CHECK POINT™

SECURING YOUR MOBILE WORKFORCE

Amplify Oshkosh

Sam Belongia – Threat Prevention Sales Manager

YOU DESERVE THE BEST SECURITY

Agenda

- About me
- Threat landscape
- Current state of remote workforce security
- Key takeaways
- Q&A

©2022 Check Point Software Technologies Ltd.

THREAT LANDSCAPE

[Protected] Distribution or modification is subject to approval

Biological Pandemic vs. Cyber Pandemic:

Similarities and Parallelization, Lessons Learned

BIOLOGICAL PANDEMIC

INFECTION RATE

Virus infection rate (R0) (source:WHO)
The average number of people that one person with a virus infects

Flue: 1.3, SARS: 2-4, **Corona: 2.5**
Ebola:1.6-2, ZIKA:2-6.6,Measels:11-18

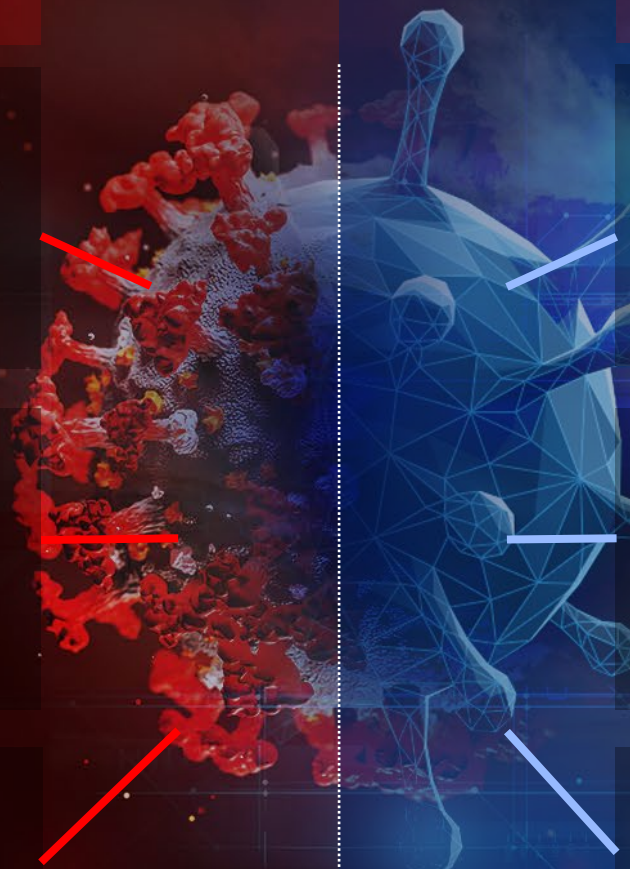
INFECTION PREVENTION

Best treatment: **Vaccination**
Dealing with Infection Best Practices:

1)Quarantine, shelter in place
2)Isolation
3)Contact tracing

SAFETY BEST PRACTICES

common treatment (until vaccination):
1)Mask
2)Hygiene
3)Social distancing



CYBER PANDEMIC

INFECTION RATE

Malware infection rate (R0) The average number of infections that one host with a malware causes

Cyber attack- >27(source: WEF, NSTU),
Slammer: doubled in size every 8.5 seconds,
Code red – 2000 new hosts per minute

INFECTION PREVENTION

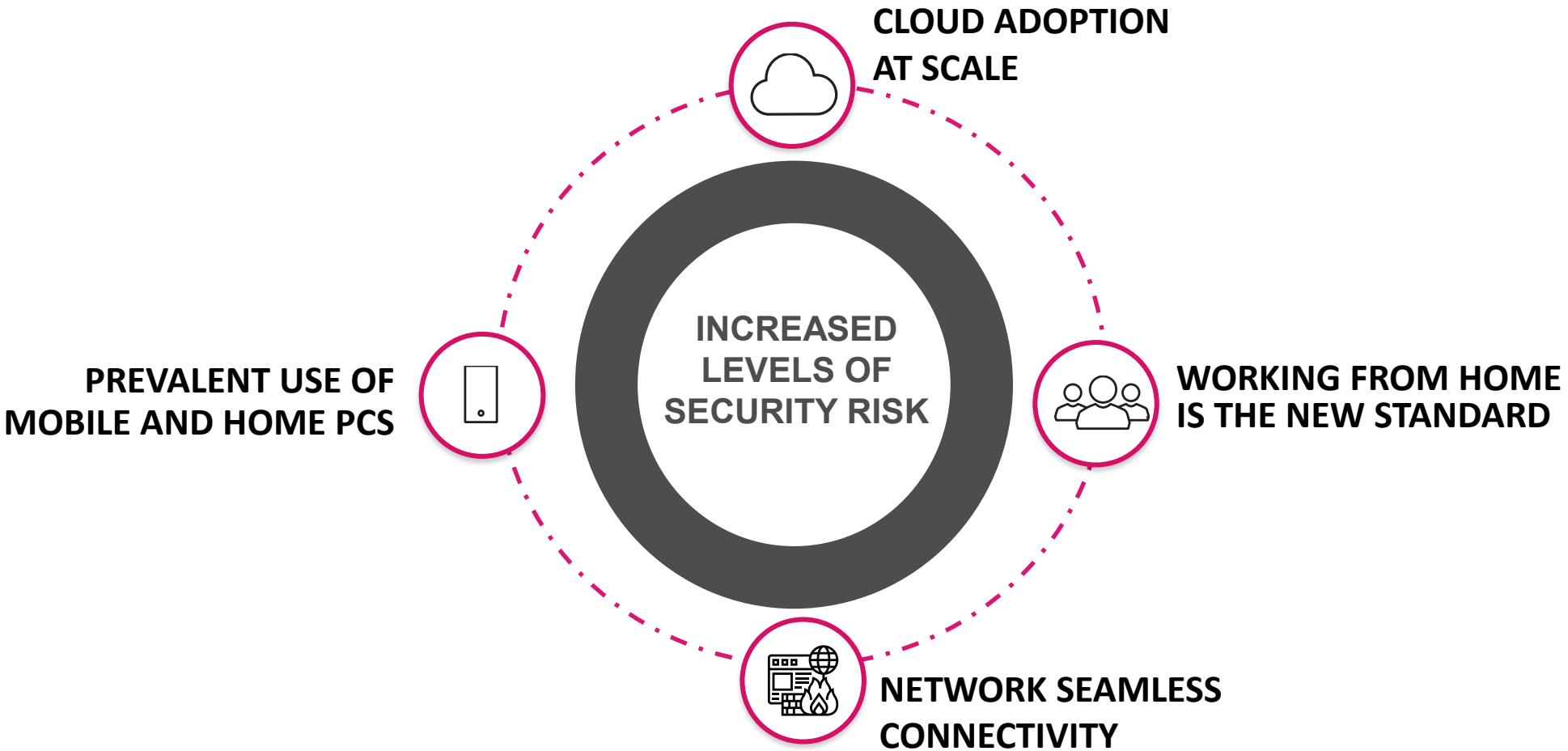
Best treatment: **Real Time Prevention**

Best Practices- **Continuous** process of:
1)**Quarantine**: sandboxing, micro segmentation
2)**Isolation**: Zero Trust, segregation
3)**Tracing:** Threat Intel., AI, SOC, Posture management

SAFETY BEST PRACTICES

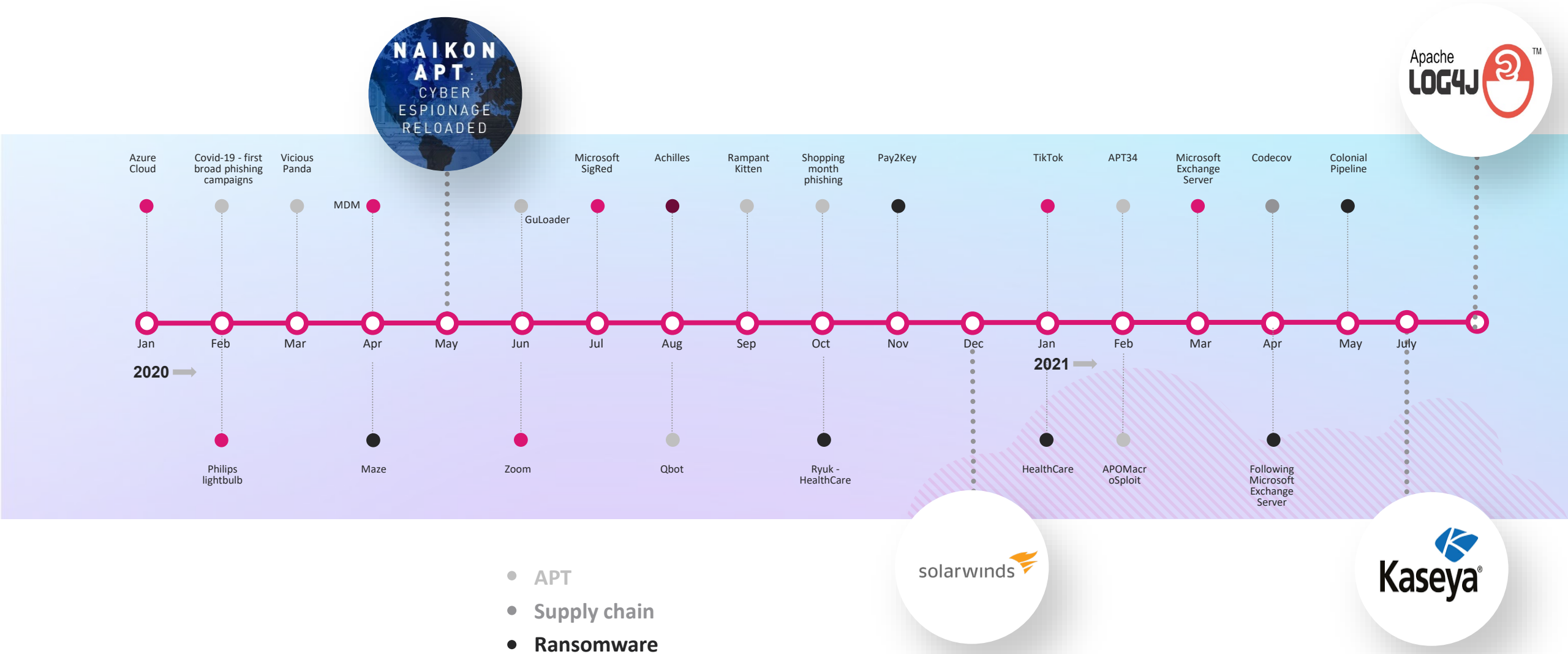
1)**Awareness**: think before you click …
2)**Cyber Hygiene**: Patches, Compliance…
3)**Asset distancing-** network Segmentation, Multi Factor authentication…

THE PANDEMIC WILL DISAPPEAR.
ITA CYBER EFFECT IS HERE TO STAY



©2022 Check Point Software Technologies Ltd.

2021'S SIGNIFICANT CYBER ATTACKS MORE FREQUENT, MORE INTENSE

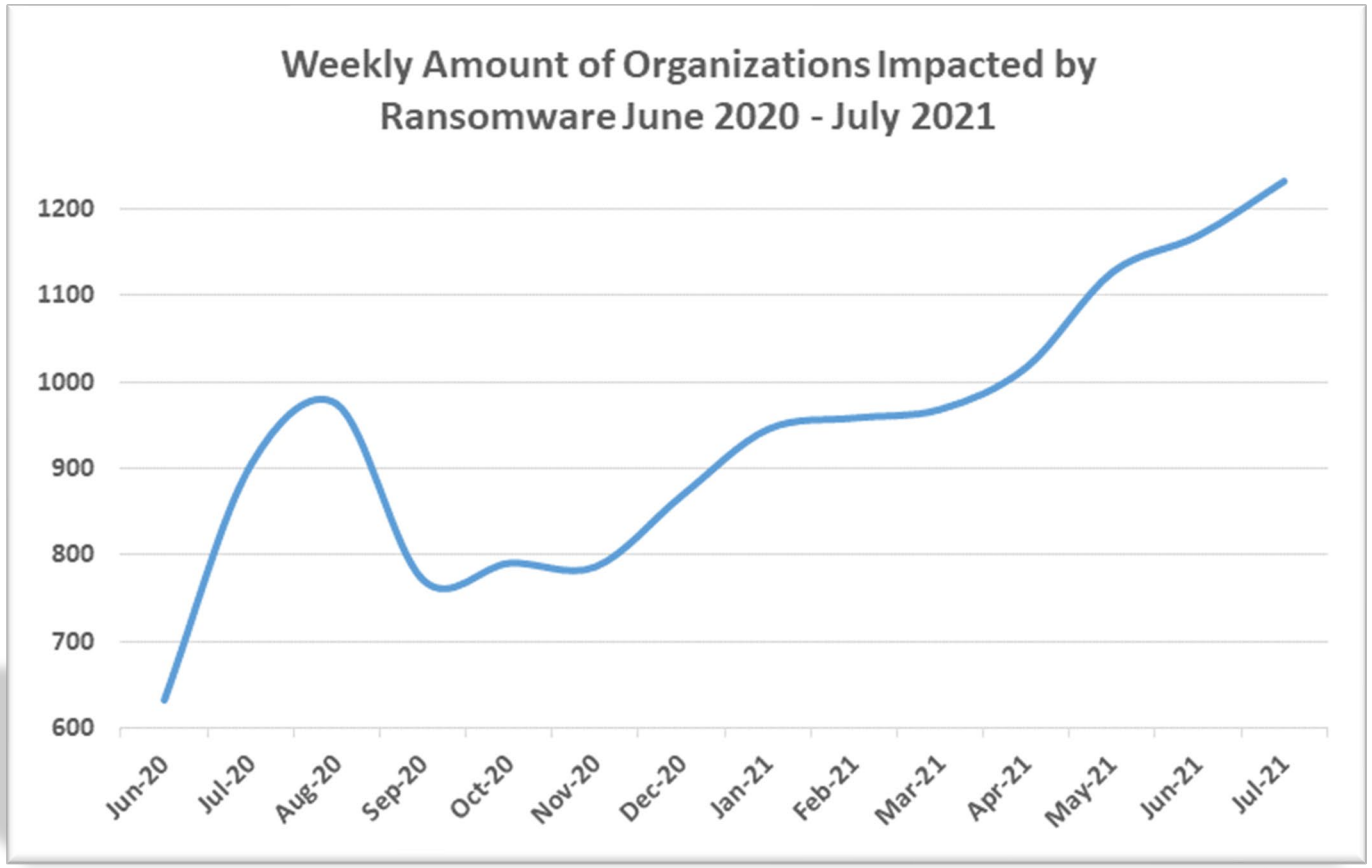


- APT
- Supply chain
- Ransomware
- SW vulnerabilities

©2022 Check Point Software Technologies Ltd.

Ransomware attacks surge globally, hitting a 93% increase year on year

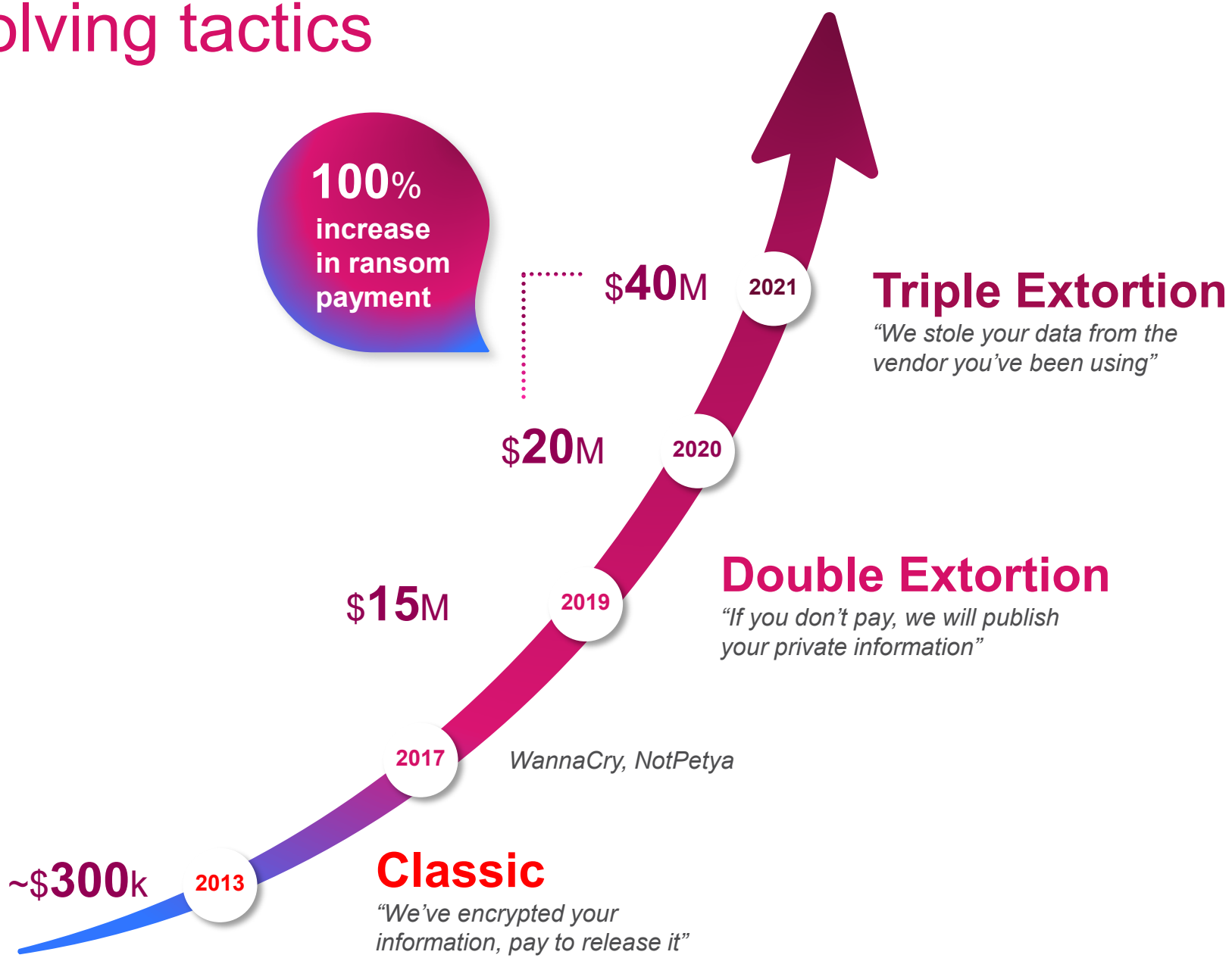
- Over 1210 organizations impacted weekly
- **93% increase** year over year



©2022 Check Point Software Technologies Ltd.

Ransomware evolving tactics

Attack sophistication & cost increase



*June 2020 – June 2021

©2022 Check Point Software Technologies Ltd.

MAY 7, 2021

Colonial pipeline halts operations after ransomware attack

Colonial Pipeline attack - What do we know?

- **Motivation**: Financial/Target critical infrastructure
- Billing system was compromised resulting in the inability to bill the customers
- Shut down the pipeline as a precaution
- Double extortion - The attackers stole 100GB of data. threatened to release it if ransom was not paid
- Ransom paid close to $5M
- Department of Justice recovered $2.3M in value from the ransom payment
- FBI declared it retrieved the private key of the ransom account and recovered 63.7 of the bitcoins paid

©2022 Check Point Software Technologies Ltd.

JUNE 10, 2021

Meat supplier JBS pays ransomware hackers $11 million

The world's largest beef supplier has been hit with a ransomware attack

- **Motivation**: Financial
- JBS – processes 20% of North America meat supply
- Attack conducted by Russian speaking REvil group
- Campaign started in February and discovered in June
- SIX JBS plants in the U.S. shut down
  - Also affecting plants in Canada and Austalia
- Over 45 GB of data exfiltrated
- JBS indicated that while it was able to get most of its systems running, it chose to pay $11M ransom to keep its files safe

©2022 Check Point Software Technologies Ltd.

JULY 2, 2021

“KASEYA ATTACK”:

Over 1000 organizations globally attacked on biggest supply chain attack since SUNBURST

What Happened?

- **Motivation**: Financial/Data theft
- Delivered through an automatic update of the Kaseya VSA client management and monitoring software
- Attack affecting numerous organizations
  - 1,500 businesses impacted
  - Victims in 17 countries
- Ransom demands ranged between US$45K to US$5 million
- Attack associated to Russian group REvil

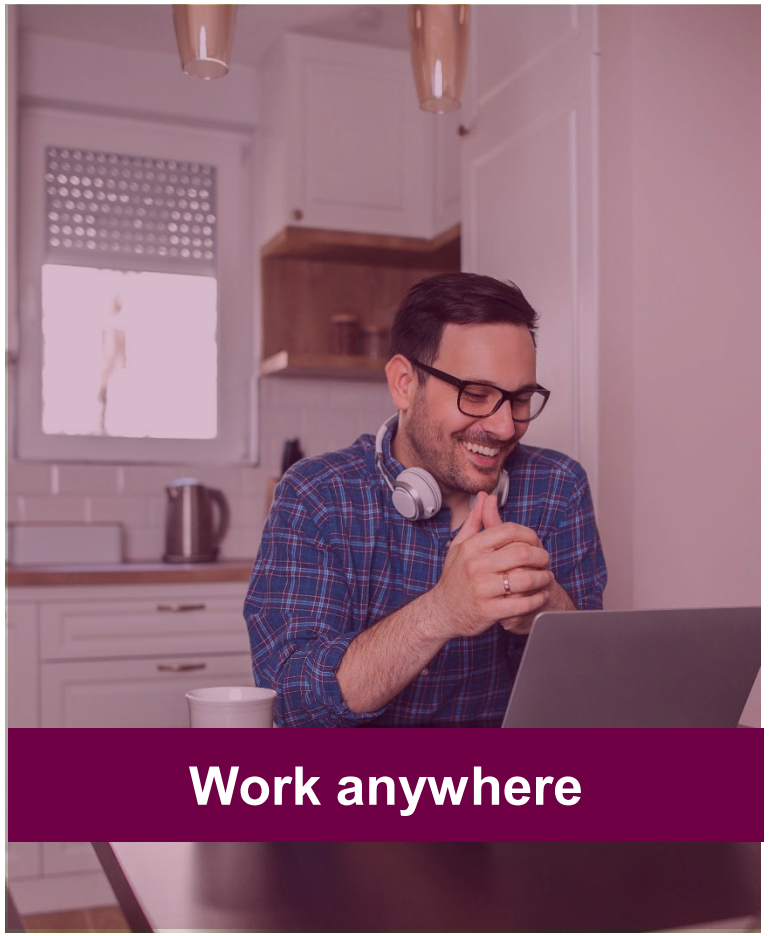
©2022 Check Point Software Technologies Ltd.

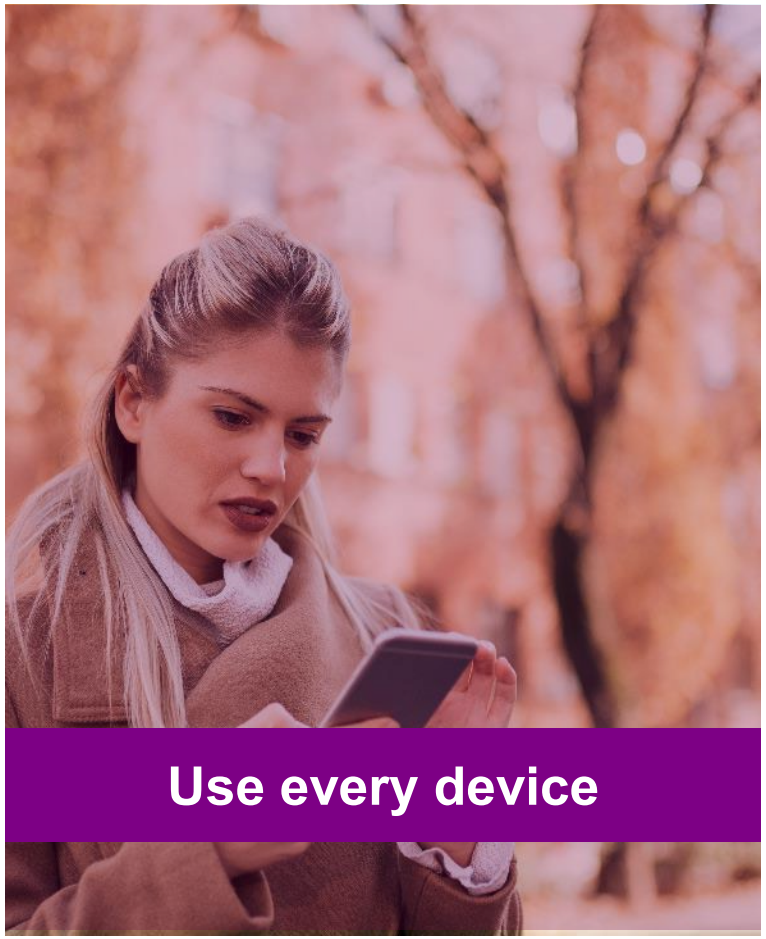
CURRENT STATE OF REMOTE WORKFORCE SECURITY

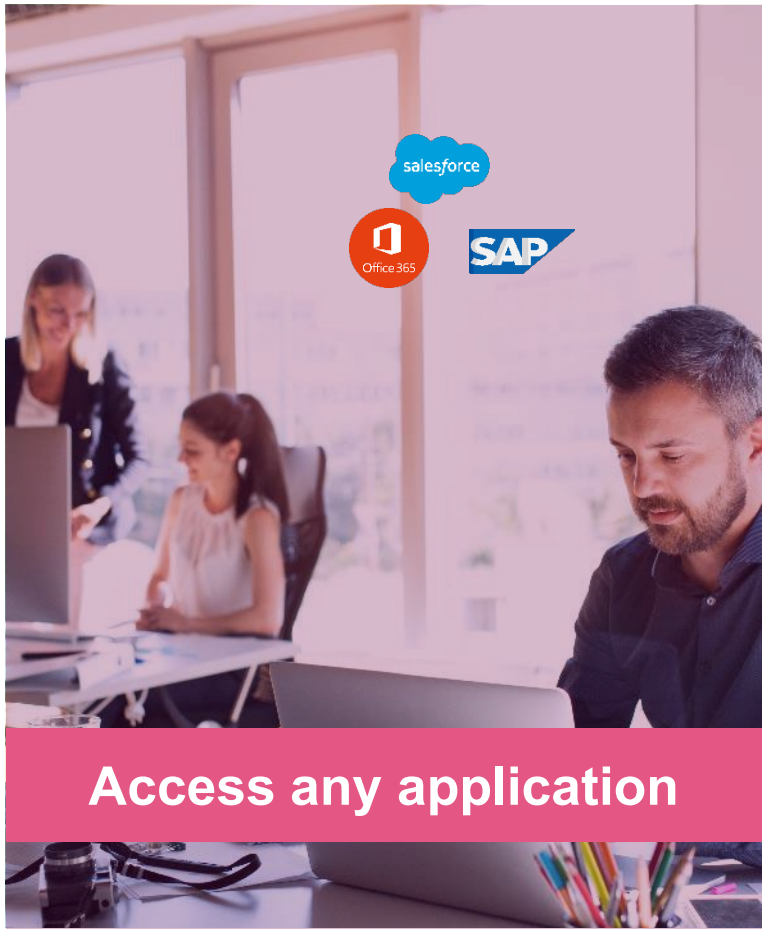
[Protected] Distribution or modification is subject to approval

Remote work is here to stay

57% of businesses report that most of their employees work remotely at least 2 days a week*







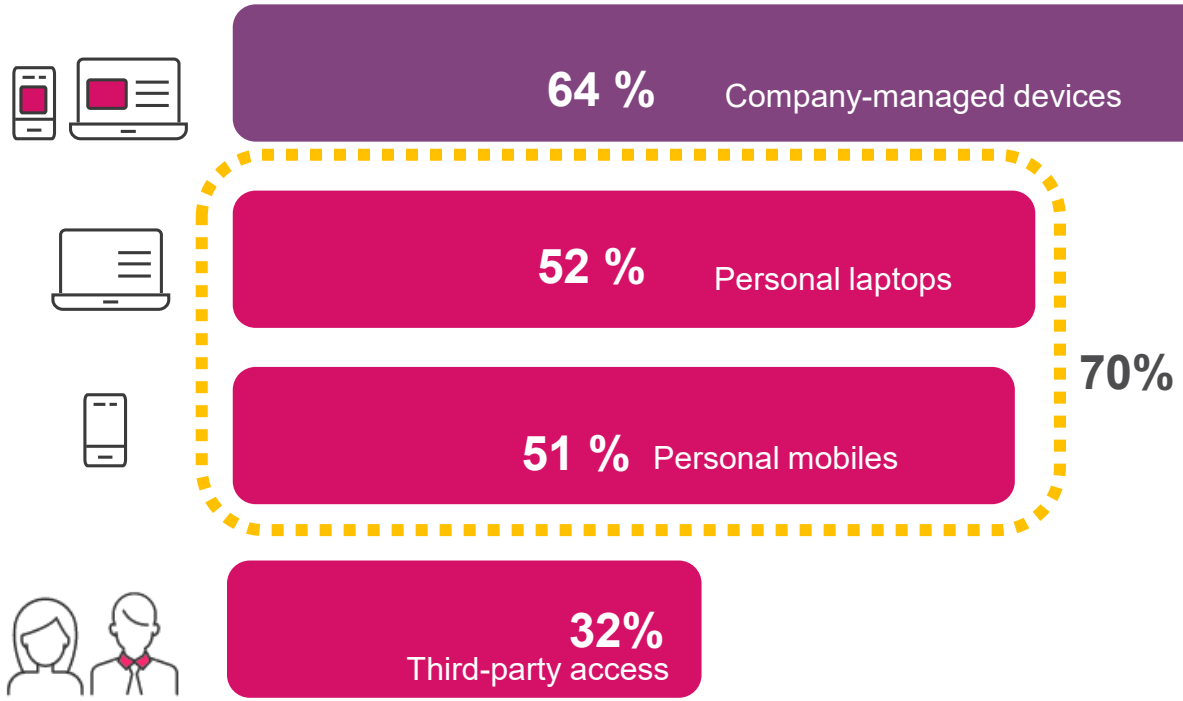
* Based on 2021 remote workforce security survey, among 1208 security professionals WW.

©2022 Check Point Software Technologies Ltd.

The state of remote access

70% of companies allow access to their corporate assets from personal laptops and mobiles

Your organization's security policy allows remote access to corporate applications...
choose all that apply



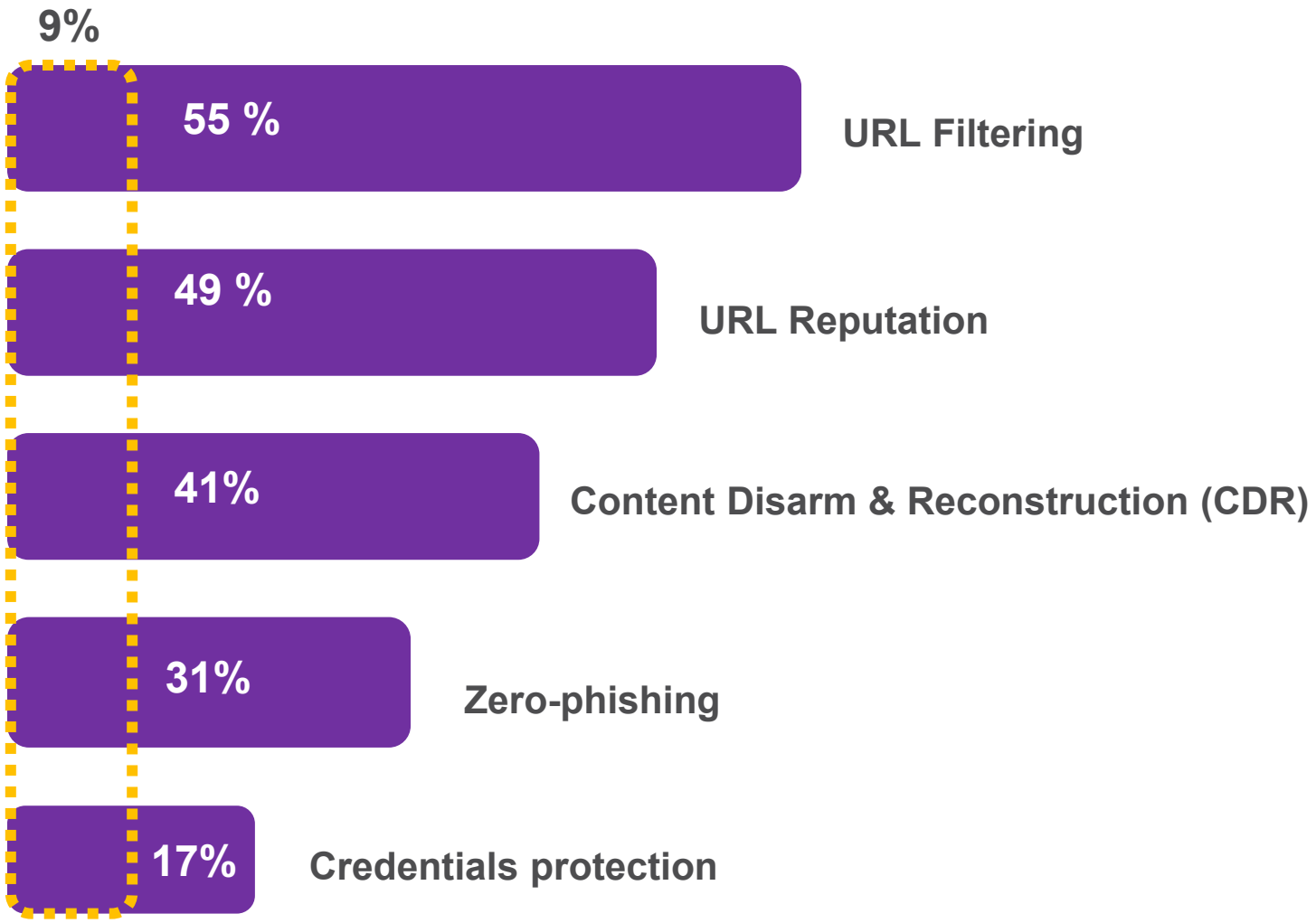
* Based on 2021 remote workforce security survey, among 1208 security professionals WW.

©2022 Check Point Software Technologies Ltd.

The state of Internet Access Security

Only 9% of organizations use all the 5 must-have protections

How do you protect remote users while they are browsing the internet?

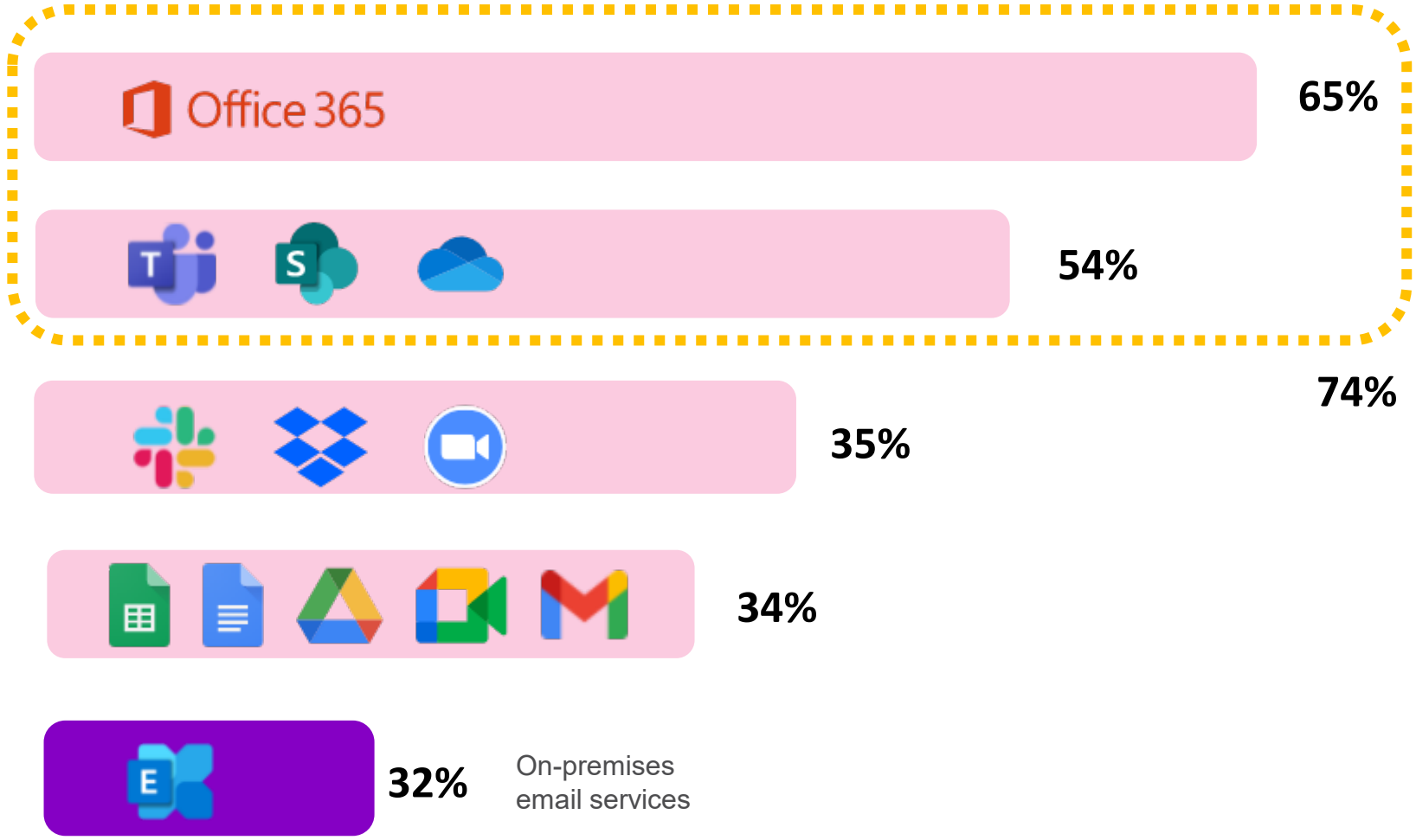


©2022 Check Point Software Technologies Ltd.

The state of email security

74% use Office 365 email and collaboration apps like Teams, SharePoint, and OneDrive.

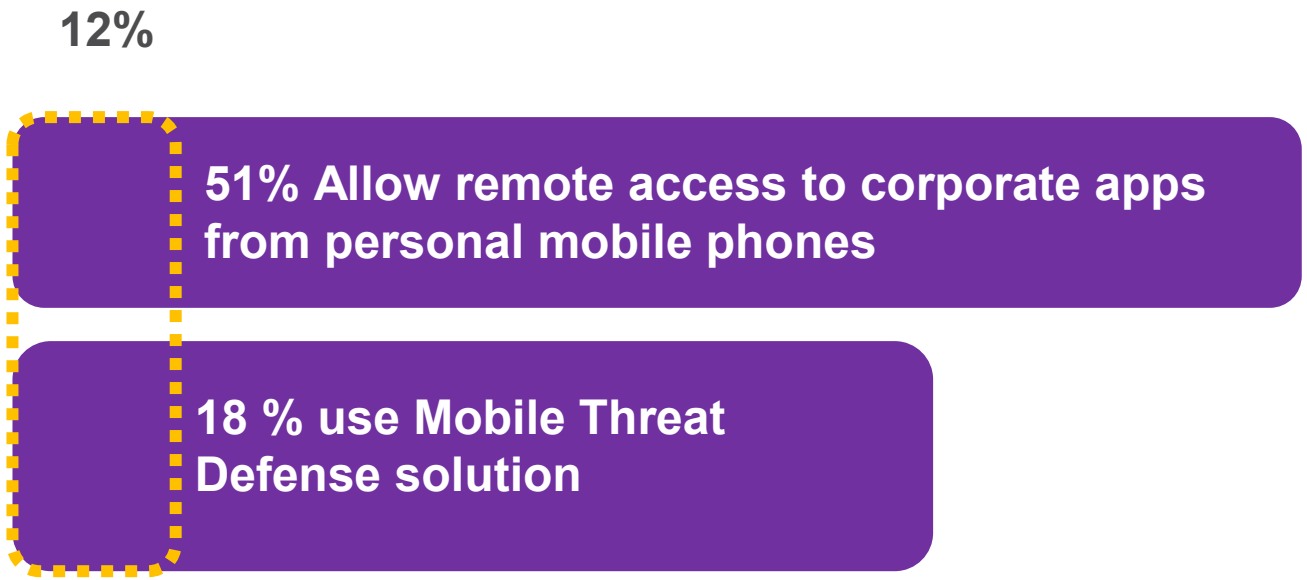
What applications your company's employees use for corporate email and collaboration?



©2022 Check Point Software Technologies Ltd.

The state of Mobile security

Only 12% of organizations allow mobile access with a proper protection



* Based on 2021 remote workforce security survey, among 1208 security professionals WW.

©2022 Check Point Software Technologies Ltd.

KEY TAKEAWAYS

[Protected] Distribution or modification is subject to approval

Key Takeaways

- Endpoint
  - Minimize the attack surface
  - Prevent zero days
  - Autonomous remediation and recovery
  - Forensics (EDR/MDR)

- Email
  - Prevent advance phishing and spear phishing attacks
  - Block impersonation and Business Email Compromise attempts
  - Block malicious attachments with malware
  - Protect users from threats hiding in malicious links
  - Prevent malicious and unintentional data leakage

©2022 Check Point Software Technologies Ltd.

Key Takeaways (cont)

- Internet access (SASE)
  - Deploy a cloud-based secure web gateway to allow remote users to securely access the internet
  - Prevent malicious downloads
  - URL filtering
  - Data loss prevention (DLP)
  - Browser exploit prevention
  - Corporate credential reuse prevention
  - VPN-as-a-service
  - Move to Zero Trust application-level access
- Mobile
  - Prevent the download of malicious apps
  - Prevent phishing and man-in-the-middle attacks
  - Detect device vulnerabilities and OS configuration changes

©2022 Check Point Software Technologies Ltd.

THE MOST COMPLETE SECURITY

CloudGuard — SECURE THE CLOUD

CloudGuard Posture Management
Posture Management & Visibility

CloudGuard Intelligence
Network Traffic Analysis

CloudGuard Workload
Runtime Workload Protection

CloudGuard Network
Cloud Access Control & Prevention

CloudGuard AppSec
Web and API Protection

Multi & Hybrid Cloud

SD-WAN

Quantum — SECURE THE NETWORK

Quantum Security Gateway
Perimeter & Data Center

Quantum Maestro
Hyperscale

Quantum SMB
Branch & SMB

Quantum Rugged
ICS Security

Quantum IoT Protect
IoT Security

- Access Control
- Multi-layered Security
- Advanced Threat Prevention
- Data Protection

- Access Control
- Multi-layered Security
- Advanced Threat Prevention
- Wi-Fi, DSL, 3G/4G/ LTE

Infinity-Vision

CONSOLIDATED MANAGEMENT & SECURITY OPERATIONS

INFINITY PORTAL
Management & Unified Visibility

Infinity SOC
Security Operations & XDR

R81
Security Platform

Quantum Smart-1 Cloud
Management

THREATCLOUD
Threat Intelligence

Harmony — SECURE USERS & ACCESS

REMOTE ACCESS

Harmony Connect
- Corporate Access
- Internet Access

EMAIL AND OFFICE

Harmony Email & Office
- Account Takeover Protection
- Data Loss Prevention
- Threat Prevention
- Zero Phishing

ENDPOINT AND MOBILE

Harmony Endpoint
- Threat Prevention
- Anti-Ransomware
- Forensics
- Secure Media
- Access Control

Harmony Browse
- Zero Day Browser Protection
- Threat Prevention
- Zero Phishing

Harmony Mobile
- App Protection
- Network Protection
- Device Protection

©2022 Check Point Software Technologies Ltd.

THANK YOU

YOU DESERVE THE BEST SECURITY

[Protected] Distribution or modification is subject to approval