Complete Protection for Cloud Email & Productivity Suites

MAIN BENEFITS:

Complete protection - all the email & productivity suite security you need

Bulletproof security – we catch what everyone else misses

Best TCO - a single, efficient and cost-effective solution for email and productivity suites

MAIN CAPABILITIES:

Anti-Phishing: block the most sophisticated phishing attacks such as impersonation and Business Email Compromise (BEC)

Malware protection: thwart evasive malware and provide sanitized files within seconds

Prevent data leak: set custom policies to keep data safe and maintain compliance

Prevent Account Takeover: block suspicious logins using patent-pending technology

SECURE OFFICE 365 & G SUITE APPLICATIONS:

CLOUD MAILBOXES ARE YOUR WEAKEST LINK

Over 90% of attacks against organizations start from a malicious email. Since email attacks usually involve the human factor, your Office 365 and G Suite environments are your organization's weakest link. Closing this security gap requires protections from various threat vectors: phishing, malware, data theft and account-takeover. This might force you to choose between the security level your need to what you can actually afford and efficiently manage.

SO WHAT TYPE OF DAMAGE CAN A MALICIOUS EMAIL DO?
One small example includes a 2019 attack on a Toyota parts supplier where attackers convinced the accounts payable team to *electronically transfer $37M to the criminals' account.*

CLOUDGUARD SAAS

Cloud Email and Productivity Suite Security Solution

With CloudGuard SaaS you get all the protections you need for Office 365 and G Suite apps in a single, efficient and cost effective solution, and at the highest-caliber security.

The solution's main capabilities:

• Block sophisticated social engineering attacks such as zero-day phishing, impersonation, and BEC using AI-trained engines

• Block malicious attachments before they reach users' mailboxes, without impacting business productivity (instantly delivers sanitized files to users)

• Protect sensitive business data and maintain regulatory compliance with advanced data loss prevention (DLP)

• Prevent sophisticated account takeover attacks by augmenting authentication processes with patent-pending technology

HOW IT WORKS

All the email & productivity suite security you need

a. Block sophisticated social engineering attacks such as impersonation, zero-day phishing and Business Email Compromise (BEC) using AI-trained engines

Built-in security is not enough to stop advanced phishing attacks such as BEC that combine vulnerabilities and social engineering to deceive and manipulate end-users. CloudGuard SaaS deploys as the last line of defense and secures inbound, outbound, and internal emails from phishing attacks that evade platform-provided solutions and Email Gateways. The solution inspects the communication's metadata, attachments, links and body, as well as all historical communications, in order to determine prior trust relations between the sender and receiver, increasing the likelihood of identifying user impersonation or fraudulent messages. It also inspects internal communication in real time in order to prevent lateral attacks.

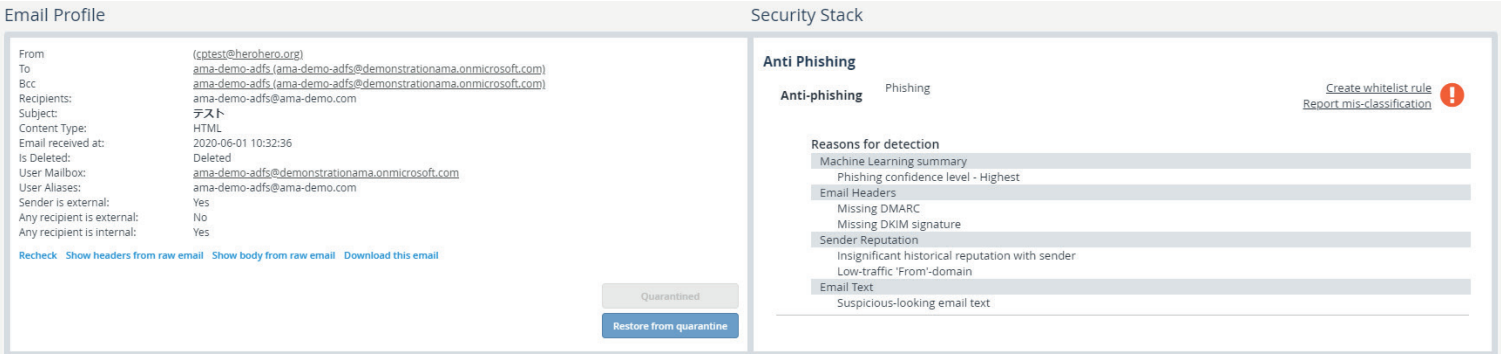

Figure 1: Phishing email drill-down view

b. Block malicious attachments before they reach users' mailboxes, without impacting business productivity

CloudGuard SaaS uses Check Point's SandBlast technology, recognized by the NSS Labs as 'most effective in breach prevention'*, and includes:

- Threat emulation - evasion-resistant CPU-level sandbox that blocks first-time seen malware and keeps you protected from the most advanced cyber threats
- Proactive Threat Extraction – cleans files and eliminates potential threats to promptly deliver a safe file version to users in under 2 seconds

Threat Extraction maintains uninterrupted business flow, while the sandbox continues in the background. Threat Extraction eliminates unacceptable delays created by traditional threat emulation, while instantly cleaning files of any active content, with the industry's only fully integrated document and image sanitization solution.

**NSS Labs report: https://www.nsslabs.com/tested-technologies/advanced-endpoint-protection/*

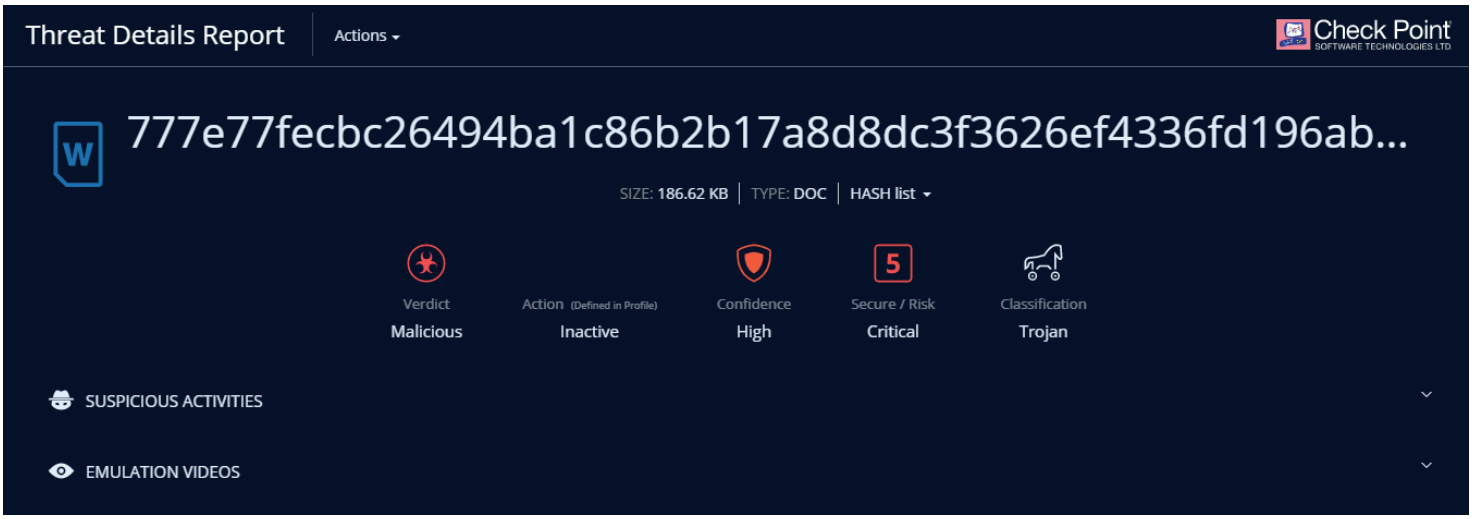

Figure 2: Threat Emulation report

The technology eliminates risks from all communications within your organization, as well as vetting all aspects of email messages before they enter your users' mailbox, including emails with attachments, links, sender and recipient details and its body. To this end, CloudGuard SaaS evaluates over 300 parameters per email with multiple innovative technologies and rule-based engines, which include Natural Language Processing (NLP), Threat Emulation, AI-based phishing protection, AI-based fraud protection, URL reputation and Click-Time Protection (also called URL Rewriting) which analyzes and blocks malicious links in real time, as they are clicked.

c. Protect sensitive business data and maintain regulatory compliance with advanced data leak prevention (DLP)

CloudGuard SaaS detects sensitive data sharing via email and other productivity applications and immediately limits data exposure. It enables you to enforce a data leakage policy based on your company needs, with hundreds of predefined and custom data types.

When an employee shares data through their email or other productivity suite applications, CloudGuard SaaS examines it. The email subject, body, and attachments are scanned, and in an event of sensitive data sharing such as credit card details or competitive information, the communication is blocked or "unshared" to prevent data leaks.

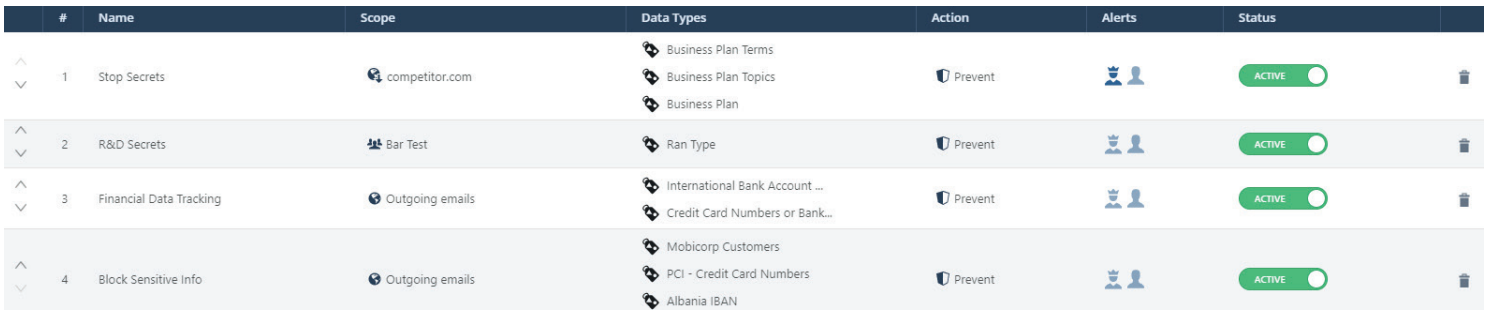

Figure 3: DLP policies

d. Prevent advanced account takeover attacks by augmenting authentication processes

CloudGuard SaaS uses a patent-pending technology to prevent unauthorized users and compromised devices from accessing your cloud email or productivity suite applications, thus mitigating the risk of an account takeover attack. CloudGuard SaaS intercepts attackers using machine-learning algorithms, which analyze user behavior and feed off sources like mobile and endpoint on-device detection of OS exploits, malware and network attacks, SaaS native APIs, and Check Point's ThreatCloud.

CloudGuard SaaS provides additional data into the identity provider's authentication process, so suspicious logins (e.g.: seen in two different locations, bad IP reputation) are immediately denied and blocked. CloudGuard SaaS Identity Protection is transparent to users and does not require their involvement.

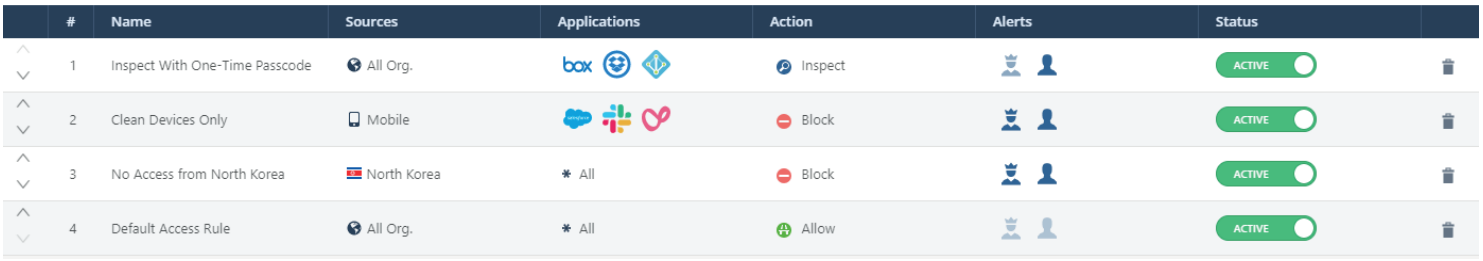

Figure 4: Identity Protection policies

CloudGuard SaaS Identity Protection works in two modes – agent and agentless:

- **Agent mode** offers an endpoint agent on company and personal desktops, laptops, and mobile devices, and secures logins deterministically.
- **Agentless mode** allows CloudGuard SaaS to instantly work across all your organization, without the need to deploy endpoint agents. Besides allowing two-factor authentication through SMS; network, location, or device type are used as basic but efficient controls. This mode leverages Check Point ThreatCloud, the market leading threat intelligence database.

Bulletproof security – catches what everyone else misses

a. Part of Check Point Infinity, a consolidated security architecture, and powered by the world's most powerful threat intelligence

CloudGuard SaaS is a part of a consolidated security architecture that delivers consistent security across networks, clouds, endpoints, mobile devices, and IoT; powered by ThreatCloud, the world's largest threat intelligence engine. ThreatCloud monitors a third of the world's internet and is constantly updated with new threat information from a worldwide network of sensors, third party feeds, Check Point threat researchers, and Check Point connected gateways.

THREATCLOUD STATISTICS:

86 Billion Transactions a day	4 Million Emulated files a day	100,000 Connected networks	8,300 Zero-day files blocked a day

b. The only email security solution tested and proven to have the industry's best malware catch rate (99.91%) by the NSS labs

CloudGuard SaaS leverages the SandBlast technology, recognized by NSS Labs as 'most effective in breach prevention', with 100% block rate and the highest score in evasion testing - providing a multi-layered protection for SaaS users.

c. Inline API-based protection for inbound, outbound and internal email communication

API-based integration allows CloudGuard SaaS to not just scan inbound emails but also outbound and internal communication in real time to prevent lateral attacks within the organization and data leakage. In addition, its architecture does not require any MX record changes that expose the solution to hackers, making it invisible. CloudGuard SaaS deploys as the last line of defense and uses Artificial Intelligence (AI) to train on what the built-in security misses, thus providing multi-layered defense. AI and Indicators of Compromise (IoCs) used in the past train the CloudGuard SaaS platform for what to look for in complex zero-day phishing attacks, providing a 30% better catch rate than built-in security.

Lowest TCO

a. A single license for both email and productivity apps with all security functionality included

CloudGuard SaaS provides all security functionality for both cloud email and productivity applications like OneDrive, SharePoint and Google Drive in a single license, alleviating purchasing and management overhead and providing organizations with an all-encompassing solution in a one-stop-shop, reducing overall TCO.

b. Monitor one simple dashboard with actionable insights and reporting

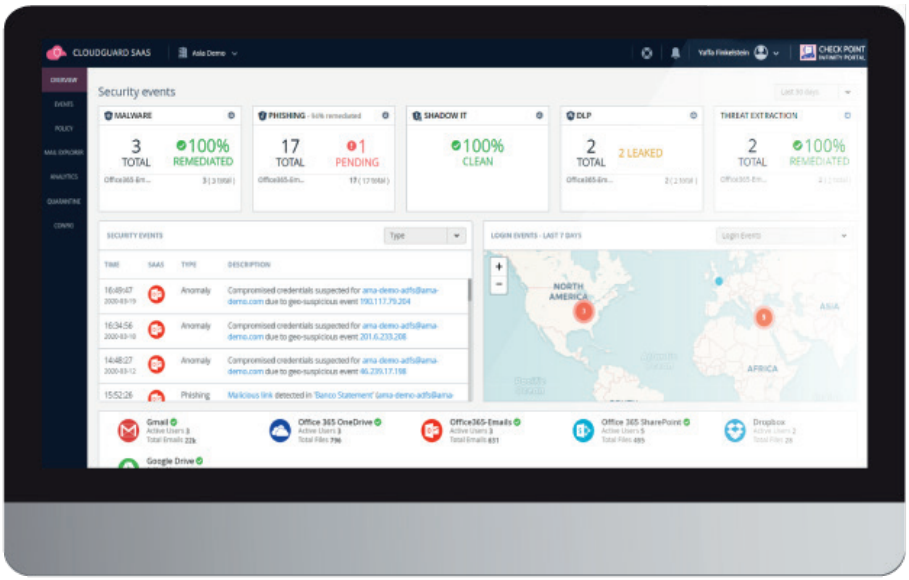

Figure 5: CloudGuard SaaS Dashboard

CloudGuard SaaS provides granular visibility into security events, all from one simple dashboard for all security functionality. By providing actionable insights and reporting, it reduces management overhead and improves productivity.

Granular visibility into attacks

See every threat caught by CloudGuard SaaS including the email subject, content, and why it was determined to be phishing, based on the 300+ indicators the solution looks at in every email. Phishing indicators are explained in plain English, so it is easy to assess the potential impact of an attack.

c. Deploy instantly and see results within hours, including retroactive scanning for existing malicious emails

CloudGuard SaaS's auto-deployment is a 3-step process that takes minutes, and enables security admins to deploy instantly and fine-tune policies to start catching malicious activity within a couple of hours. When it is deployed, CloudGuard SaaS does a retroactive scan to find existing threats in your organization to ensure maximal security posture from the get-go.

SUMMARY

Email is the first link in a chain of attacks, and with the rise of remote work, the use of cloud mailboxes and productivity applications increases exponentially. CloudGuard SaaS provides organizations with complete protecting that is constantly adapting and evolving to the ever-changing threat landscape, while providing security admins with an easy-to -deploy and manage platform, lowering TCO and strengthening security posture.

INFO EXCHANGE

AUTHORIZED PARTNER
JAMAICA

To get started with Checkpoint's CloudGuard Solution, email the Info Exchange team at **mybusiness@infoexchangeja.com** or give us a call at **(876) 931-9552**

CHECK POINT
CloudGuard™
SaaS