infection or other data loss.

A BETTER APPROACH TO SECURING BUSINESS

By leveraging an organization's existing infrastructure and policies, kiteworks and Check Point SandBlast ensures that any in-bound file will be free of malicious software, regardless of the source or target. Newly discovered threats are sent to the ThreatCloud intelligence database and each newly discovered threat signature is distributed across the ThreatCloud ecosystem to protect the kiteworks environment. The flexibility in kiteworks' platform provides organizations a secure, compliant and efficient means to send and receive information through a variety of protocols, plugins and services but not before each incoming or outgoing file is sent through the SandBlast Thread Emulation service to identify any threat of malicious code. Once scanned, a log is generated and the recipient can access the file.



ALL-INCLUSIVE SECURITY SOLUTIONS

Most file sharing solutions are limited to a specific method of transferring data from one location to another. For example, some solutions limit all file transfers to be executed via the web browser. With kiteworks, not only is the Web effectively utilized for data transfer, but native SFTP, a suite of native and embedded productivity plugs, a secure mobile application, and customizable automation agents are all included to provide maximum functionality to end users. Regardless of the protocol used to access files, the kiteworks security framework applies native and integrated layers of security and governance seamlessly, based on the policies and configurations established by the organization. All files are scanned, logged, approved or quarantined appropriately by leveraging the power of the Check Point SandBlast system to protect the organization. Because of the simplicity of the integration, administrators not only have a simple method of reporting and threat remediation, they can also provide end users an effective and flexible method for collaborating and requesting information from sources outside of the organization.

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

Capabilities:

- Ability to securely request data from outside sources:
  - An organization can immediately and safely accept files from outside, which may include untrusted sources, by utilizing the built-in request file functionality. The solutions will detect and block new or previously undiscovered threats across a wide range of file types.

- Centralized and granular audit of violations:
  - All data transferred through the platforms will be logged in a detailed, normalized and secure manner and can also be streamed to an existing SIEM solution.

- Granular security control:
  - Based on the enterprise risk policy, organizations can simply report on (rather than lock) files when malicious content has been detected.

- Simple configuration:
  - Both solutions provide simple web-based administration utilities to manage system configuration and maintenance.

- Multiple Deployment Options:
  - With flexible deployment options between hosted private cloud, hybrid cloud and on-premise, any security posture can be accommodated.

- Enable secure collaboration:
  - Administrators can safely allow end users to exchange information between internal and external users, knowing that all files found to contain malicious software will be blocked and reported.

- Added security around legacy or internal data sources:
  - SandBlast and kiteworks will enable the secure transfer of information utilizing internal systems by adding access control and threat emulation to each transaction whether the information is directed to an outside or inside target.

- Multi-tiered infrastructure compatible with secure and complex infrastructure:
  - Both kiteworks and SandBlast products work together to enable administrators to deploy into complex environments.