Check Point SOFTWARE TECHNOLOGIES LTD.

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT CLOUDGUARD SAAS

MORE THAN JUST A CASB

Superior Threat Prevention for SaaS apps & Cloud Email

Protect data by stopping enterprise-targeted attacks on SaaS applications

Product Benefits

- 'Most Effective Breach Prevention' for malware and zero-days (NSS Labs)
- Blocks account takeovers wherever they happen, with unpassable Identity Protection
- Catches more phishing attacks, leveraging artificial intelligence
- API architecture enables seamless integration with SaaS applications and instant threats visibility

Product Features

- Delivered as a cloud service
- Zero-Day Threat Protection
- Phishing Protection
- Identity Protection
- Data Leakage Prevention
- SaaS Shadow IT Discovery
- Intuitive Cloud Management
- Deployed within minutes

Learn More

https://www.checkpoint.com/products/saas-security/

TRUE STORY

Customers of a North American financial services company received emails from the company's chief financial officer directing them to use a new bank account for money transfers. As it turns out, the emails were sent by hackers who stole the CFO's Office365 account credentials, accessed it, and sent the emails in his name. More than $2 million was transferred to foreign accounts before the exploit was discovered.

Organizations seeking to optimize business operations and reduce costs increasingly move to cloud applications and software-as-a-service (SaaS) products.

SAAS SECURITY CHALLENGES

While SaaS applications help increase business agility, they also challenge traditional security approaches. SaaS apps are:

- **Exposed**: SaaS applications merely require an internet connection to be accessed from any device, location, and user
- **Provided as an external service**: SaaS applications cannot embed existing security controls and provide risk visibility as needed
- **Equipped with minimal built-in security**: Frequently, SaaS applications only have minimal default security that allows unrestricted file sharing and malware delivery

ENTERPRISES ARE TARGETED WHEN USING SAAS

Security breaches on SaaS are increasingly common and get media coverage. To answer this, most security solutions offer data leakage protection and application control. However, 90% of SaaS data breaches occur from targeted attacks, with 50% of the breaches happening through account takeovers of employee SaaS accounts.* Hacking into SaaS applications and taking over employee SaaS accounts has become a preferred method to steal company data, money, and interfere with business processes. Securing data effectively in SaaS applications is a cybersecurity must-have.

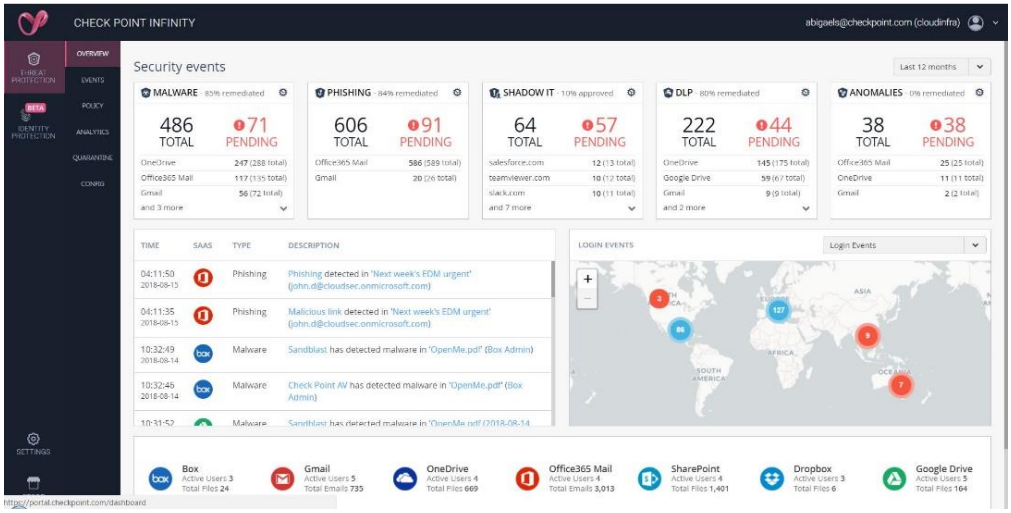
CLOUDGUARD SAAS – ELIMINATE REAL SAAS THREATS

To protect from SaaS threats, Check Point offers CloudGuard SaaS – a cloud service that prevents attacks on enterprises using SaaS applications:

- ✓ Prevents malware and zero-day threats from attacking SaaS users
- ✓ Stops sophisticated phishing attacks on Office365 and Gmail accounts
- ✓ Eliminates the top SaaS threat by blocking account hijacks
- ✓ Provides instant visibility into unauthorized SaaS activity
- ✓ Protects shared files and sensitive business data

* Check Point Incident Response team, 2017

Office 365 G Suite salesforce servicenow slack EGNYTE box Dropbox ShareFile



MOST EFFECTIVE BREACH PREVENTION FOR MALWARE AND ZERO-DAYS

CloudGuard SaaS prevents malware and zero-day threats from attacking SaaS users. Utilizing Check Point's industry leading SandBlast technology, it protects Office365 and Gmail attachments, as well as in-app file sharing and web downloads on Box, OneDrive, and others. SandBlast technology, recognized by NSS Labs as 'most effective in breach prevention', with 100% block rate and highest score in evasion testing, provides a multi-layered protection for SaaS users. CloudGuard SaaS leverages CPU-level threat emulation to scan and quarantine zero-days on email attachments, shared files, and web downloads, extracting threats to deliver safe files in seconds.

BLOCKS ACCOUNT TAKEOVERS, WHEREVER THEY MAY HAPPEN

CloudGuard SaaS eliminates the primary threat to SaaS usage: employee account takeovers. Its Identity Protection feature blocks unauthorized user access, and logins from compromised devices. CloudGuard SaaS Identity Protection uses comprehensive SaaS intelligence by thoroughly monitoring and detecting suspicious user activities and SaaS configurations. In addition, CloudGuard SaaS pairs and verifies users and devices using ID-Guard™ technology, and guarantees that compromised PCs or mobile devices will not be able to access your SaaS. Only CloudGuard SaaS blocks account takeovers anywhere they happen, using this centralized, hassle-free, multi-factor authentication.

STOPS SOPHISTICATED PHISHING ATTACKS

CloudGuard SaaS detects and blocks phishing, spear phishing, email spoofing, and further clever phishing attacks that manage to bypass other products. It utilizes artificial intelligence to detect malicious content on Office365 and Gmail, and advanced URL filtering to identify dangerous email sources. Its artificial intelligence engines digest hundreds of indicators like language & text, and email meta-data to provide high-precision verdicts and block malicious content on SaaS email accounts. As a result, CloudGuard SaaS has a higher catch-rate than any other solution, spotting sophisticated techniques like split URLs, hidden words insertion, and phishing links hosting on Microsoft SharePoint.

INSTANT THREAT VISIBILITY, DATA CONTROL & PROTECTION

CloudGuard SaaS is a cloud service with a cloud-to-cloud API architecture. This allows it to provide instant visibility into unauthorized SaaS activity, and data control and protection. It allows IT teams to easily identify unsanctioned SaaS applications in use, and prevents data leakage by blocking sharing of sensitive data and leveraging 800 recognized data types. Deploy CloudGuard SaaS seamlessly and centralize monitoring via an intuitive web portal.

SUMMARY

Check Point CloudGuard SaaS in more than just a CASB. It provides complete protections against enterprise-targeted attacks like zero-days, phishing, and account takeovers, addressing real SaaS threats, and preventing breaches on SaaS applications.

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; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com