

CHECK POINT + FIRELAYERS EXTEND PERIMETER SECURITY

Benefits

- **EXTENDING THE PERIMETER**
Widen your circle of protection off premise to include SaaS, IaaS, and PaaS apps.
- **SECURE COLLABORATION**
Safely leverage and empower collaboration with cloud-based platforms such as Office 365, Box, DropBox, Jive, etc.
- **IDENTIFY & MONITOR FILES**
In real-time, detect malicious content in your cloud applications and mitigate risk with quarantines and alerts.
- **PREVENT MALICIOUS UPLOADS**
Intercept malicious content before it is uploaded to your cloud apps and notify administrators and users of risky behavior.
- **ENABLE BUSINESS**
Real-time user mitigations and a transparent user experience reduces false positives and ensures cloud applications remain uninterrupted.

INSIGHTS

The massive shift to cloud computing and mobile devices has radically changed the corporate IT structure. The corporate network, which once had clear perimeters has morphed into a multi-layered, virtualized and distributed network supported by third party data storage, software-as-a-service (SaaS)-based business processes and the diverse use of mobile devices.

The result: lack of control over who can access the organization's cloud applications and the data housed within, limited visibility of activity inside these applications, and a disconnect between the traditional security tools and the security needs of cloud applications. The emerging cloud-based IT structure of the extended enterprise demands a new type of protection. Your extended enterprise requires cloud application security to proactively protect cloud application access, data and usage.

EXTENDING SECURITY TO THE CLOUD

Extend protection of your data to the cloud with our Threat Emulation Service (sandboxing) combined with FireLayers. Protecting your cloud applications, FireLayers integrates context and risk factoring into your security policy and triggers mitigations to prevent data breaches.

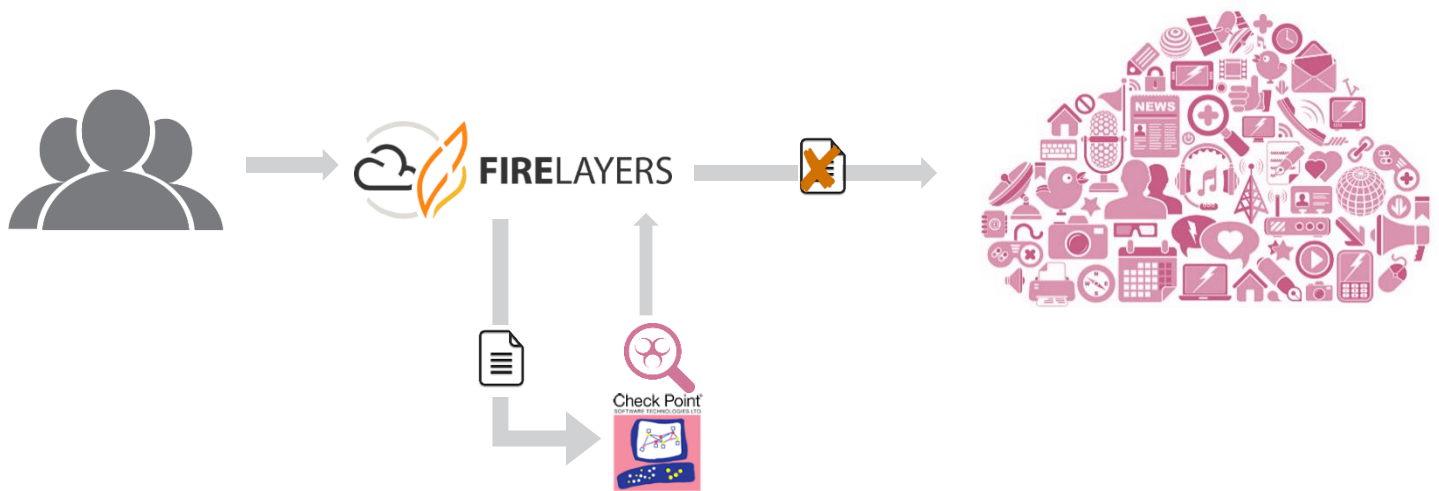
FireLayers proactively identifies file sharing related actions, in real-time, in any application. This includes homegrown applications running on Azure, AWS, and Google Cloud among other IaaS (infrastructure-as-a-service), customized applications, and off-the-shelf SaaS tools like Box, Google Apps, Office 365, and ServiceNow.

After intercepting files in transit or resting in document repositories, FireLayers delivers them to our Threat Emulation for inspection on premise or in the cloud. Threat Emulation inspects the file, evaluating if the content is malicious or not. It then informs FireLayers of its analysis, triggering the following mitigations as needed: blocking, quarantine, admin alerts, user notifications, or a combination of these actions.

STOP THE SPREAD OF MALWARE - APPLY MITIGATIONS AT THE SECURITY DECISION POINT

Hackers are targeting your company with sophisticated malware that cannot be detected with traditional solutions. A sandbox can catch new or well-hidden threats. Get immediate protection from zero-day threats when you deploy the Check Point and FireLayers integrated solution.

- We first scan all file repositories in the cloud to identify and detect any malware infected files. Depending upon our verdict, FireLayers enforces security policies to mitigate risk.
- Protecting you from active threats, we continuously evaluate all files as they are used. This includes malicious file uploads, shared file downloads, opening infected files, and more.



Check Point + FireLayers Perimeter Extension Solution in Action

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (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 FIRELAYERS

FireLayers (www.firelayers.com) enables the responsible adoption of cloud apps, while ensuring security, compliance and governance of any cloud application on any device by any user. The FireLayers Secure Cloud Application Platform delivers full control over homegrown and popular apps like Salesforce, Office365, SuccessFactors, NetSuite and endless others. With our Secure Cloud Application Platform, enterprises gain new levels of security, visibility and control across their cloud resources. FireLayers provides the granular control IT teams need to create safe zones for productive work while protecting enterprise data, networks and financial transactions from malicious attackers, external threats and accidental risky employee behavior.

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