Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURING SAAS APPLICATIONS WITH CHECK POINT CLOUDGUARD SAAS

Office 365 G Suite salesforce servicenow slack EGNYTE box Dropbox citrix ShareFile

CLOUDGUARD SAAS – SAAS SECURITY IS ONE CLICK AWAY

The only security solution to prevent attacks on SaaS applications

Features & Benefits

Identity Protection - Prevent Account Takeovers with ID-Guard technology

CloudGuard SaaS uses ID-Guard patent pending technology to prevent unauthorized users and compromised devices from accessing your SaaS app. It intercepts them using CloudGuard SaaS' risk cloud and user behavior engine that feed-off of sources like: mobile and PC on-device detection of OS exploits, malware, and network attacks, APIs, and Check Point's Threat Cloud.

Zero-Day Threats Protection

CloudGuard SaaS prevents malware and zero-day threats from getting into SaaS apps. It prevents phishing attacks on Office365 and Gmail; protects in-app file sharing; quarantines malicious emails and files; and provides a multi-layered protection.

Data Protection

CloudGuard SaaS detects sensitive data sharing via SaaS and immediately limits data exposure. This can be done with a built-in DLP engine or by integrating with existing DLP engines.

End-to-End SaaS Security Coverage

CloudGuard SaaS enables consistent policies between mobile, cloud and even gateways and unifies management across the board.

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

Customers of a North American financial services company received emails from the company's accounting directing them to use a new bank account for money transfers. The email was sent by hackers who managed to access an employee's compromised account, steal his credentials, and log in to his Office365 account. More than $2 million was transferred to foreign accounts before it was discovered.

Organizations seeking to optimize business operations and drastically reduce cost increasingly have moved to cloud applications and software-as-a-service (SaaS) products. Gartner maintains 70% of the organizations already use cloud applications. (*Gartner, 2016*)

SAAS SECURITY CHALLENGES

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

- **Exposed**: SaaS apps can be accessed from any device, in any location, and by anyone; they merely require an internet connection for that
- **Provided as external service**: SaaS apps cannot embed existing security controls and provide risk visibility as needed
- **Provided with insufficient default security**: At best, SaaS apps are provided with default security that allows unrestricted file sharing and malware delivery

SAAS APPLICATIONS ARE BREACHED

SaaS security breaches are becoming increasingly common and get media coverage. To answer this, most security solutions offer data leakage protection and application control, but it is found that **90% of SaaS breaches occur due to external threats**. Specifically, **50% of the breaches happen through an illegitimate takeover of employee SaaS accounts by hackers**. Hacking into SaaS applications and takeover of employee SaaS accounts has become prevalent to steal company data, money, and interfere with business processes.

CLOUDGUARD SAAS - SAAS SECURITY IS ONE CLICK AWAY

To protect from SaaS threats, Check Point offers CloudGuard SaaS – a new cloud service that prevents attacks on enterprise SaaS applications, within minutes' deployment.

- ✓ Prevent malware and zero-day threats from getting into SaaS apps
- ✓ Blocks cybercriminals from taking over employee SaaS accounts with ID-Guard technology
- ✓ Keeps data protected by blocking sensitive data sharing and forcing its encryption
- ✓ Provides full security coverage with synced policies and unified management across gateways, endpoints, and cloud