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 company discovered.

Organizations seeking to optimize business operations and reduce costs increasingly move 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 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 prevalent 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 enterprise-targeted attacks on SaaS applications:

- Prevents malware and zero-day threats from attacking SaaS users
- Stops sophisticated phishing attacks on Office365 and Gmail email accounts
- Eliminates the #1 SaaS threat by blocking account takeovers where others can’t
- Provides instant visibility into unauthorized SaaS activity, data protection for shared files, and intuitive management

* Check Point Incident Response team, 2017
MOST EFFECTIVE BREACH PREVENTION FOR MALWARE AND 0-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 messaging on Box, OneDrive, Slack, Salesforce, 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 its CPU-level Threat Emulation to scan and quarantine zero-days on email attachments, shared files, and messages, and delivers users safe files through Threat Extraction, enabling user productivity.

BLOCKS ACCOUNT TAKEOVERS, WHERE OTHER SOLUTIONS CANNOT
CloudGuard SaaS eliminates the #1 threat to SaaS usage: employee account takeovers. Its Identity Protection feature blocks unauthorized user access, and importantly, logins from infected devices. CloudGuard SaaS Identity Protection ensures comprehensive SaaS intelligence all across the organization and in SaaS, by thoroughly monitoring and detecting suspicious user activities and SaaS configurations. In addition, pairing users to devices and leveraging ID-Guard™ machine-learning technology, CloudGuard SaaS guarantees that even when devices and users are matched, compromised PCs or mobile devices will not be able to access your SaaS. This centralized, hassle-free, multi-factor authentication allows CloudGuard SaaS to stop account takeovers where other solutions cannot, because they lack critical threat indicators.

STOPS SOPHISTICATED PHISHING ATTACKS
Cloud Guard 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 verdict and block malicious content on SaaS email accounts. This means CloudGuard SaaS has a higher catch-rate and less false positives than any other major market vendor, spotting tricky techniques like split URLs, hidden words insertion, and hosting phishing links on SharePoint.

INSTANT DATA VISIBILITY, CONTROL, AND PROTECTION
CloudGuard SaaS is a cloud service with a cloud-to-cloud architecture based on APIs. This allows it to provide instant visibility into unauthorized SaaS activity, and immediate data control and protection. It offers Shadow IT Discovery that easily identifies unsanctioned SaaS applications in use, Data Leakage Prevention that blocks sharing of sensitive data, leveraging 800 data types, and an intuitive Cloud Management that allows seamless deployment (scanning even historic threats), as well as centralized monitoring via a 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.