CHECK POINT SANDBLAST MOBILE

WITH ON-DEVICE NETWORK PROTECTION

AT A GLANCE

ON-DEVICE NETWORK PROTECTION

On-device Network Protection is a new and fundamentally unique mobile security infrastructure that allows businesses to stay ahead of new and emerging Gen V threats.

Protection Methodology
- All traffic inspected locally on the device
- Cellular traffic data is not routed through an external gateway or proxy
- Checks for threats against ThreatCloud, the world's largest security intelligence database
- Negligible impact on latency
- Negligible impact on battery

Privacy
- No PII inspected on device
- No PII sent to external gateway or proxy
- Configurable option to allow user to disable inspection for specific categories

Phishing Protection
- Blocks access to phishing sites on browser apps
- Blocks access to phishing sites on all non-browser specific apps (Facebook Messenger, Slack, WhatsApp)
- Blocks access to known and unknown phishing sites

Malicious Site Protection
- Blocks access to malicious sites on all browsers
- Types of malicious sites that are blocked (i.e. only botnets or spyware) can be defined

Conditional Access
- Blocks access to company resources if device is at risk
- Blocks access to cloud apps
- Blocks access to on-premise apps

Anti-Bot
- Blocks communications between malware and command and control servers
- Blocks all communications by malware

URL Filtering
- Over 60 site-based URL categories (e.g. gambling, adult, violence, etc.)
- Blocks access to restricted sites on all browsers and non-browser apps
- Extend policies from endpoints to mobile

THE MOBILE WORLD IS CHANGING

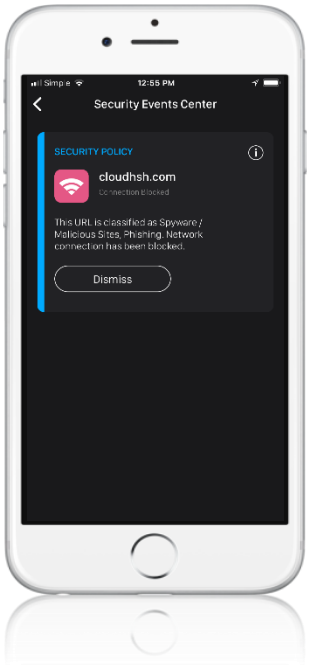
Ninety percent of all cyberattacks begin with a phishing campaign.[1] So it's no surprise that threat actors exploit enterprise mobility's multiple unprotected phishing channels: private and corporate email, SMS, and a host of messaging apps like Slack, Facebook Messenger, WhatsApp and many others. Preventing mobile phishing attacks was one of the most challenging technological problems to solve until now. SandBlast Mobile with On-device Network Protection prevents mobile phishing attacks, while identifying all malicious network traffic to and from the device.

OVERVIEW: SANDBLAST MOBILE WITH ON-DEVICE NETWORK PROTECTION

SandBlast Mobile's unique security infrastructure – **On-device Network Protection** – allows businesses to stay ahead of new and emerging Gen V threats by extending Check Point's industry-leading network security capabilities to mobile devices. The SandBlast Mobile application constantly validates cellular traffic on the device itself without routing the data through a corporate gateway. This ensures user and data privacy and allows for a seamless browsing experience.

ANTI-PHISHING

SandBlast Mobile's On-device Network Protection prevents phishing attacks on any email or messaging app by instantly detecting and blocking malicious URLs sent to the device. The Anti-Phishing capability is powered by ThreatCloud™, the industry's largest collaborative network and knowledge base that delivers real-time, dynamic security intelligence. This feature also leverages Check Point's Zero-Phishing[2] technology, which uses dynamic analysis and advanced heuristics to identify and prevent access to new and unknown phishing sites that target user credentials through web browsers in real-time.



SAFE BROWSING

SandBlast Mobile prevents access to malicious websites on any browsing app by blocking access to the sites based on the dynamic security intelligence provided by ThreatCloud™. In addition, it also prevents users from unwittingly visiting malicious websites where their device can be infected with drive-by malware.

[1] 2018 Data Breach Investigations Report
[2] Available Q3 2018

July 22, 2018

SANDBLAST MOBILE WITH *ON-DEVICE NETWORK PROTECTION*

Check Point SandBlast Mobile is an innovative approach to mobile security that detects and blocks attacks on iOS and Android mobile devices before they start.

Product Benefits

- Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, in the network, and delivers the industry's highest threat catch rate
- Keeps business assets and sensitive data on devices safe from cyber attacks

Product Features

Advanced app analysis

Runs apps downloaded to mobile devices in a virtual, cloud-based environment to analyze behavior then approves or flags them as malicious.

Network-based attacks

Detects malicious network behavior and automatically disables suspicious networks to help keep mobile devices and data safe. On-device network protection, inspects and controls network traffic to and from the device, blocking phishing attacks on all apps and browsers, and communications with malicious command and control servers.

Device vulnerability assessments

Analyzes devices to uncover vulnerabilities that cyber criminals exploit to attack mobile devices and steal valuable, sensitive information.

CONDITIONAL ACCESS

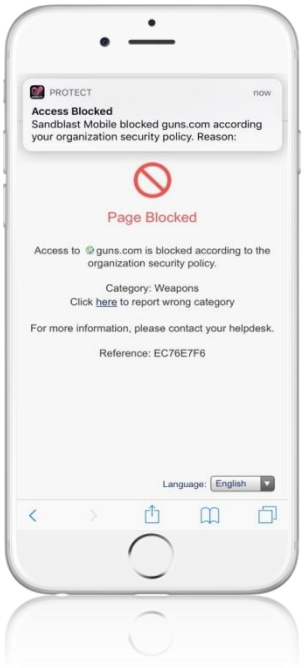
When a compromised device accesses corporate resources, data is immediately at risk. The Conditional Access feature allows an organization to automatically restrict access to corporate resources by compromised devices. As a result, if a device is exposed to an attack, access to corporate networks or any on-premise and cloud apps will be controlled. The enforcement of this policy is independent of Unified Endpoint Management (UEM) solutions.

ANTI-BOT

This feature extends Check Point's Anti-Bot technology to mobile devices. By detecting bot-infected devices and automatically blocking all communication to command and control (C&C) servers and other malicious servers, organizations can prevent exfiltration of sensitive data.

URL FILTERING

The URL Filtering feature prevents access to websites deemed inappropriate by an organization's corporate policies. SandBlast Mobile's URL Filtering technology allows businesses to blacklist and whitelist websites in granular detail based on URLs, domains, hostnames and IP addresses. URL Filtering enforces polices on mobile devices across all browser apps and on all non-browser specific apps, such as Facebook Messenger, Slack, WhatsApp and others.



THREATCLOUD

ThreatCloud is the first and largest collaborative network to fight cybercrime. It is a knowledge base that delivers real-time, dynamic security intelligence. That intelligence is used to identify emerging outbreaks and threat trends. ThreatCloud powers the Anti-Phishing, Safe Browsing and URL Filtering technologies for SandBlast Mobile, by investigating malicious IP, URL, and DNS addresses. ThreatCloud's knowledge base is dynamically updated daily using feeds from a network of more than 100,000 security gateways and 100 million endpoints worldwide, Check Point research labs, and the industry's best threat intelligence feeds.

USER PRIVACY AND DEVICE PERFORMANCE

End-user privacy is critical, so SandBlast Mobile never analyzes files, browser histories, or application data. The solution uses metadata from operating systems, apps, and networks to determine if a device is compromised. It anonymizes the data it uses for analysis to keep it and security intelligence information separated. App analysis is performed in the cloud to avoid impacting device performance. Since device protection runs automatically in the background, SandBlast Mobile delivers a user experience that is both elegant and unobtrusive.

Learn more
checkpoint.com/mobilesecurity

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