



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

# CYBERSECURITY INNOVATIONS THAT MATTER

MOTI SAGEY  
HEAD OF STRATEGIC MARKETING & INTELLIGENCE

**CPX  
360**

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY



CLOUD • MOBILE • THREAT PREVENTION



Check Point®  
SOFTWARE TECHNOLOGIES LTD

PERCEPTION VS. REALITY

# THE STATE OF CYBER-SECURITY TODAY

*"THE IMAGINATION OF MAN'S  
HEART IS EVIL FROM HIS YOUTH"*

Genesis 8:21



WHAT DO OUR  
BUSINESSES NEED

INNOVATION  
THAT  
MATTERS!



Check Point  
SOFTWARE TECHNOLOGIES LTD





Check Point®  
SOFTWARE TECHNOLOGIES LTD

“

Innovation is  
change that  
unlocks new  
value

”

- Steve Jobs



The diagram illustrates a network of cybersecurity research projects and their interconnections. The nodes are organized into several clusters, with some nodes highlighted in pink to indicate specific areas of focus or collaboration.

**Key Nodes and Connections:**

- Top Row (Pink Nodes):** ACCOUNT TAKEOVER PREVENTION, DROPPED FILES EMULATION, INTELLIGENCE COLLABORATION, HUMAN INTERACTION SIMULATION, ZERO PHISHING, TRANSPARENT HTTPS INSPECTION.
- Second Row:** STATIC ANALYZER, FILE FEEDER, ADVANCED JAILBREAK PROTECTION, HYPERVISOR LEVEL SECURITY, CAMPAIGN HUNTING, ICON SIMILARITY, DGA Generator.
- Third Row:** CPU EXPLOIT DETECTOR, PUBLIC-CLOUD AUTO PROVISION, URL REPUTATION, MACHINE LEARNING, DOMAIN PREDICTION.
- Fourth Row:** FP-GUARD, ENDPOINT FORENSICS, EMBEDDED OBJECTS INSPECTION, BEHAVIORAL BOT PROTECTION, BLUETOOTH ATTACK DETECTION, MOBILE MAN IN THE MIDDLE ATTACK, SS7 ATTACK PREVENTION.
- Fifth Row:** MOBILE CODE ANALYSIS, MOBILE APP SCANNING, THREAT EXTRACTION, OS-LEVEL SANDBOX, ANTI-RANSOMWARE.
- Sixth Row:** MOBILE SMS PHISHING, ADAPTIVE CLOUD SECURITY, IMAGE FILE SANITIZER, CPU LEVEL SANDBOX, Behavior similarity, FLASH EMULATION.
- Bottom Row:** ENDPOINT EXPLOITATION DETECTION, SMEP Detector, MACRO ANALYSIS, MEMORY ANALYSIS, DECOYS & TRAPS, INTRUSION PREVENTION.

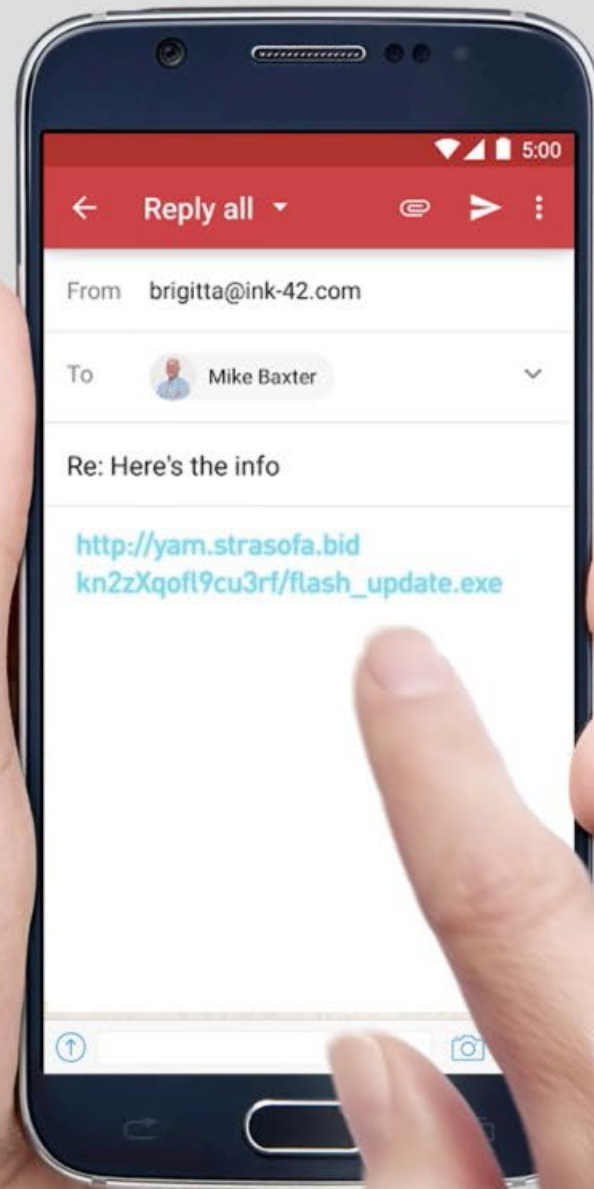
The diagram shows a dense network of connections between these nodes, representing the collaborative nature of the research projects. The pink nodes are interconnected with various other nodes, highlighting their central roles in the network.

# LETS SEE A FEW EXAMPLES





DOES THIS COME  
FROM A FRIEND  
OR A FOE?



# LETS TALK ABOUT REAL TIME PREVENTION







Check Point®  
SOFTWARE TECHNOLOGIES LTD

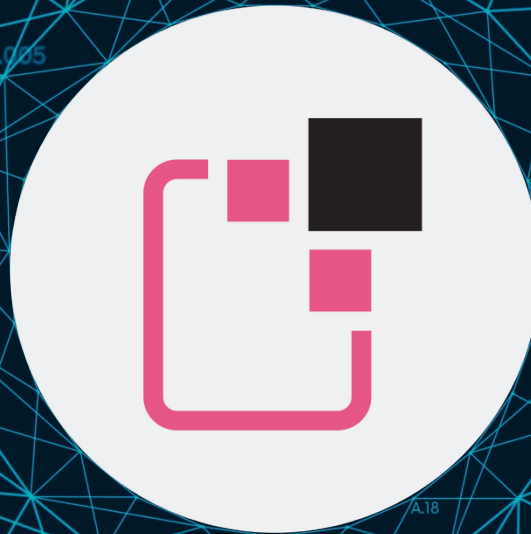
# REAL TIME PREVENTION



# REAL TIME PREVENTION



Check Point®  
SOFTWARE TECHNOLOGIES LTD



# WITH UNIQUE THREAT EXTRACTION



# CHECK POINT REAL-TIME PREVENTION INNOVATIONS



Check Point®  
SOFTWARE TECHNOLOGIES LTD

“Perhaps the most impressive element of Check Point’s malware analysis approach is the ability to capture an email attachment, analyze it, and render the content for the end user or security team while the malware is mitigated.

FORRESTER®







# PHISHING ATTACKS

76%

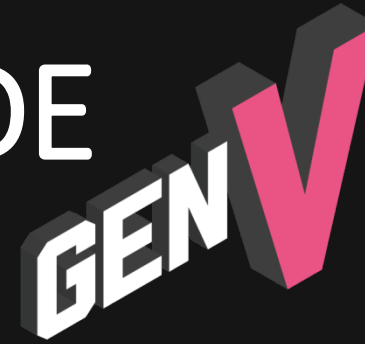
OF ORGANIZATIONS HAVE  
EXPERIENCED A PHISHING  
ATTACK IN THE PAST YEAR

2019 Security Report



2018 Security Report

# NOT ALL VENDORS PROVIDE REAL-TIME PREVENTION



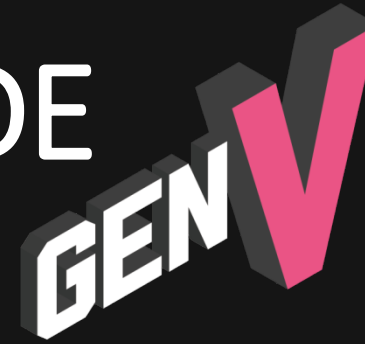
Check Point®  
SOFTWARE TECHNOLOGIES LTD

## About WildFire

The WildFire [Virtual Sandbox](#) identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block the malware. When a Palo Alto Networks firewall detects an unknown sample (a file or a link included in an email), the firewall can automatically forward the sample for WildFire analysis. Based on the proWildFire Administrator's Guide properties, behaviors, and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire determines the sample to be benign, grayware, or malicious. **WildFire then generates signatures** to recognize the newly-discovered malware, and makes the latest signatures globally available every five minutes. All Palo Alto Networks firewalls can then compare incoming samples against these signatures to automatically block the malware first detected by a single firewall.

# 5 MINUTES

# NOT ALL VENDORS PROVIDE REAL-TIME PREVENTION



Check Point  
SOFTWARE TECHNOLOGIES LTD

## DOES NOT BLOCK

Sending files to the FortiSandbox Cloud **does not block** files that it uploads. Instead they are used to improve how quickly new threats can be discovered and signatures created for them and added to the FortiGuard antivirus database.



FortiOS™ Handbook - FortiOS Handbook

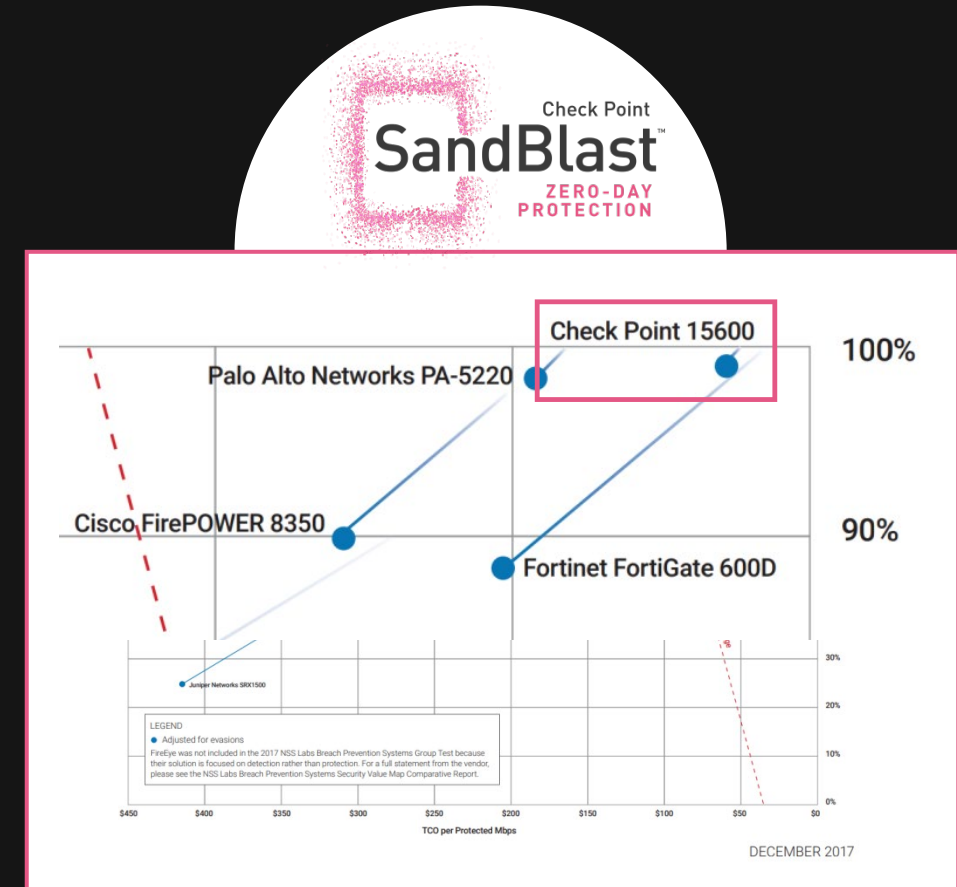
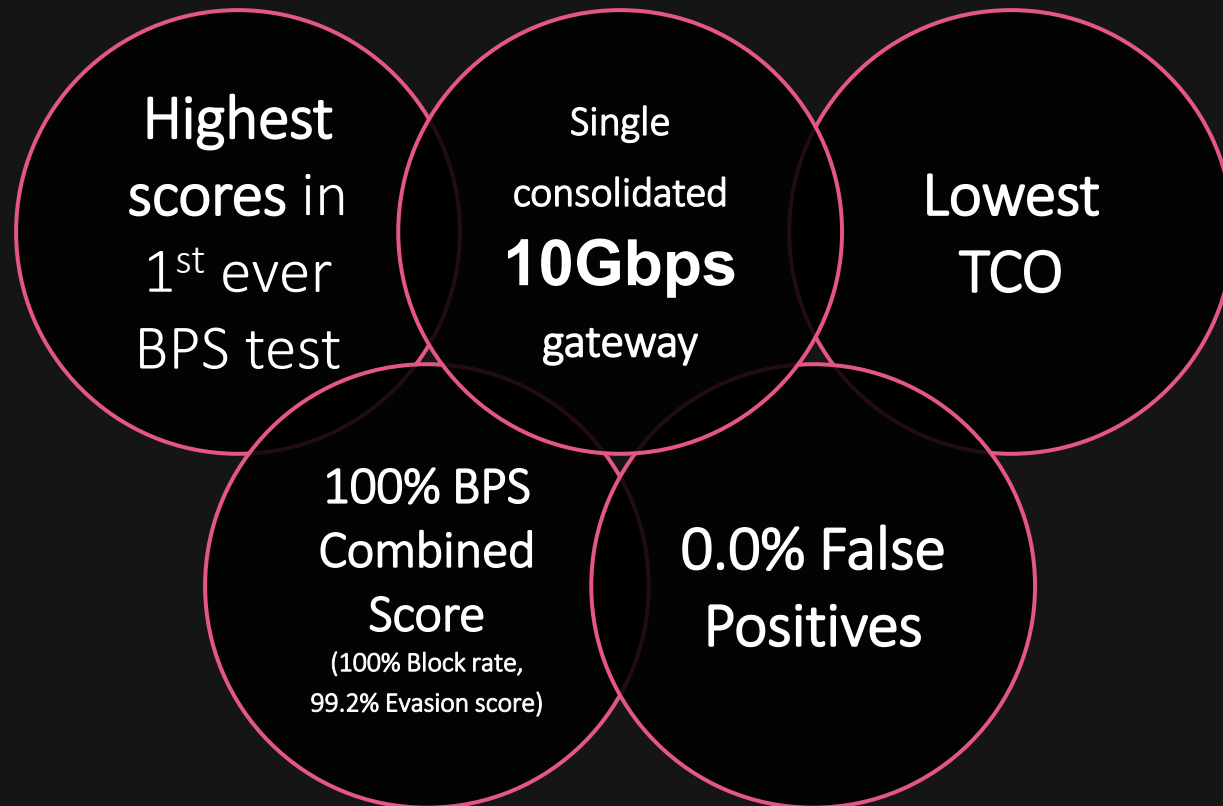


# INNOVATION THAT MATTERS

## NSS LABS: THE BEST PROTECTION AND VALUE TO OUR CUSTOMERS



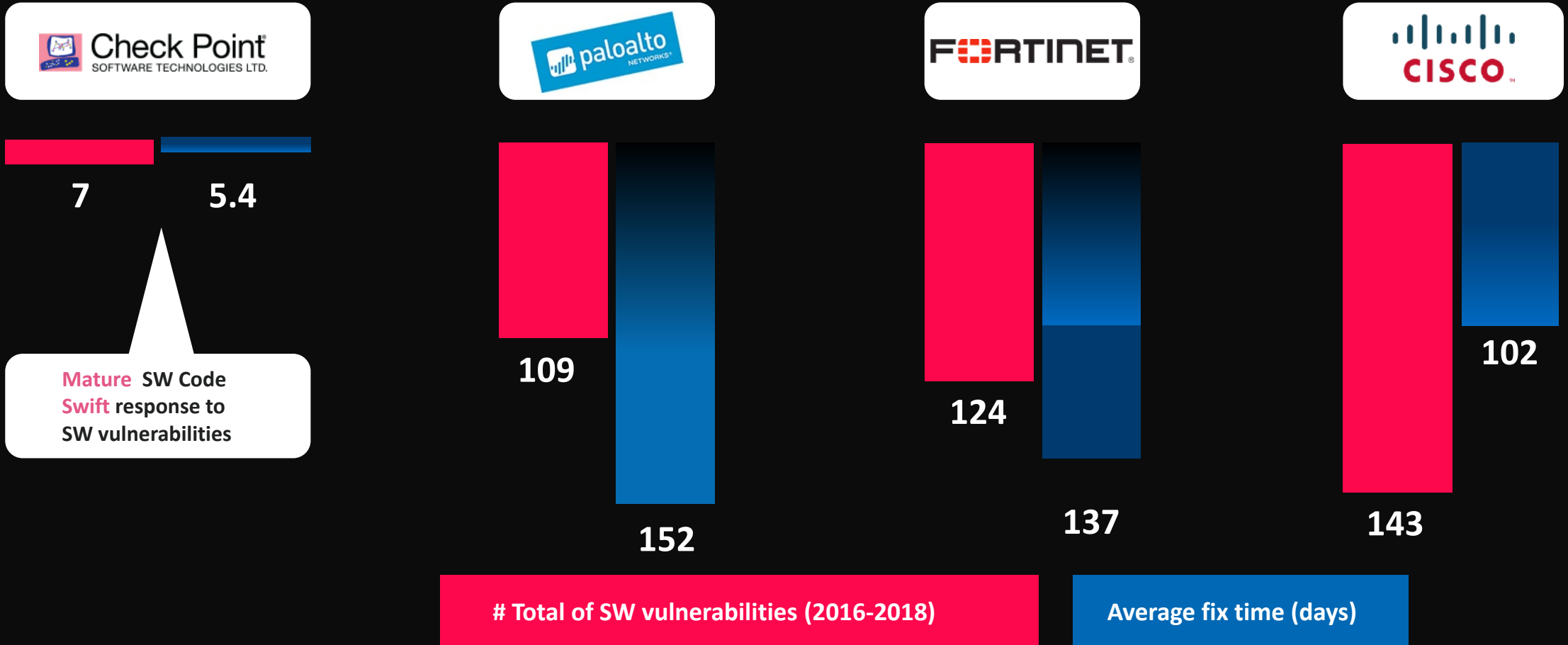
Check Point  
SOFTWARE TECHNOLOGIES LTD



# ONE LAST WORD ABOUT FOCUS & TRUST



# MAKE SURE YOUR SYSTEMS ARE NOT EXPOSED...



Source: vendors security advisories web pages & <http://tiny.cc/urgency>



# THE BRAINS BEHIND THE INNOVATION



Check Point®  
SOFTWARE TECHNOLOGIES LTD

1532

30%  
OF TOTAL EMPLOYEES



Check Point®  
SOFTWARE TECHNOLOGIES LTD

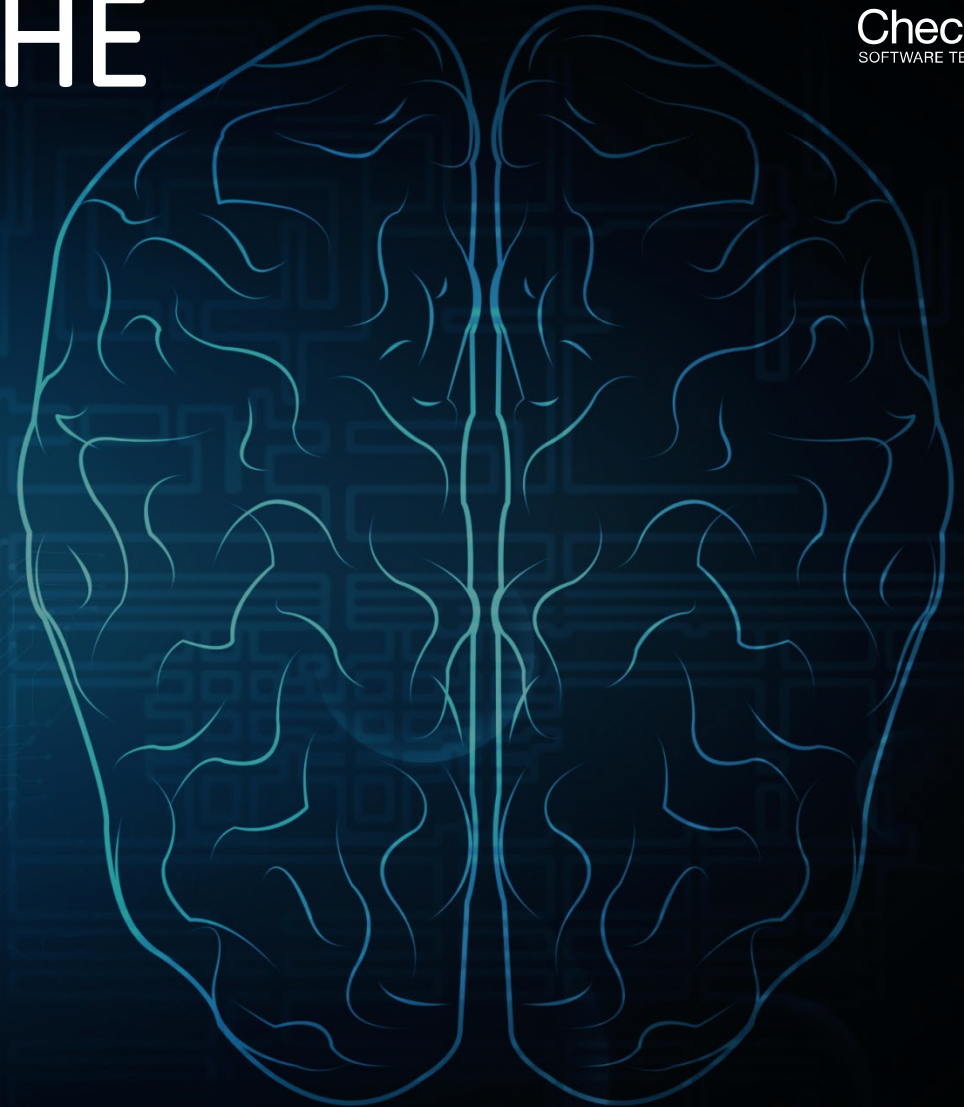
1319

25%  
OF TOTAL EMPLOYEES

FORTINET®

1047

19%  
OF TOTAL EMPLOYEES



## # R&D ENGINEERS



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

# THANK YOU

For slides: <http://tiny.cc/moti19>

MOTI SAGEY (MBH)

HEAD OF STRATEGIC MARKETING & INTELLIGENCE

**CPX  
360**

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY



CLOUD • MOBILE • THREAT PREVENTION