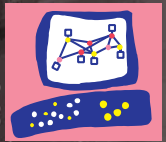


# PROTECT YOUR ENTERPRISE FROM THE NEXT SECURITY BREACH: MOBILE DEVICES

WITH CHECK POINT  
SAND BLAST MOBILE



**Check Point®**  
SOFTWARE TECHNOLOGIES LTD

**PharmaKera**

A global healthcare company  
providing medical solutions

CEO: "Our supplier claims we  
didn't pay them for the last two  
orders, a total of \$520,000!"

CFO: "Yes we did, we transferred the  
money to their new bank account"

CEO: "Their new what?!"



# THE WHALE SCAM

Hackers learn about the relationship with the supplier

Money transferred to the hackers' bank account



1 MONTH EARLIER

Purchasing manager's 8 year old son downloaded a malicious app to his dad's BYOD mobile device



USER

PASSWORD

App was infected and contained corporate email credentials



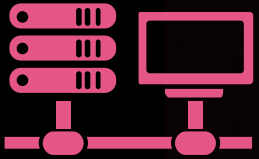
Sent mail asking to transfer the money to a new bank account, controlled by the hacker

Compromised business email accounts have cost companies more than \$2.3 billion in losses over the past three years

source: [www.fbi.gov](http://www.fbi.gov)



# THE HACKERS CAN:



Access  
corporate file  
servers



Infect corporate  
computers by sending  
internal malicious emails



Access the data center  
after obtaining VPN  
credentials from  
corporate helpdesk



# PUBLIC COMPANY'S STOCK PRICES SUDDENLY DROP

CASE II



\*a fictitious story inspired by actual cases

# 3 WEEKS EARLIER...

Hackers tapped into the CFO's device



CFO downloaded a malicious conference app by scanning a QR code



Hackers recorded the quarterly results discussed at a board meeting before the public announcement



# MOBILE IS MORE VULNERABLE AND LESS PROTECTED THAN PCs





MOBILE IS THE  
NEW WINDOW  
INTO CORPORATE  
NETWORKS







80%

of organizations already  
**ADOPTED  
BYOD**  
programs or plan  
to adopt in the  
next 12 months



HOW DO YOU PROTECT  
YOUR NETWORK FROM  
MOBILE THREATS?



# HOW MOBILE DEVICES ARE INFECTED?



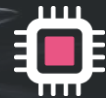
# MOBILE'S UNIQUE ATTACK VECTORS



Infected Apps



Network Attacks



OS Exploits



SMS Phishing (Smishing)



# DAMAGES

Breaking into  
corporate network

Tracking  
location

Stealing  
email

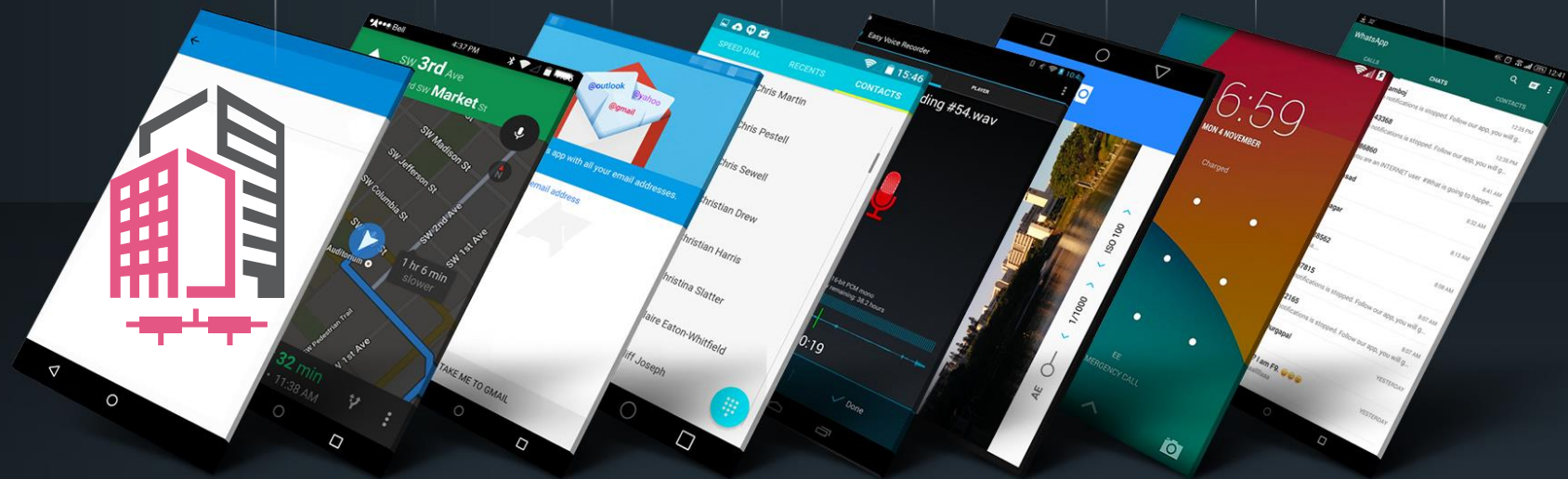
Stealing  
contact lists

Microphone  
recordings

Taking  
photos

Stealing  
passwords

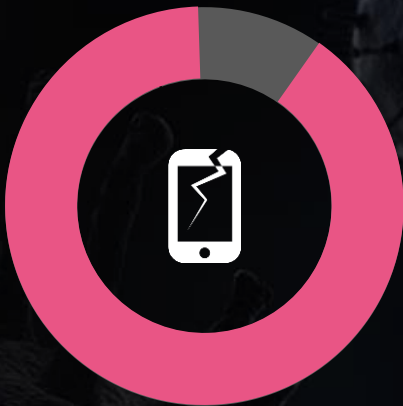
Intercepting  
text messages



**100%**  
OF ALL  
ORGANIZATIONS  
ARE INFECTED WITH  
MOBILE MALWARE

**74%**

Averaged 35  
jailbroken or  
rooted devices



**89%**

Experienced a  
man-in-the-middle  
attack over Wi-Fi



UNIQUE CHALLENGES  
REQUIRE  
UNIQUE SOLUTIONS





# MOBILE THREAT PREVENTION

## ZERO DAY PROTECTION FOR MOBILE DEVICES



# MOBILE THREAT PREVENTION

Advanced threat detection and mitigation

- Best mobile threat catch rate

- Full visibility

- Simple deployment



# HOW IT WORKS

## APP ANALYSIS (INFECTED APPS)

## ON DEVICE DETECTION

# CLOUD-BASED BEHAVIORAL RISK ENGINE

# REAL-TIME INTELLIGENCE, MONITORING AND CONTROL





# THE CHECK POINT ADVANTAGE

# THREATCLOUD

The world's largest  
IoC database



Daily inputs from traffic across 100K  
security gateways world wide

500,000,000+  
Malicious file hashes  
and sites

250,000,000  
C & C addresses

11,000,000  
Malware behavioral  
signatures



# SIMPLE TO DEPLOY

Cloud base SaaS solution



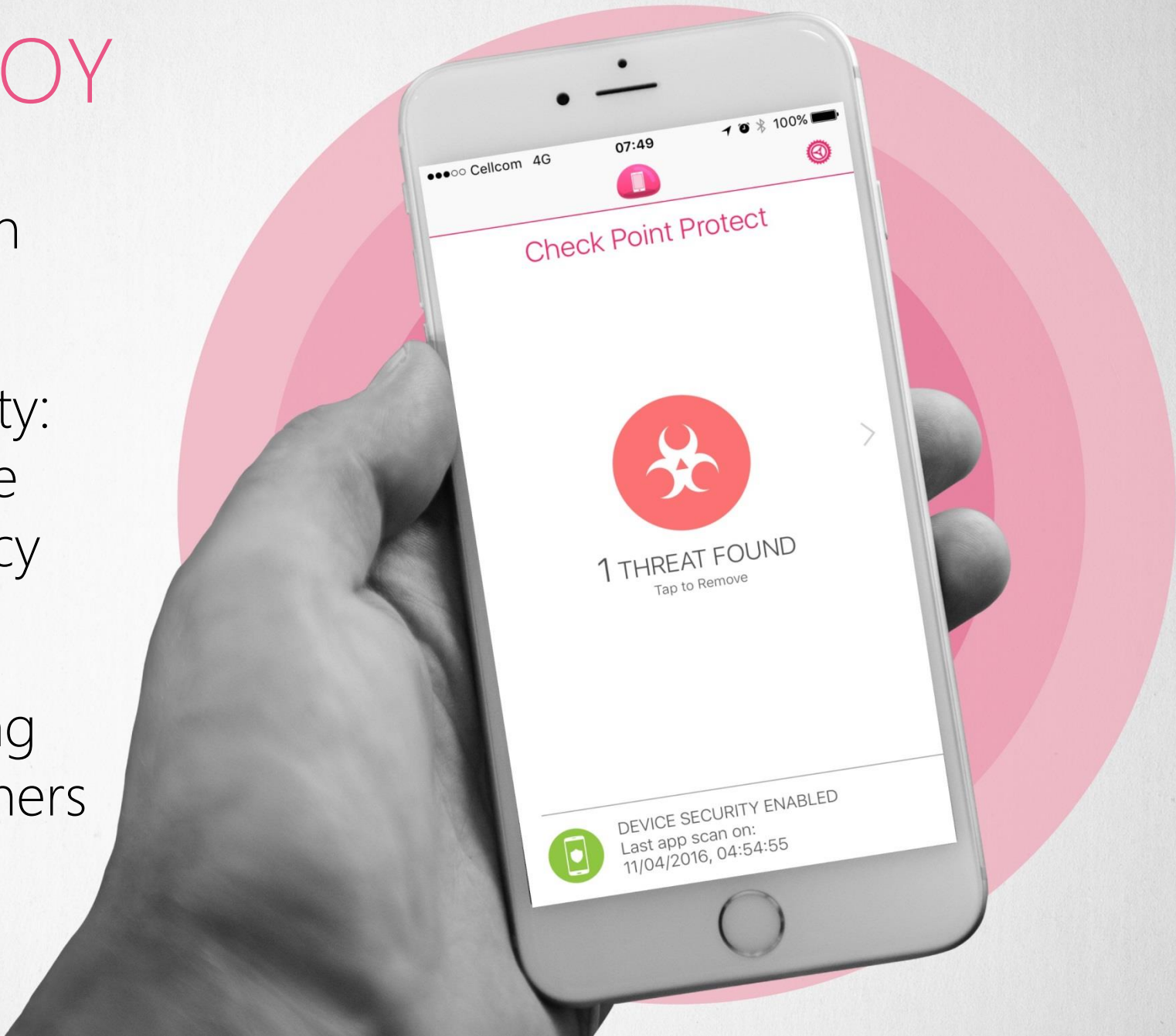
Without impacting usability:

No impact on battery life

Complete end user privacy



Integration with all leading  
EMM platforms and containers



# SUMMARY

MOBILE CYBER THREATS  
ARE ON THE RISE

EMPLOYEES' MOBILE  
DEVICES ARE WEAKEST LINK  
IN ANY IT INFRASTRUCTURE

CHECK POINT PROTECTS  
YOUR DEVICES FROM  
ADVANCED MOBILE THREATS

