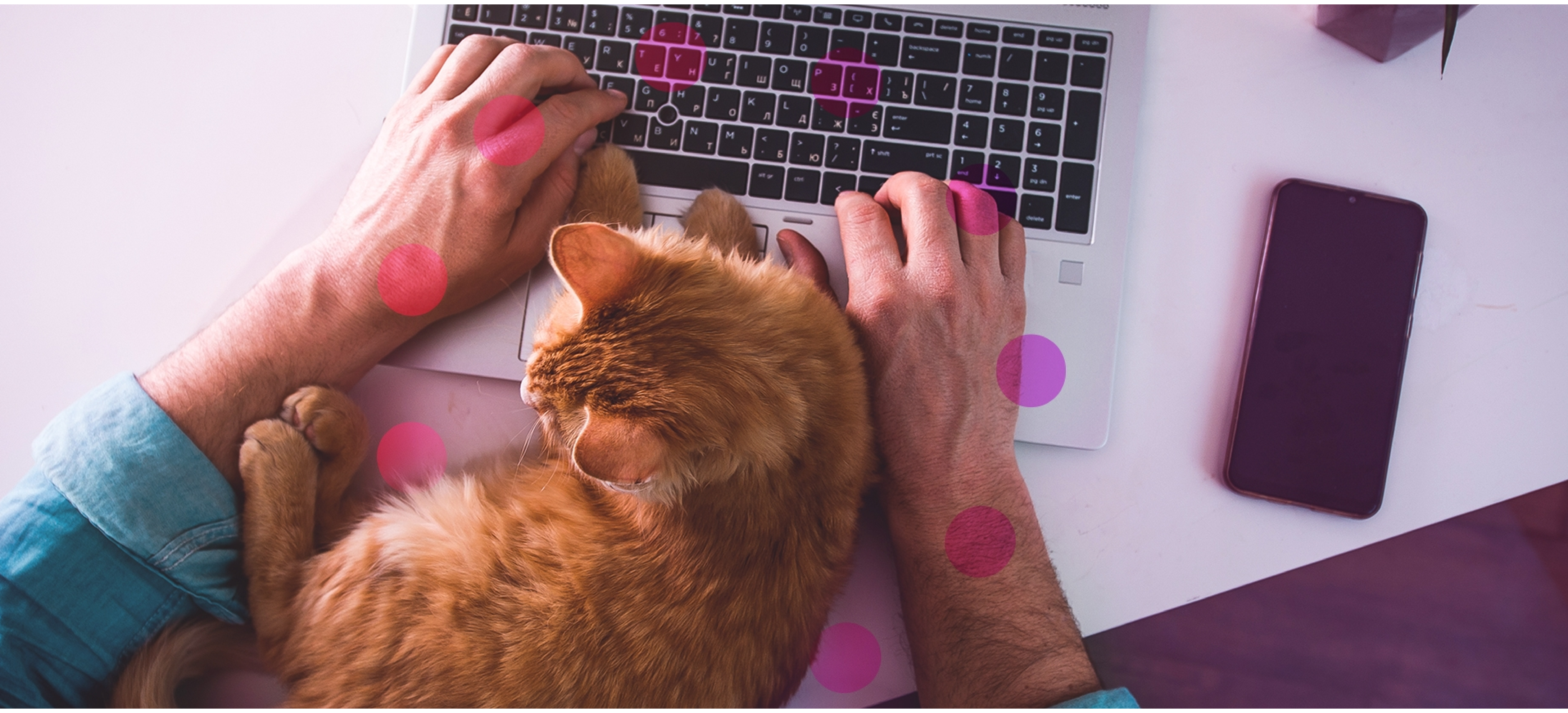
CHECK POINT™

THE ULTIMATE GUIDE TO REMOTE WORKFORCE SECURITY

And the 5 must-have protections for users, devices, and access in the new distributed workspace

CONTENTS



INTRODUCTION

The world as we know it has changed. In this new world, work is no longer being performed primarily at the corporate office.

This means that being productive requires us to always be connected, everywhere, no matter where we are, or what device we are using, and no matter which application we need to access.

What this also means is that the attack surface has never been wider.

To combat the challenge and defend against increasingly sophisticated attacks, such as phishing and ransomware, organizations can keep adding individual security products. But stitching together point solutions leaves them with security gaps, fragmented visibility, complex management, and limited options to scale.

In this paper we will cover the different cyber threats that arise from the new distributed workspace, and the five must-have protections to keep remote users safe across all threat vectors.

We will also demonstrate how organizations can enhance protection by consolidating security solutions for users, devices, and access, and how Check Point Harmony can help.

GLOBAL WORK GOES REMOTE

The everywhere employee Remote work is the new standard, with 81% of organizations having adopted mass remote working, and 74% planning to enable large-scale remote work permanently.

This makes today's employee – the "everywhere employee," who can (and does) work anywhere, and who uses multiple devices to access the internet, corporate network, and many applications. The result is that sensitive business data is continually flowing from both corporate and BYOD devices to cloud, IaaS, and datacenters, expanding the attack surface wider than ever.

Organizations need to enable access to any application from any location through any device, and to make sure that it is not only seamless but also

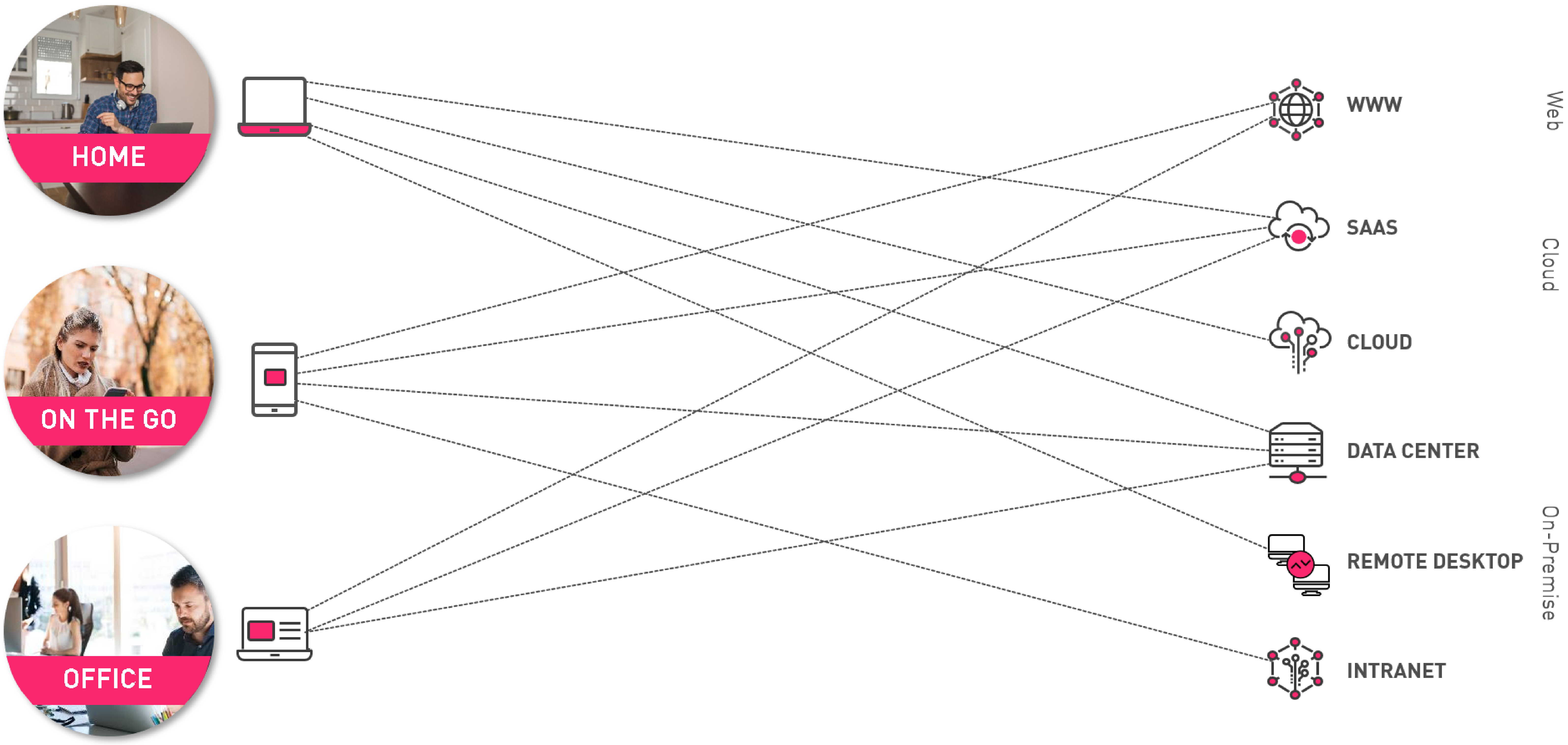
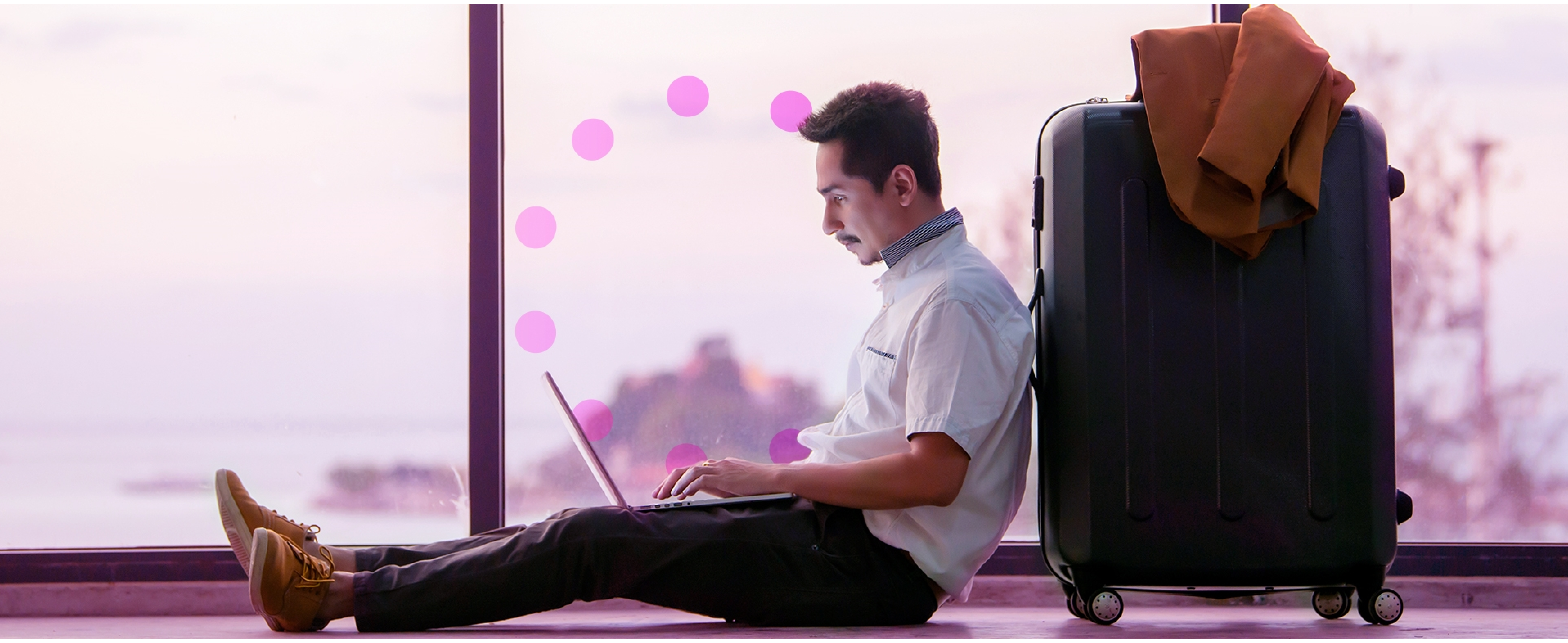


Figure 1:
In the new world we want to use any device to access any application



The inevitability of unintentional errors

Further complicating the security challenge is that remote users are more susceptible to cyber threats. According to a recent industry survey of 2,000 remote employees from across the world, 67% admit to finding workarounds to corporate security policies in order to be more productive. This includes sending work documents to personal email addresses, sharing passwords, and installing rogue applications.

Unfortunately, enhancing security awareness doesn't fully do the job of reducing risk. According to the same survey, over half (54%) of the employees said they had received remote-work specific security training, yet ~70% admit to using corporate devices for personal use. And ~60% admit that they allow other members of their household to use their corporate devices for activities such as schoolwork, gaming, and shopping.

The global surge in cyberattacks

All this has not gone unnoticed by hackers. To illustrate, in the 2021 Check Point Cyber Security report, it was noted that:

- There was a 93% increase in ransomware, with the number of organizations impacted globally having more than doubled during the first half of 2021 over 2020.
- During 2020, 100,000 new malicious websites and 10,000 new malicious files were discovered daily.
- On average, a new organization had become a victim every 10 seconds worldwide.

And the threat is very real and can be very damaging. For example, in March 2020, hotel industry giant, Marriott disclosed a new data breach impacting 5.2 million hotel guests. The breach occurred when a hacker used the login credentials of two franchise property employees to access customer information from an app's backend systems.

As we can see, to keep corporate networks and sensitive data safe, organizations have no option but to recalibrate the security approach around remote users and access.

And the first step is to make sure that they have in place the five must-haves for effectively protecting the remote workforce.

THE 5 MUST-HAVE PROTECTIONS FOR REMOTE USERS

And how Check Point Harmony can help

The importance of securing remote users cannot be understated. The business is only truly protected when its users are, as most attacks start at the weakest link – the user.

Achieving this important objective requires the following five must-have protections:

01 Endpoint Security

02 Secure Internet Access

03 Zero Trust Network Access (ZTNA) to Corporate Applications

04 Email & Office security

05 Mobile Threat Defense (MTD)

Must-Have #1

ENDPOINT SECURITY

> **70% of successful cyber-attacks originate at the endpoint.**
>
> (IDC)

With 93% increase in ransomware attacks across the globe over the last 6 months, endpoint devices have never been more vulnerable, and endpoint security plays a critical role in enabling your remote workforce. Yet, there have never been more endpoints to protect as companies opened access to their corporate applications from laptops to ensure business continuity. While maintaining productivity, remote users are more prone to incautious behavior and non-compliance to corporate policy. As a result, they are more exposed to phishing, malware, and ransomware attacks. And once a user PC or laptop is infected, the threat can move laterally and easily infect other endpoint devices and corporate assets.

Endpoint protection (EPP) and Endpoint Detection and Response (EDR) serve as the first and last line of defense against the growing wave of ransomware attacks.

The 5 pillars of a robust endpoint security solution

Anti-phishing
Defending users from phishing attacks (including zero-day phishing) while they are using their mailboxes or browsing the internet.

Anti-ransomware
Capabilities that monitor changes to files on user drives to identify ransomware behavior such as illegitimate file encryption, and to block an attack, as well as to recover encrypted files automatically

Content Disarm and Reconstruction (CDR)
CDR can remove exploitable content by sanitizing documents from any harmful elements and deliver 100% sanitized versions within seconds.

Anti-bot
Protection against bot-driven infections and sensitive data exposure.

Automated post-breach detection, remediation an response
Automation-driven analysis, contextualization, and remediation of incidents, along with an end-to-end attack view, covering entry points, lateral movement, and the impact to the business.

Take a 5-minute security assessment to find out how strong is your endpoint security.

CHECK POINT HARMONY ENDPOINT

Protect the endpoint from all imminent threats

Harmony Endpoint is a complete endpoint protection (EPP) and endpoint detection and response (EDR) solution that delivers the five pillars of robust protection for keeping remote users safe.

Complete Endpoint Protection

Protect against ransomware, phishing, bots, file-less attacks, or malware coming from web browsing or email attachments and more.

Fastest Recovery

Automating 90% of attack detection, investigation, and remediation tasks.

Best TCO

All the endpoint protection you need in a single, efficient, and cost-effective solution.

MITRE ENGENUITY™

AV TEST av-test.org 10/2020 APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT

MITRE ATT&CK® Evaluations Highlight Check Point Software Leadership in Endpoint Security.

Learn more

Harmony Endpoint recognized as a Top Product in Corporate Endpoint Protection by AV-TEST

Learn more

Must-Have #2

SECURE INTERNET ACCESS

> “100,000 new malicious websites were discovered every day during 2020”
>
> (Check Point Research)

Working outside the corporate firewall exposes users to a whole slew of internet-based threats that would otherwise be blocked at the network level. Remote workers may unintentionally put their organizations at risk by unwittingly downloading infected files and visiting phishing sites where corporate credentials are stolen.

As over 10,000 new malicious files and 100,000 new malicious websites are discovered by Check Point every single day, preventing threats from ever reaching users becomes critical, with retroactive detection and mitigation often proving to be too little too late.

So, how do you preemptively protect remote users as they access the internet for work and personal use and prevent the latest phishing and malware attacks?

Six principles for selecting a secure internet access solution

When selecting a solution for assuring secure internet access, there are six principles that should be top of mind:

Complete protection
Against phishing, malicious downloads and websites, data loss, ransomware, browser exploits, among others.

Future-proof security
Advanced security technologies that can block never seen before malicious files and phishing attacks.

A seamless user experience
Block internet-based attacks with minimal impact on user browsing experience and speed.

Scale and simplicity
Avoid backhauling traffic through the data center by adopting a global cloud-based security service, or even better - by implementing security directly in the browser.

Privacy
Keep users’ browsing history private to ensure compliance with GDPR and other data protection regulations.

100% traffic inspection
Ensure that all the traffic can be inspected, including SSL and new HTTP protocol versions.

Take a 5-minute security assessment to find out how robust is your internet access security.

CHECK POINT HARMONY FOR SECURE INTERNET ACCESS

A revolution in internet access security

Check Point Harmony delivers on the six principles of secure internet access. It provides remote users with the fastest and safest browsing experience, and complete protection from all internet-based threats, including: malicious downloads prevention, real-time phishing protection, URL filtering, data loss prevention (DLP), browser exploit prevention, and corporate credential reuse prevention

The offering is available in two deployment options with:

Harmony Connect

HARMONY CONNECT INTERNET ACCESS

A cloud-based secure web gateway service that deploys within minutes and makes it easy for remote users and branch offices to securely access the internet, with zero impact on their browsing experience.

Harmony Browse

HARMONY BROWSE

Unique in-browser protection providing secure, fast, and private web browsing by inspecting all SSL traffic directly on the endpoint without adding latency or re-routing traffic through a secure web service. It deploys quickly as a nano-agent within browsers and can be combined with any secure web gateway or endpoint security solution to enhance overall protection.

Must-Have #3

ZERO TRUST NETWORK ACCESS (ZTNA) TO CORPORATE APPLICATIONS

Remote employees can't do their job without access to their corporate applications. And to make sure they maintain enhanced productivity (even when away from the office) they need easy access from any device, be it a mobile phone, home PC, or other device.

While fast access is mandatory, it is also critical to be able to vet each user before they access the network and sensitive enterprise apps, whether hosted on-prem or in the cloud.

Traditionally, organizations have relied on VPN-based security to achieve the task and then provide users with broad network access once authenticated. This approach is no longer viable.

Today, it is necessary to secure a continually shifting attack surface and to have visibility into what users are actually doing.

This is why protection today requires a zero-trust architecture that enables administrators to eliminate the risk of unauthorized access and prevent lateral movement within the network.

6 principles for choosing the optimal ZTNA solution

When embarking on the path to zero-trust access, it is important to adhere to the following six principles and to make sure that the solution you choose enables their implementation:

Consider all users
Deliver zero-trust access across the entire organization, including third parties such as partners and contractors, while providing support for web applications, databases, remote desktops, and SSH remote terminals.

Client and clientless remote access
Choose a solution that offers both deployment methods as well as the ability to securely scale remote access within minutes.

User experience
Choose a strategy and products that create the most frictionless and SaaS-like experience for the team.

Least privilege access policy
A particular user should only be granted just enough privileges to allow them to complete a particular task. For example, an engineer who only deals with updating lines of legacy code does not need to access financial records.

Multi-factor authentication (MFA)
Strictly verify the identity of every user accessing the network using multiple factors. Ensure these factors can be adjusted depending on the sensitivity of the data/resources being accessed.

Monitor and audit everything
Monitor and review all user activity across the network to identify any suspicious activity in real time.

Take a 5-minute security assessment to better understand how secure is your organization's remote corporate access.

CHECK POINT HARMONY CONNECT REMOTE ACCESS

The easiest way to secure corporate access

Harmony Connect Remote Access makes it easy to connect any user to any enterprise application, without compromising on security. Built to prevent the most advanced cyberattacks, Harmony Connect Remote Access is a cloud-based service that deploys in five minutes and applies zero-trust policies with a seamless user experience.

Harmony Connect offers the flexibility to choose between

Clientless access
Provides employees and contractors secure and easy access to enterprise applications through a web browser from any device (even unmanaged mobile and home PCs).

Client-based access (coming soon)
Utilizes a VPN agent to provide full network-layer access to corporate networks and applications for managed devices.

Must-Have #4

EMAIL & OFFICE SECURITY

In today's modern business world, no employee, remote or otherwise, can be productive without access to email and productivity apps, such as Office 365, Teams, SharePoint, One Drive, Gmail, Google Drive, and more. These tools are not only critical for getting things done. They are also one of the channels most exploited by hackers, with business email compromise (BEC) attacks, for example, accounting for over 50% of losses caused by cybercrime.

The 5 key protections for email and office

Real-time phishing protection
That is fully automated and AI-based to prevent advanced never before seen phishing and spear phishing attacks before they happen.

Malware protection
With CDR (content disarm and reconstruction) to deliver clean attachments and files in seconds, while blocking evasive malware through AI-based static and dynamic file analysis.

Data leak prevention
That enables custom policies to be set to specific needs and which automatically blocks sensitive outbound information on email and collaboration apps.

Internal threat prevention
To scan and block threats originating in emails from inside the corporate network, and to prevent lateral movement.

All around security in a one-stop-shop
To ensure easy to manage total security and to reduce operational complexity.

Take a 5-minute security assessment to find out how secure is your organization's email and collaboration apps.

CHECK POINT HARMONY EMAIL & OFFICE

The new era of email & collaboration apps security

Harmony Email & Office protects users from all imminent threats to cloud and on-prem mailboxes and collaboration apps. On top of providing robust security, Harmony Email & Office offers operational simplicity with an easy to deploy, manage and use platform.

Among the key benefits of the solution are:

Complete protection
Protect email and collaboration apps from phishing, malware, malicious links, and sensitive data loss.

The highest level of security
By available today with a 99.8% block rate* for phishing and malware.

Simple to deploy and manage
A cloud-based solution that deploys in minutes with out-of-the-box configuration, intuitive web UI, and a single platform for all security functionality.

*According to internal test against 10 competing vendors

Must- Have #5

MOBILE THREAT DEFENSE (MTD)

> **Almost every organization experienced a mobile-related attack in 2020, with 46% of organizations having at least one employee download a malicious mobile application.**
>
> (Check Point 2021 Mobile Security Report)

Protecting corporate mobile devices has never been easy. App stores contain many malicious apps, it is more difficult to spot suspicious email contents and attachments when they come in on mobile, and phishers often exploit vulnerabilities that are specific to mobile apps and for which filters often do not exist.

But the challenge is now greater than ever. The mass mobilization of the global workforce to the home means that remote employees are accessing corporate data from mobile devices more than ever, often over public WiFi networks that are easy to compromise, sending more emails, messaging more often, and sharing more files than ever.

In fact, over the past year, researchers at Check Point have been observing a rise in the number of mobile-related attacks as well as entirely new attack methods such as sophisticated mobile ransomware and MDMs getting weaponized to attack organizations.

In 2020 alone, 97% of organizations faced mobile threats that used various attack vectors, and 46% of organizations had at least one employee download a malicious mobile application.

5 principles of the optimal mobile security

360° protection of all attack vectors
Including malicious mobile applications, network-based attacks, and vulnerable operating systems and devices.

Full visibility into the risk level
With a complete view of the organization's mobile security posture to effectively mitigate risk and accelerate response when needed.

Scalable deployment
With support for every device type, operating system, and device-ownership model.

Maximizing the user experience
By avoiding impact on device usability, the browsing experience, data consumption, and battery life.

Ensuring privacy by design
Of both corporate and BYOD devices.

Take a 5-minute security assessment to find out how secure is your mobile workforce.

CHECK POINT HARMONY MOBILE

The industry's leading mobile threat defense solution

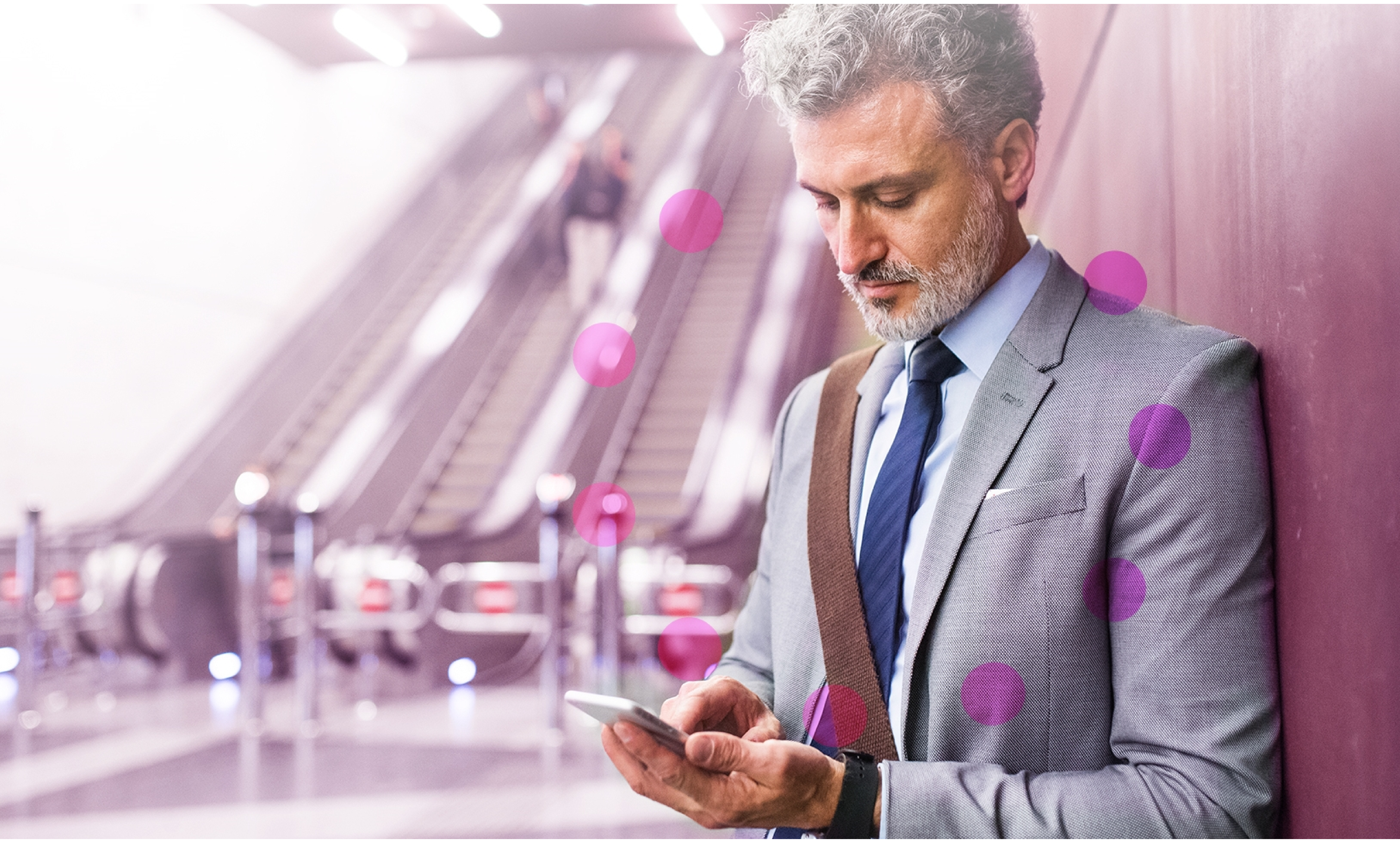
Harmony Mobile keeps corporate data safe by securing the mobile devices of employees across every attack vector, including the network, apps, and operating system. Designed to reduce admin overhead and increase user adoption, it fits perfectly into the existing mobile environment, deploys and scales quickly, and protects devices without impacting user experience nor privacy.

Complete protection
Across all attack vectors: apps, network and OS

Simple Management
Scalable and easy-to-manage security for any mobile workforce

User-Friendly
Quick user adoption with zero impact on user experience or privacy

Harmony Mobile Named a Leader in the IDC 2020 MarketScape for Mobile Threat Management



THE VALUE OF SECURITY CONSOLIDATION

Implementing the five must-have protections for remote users is a good start to securing the new ‘work from anywhere’ hybrid environment. But this can be very challenging as it requires endless protections across devices, networks, access points, and applications.

Some organizations attempt to overcome the challenge by stitching together point solutions with APIs or opting for best of breed solutions.

These approaches, however, mean complex management, and leave many security gaps untreated, where the organization has fragmented visibility at best, and is limited in its options to scale.

To keep corporate networks and sensitive data safe, organizations have no option but to recalibrate the security approach around remote users and access.

The key to overcoming the challenge is to consolidate the various security solutions into one unified solution.

CHECK POINT HARMONY: The industry's first unified security solution for users, devices and access

Harmony protects remote devices and internet connections from the most sophisticated attacks while ensuring Zero-Trust Access to corporate applications, all in a single solution that is easy to use, manage and buy. By consolidating six different security products, Harmony provide multi-layered protection for remote users against known and zero-day attacks and across all threat vectors.

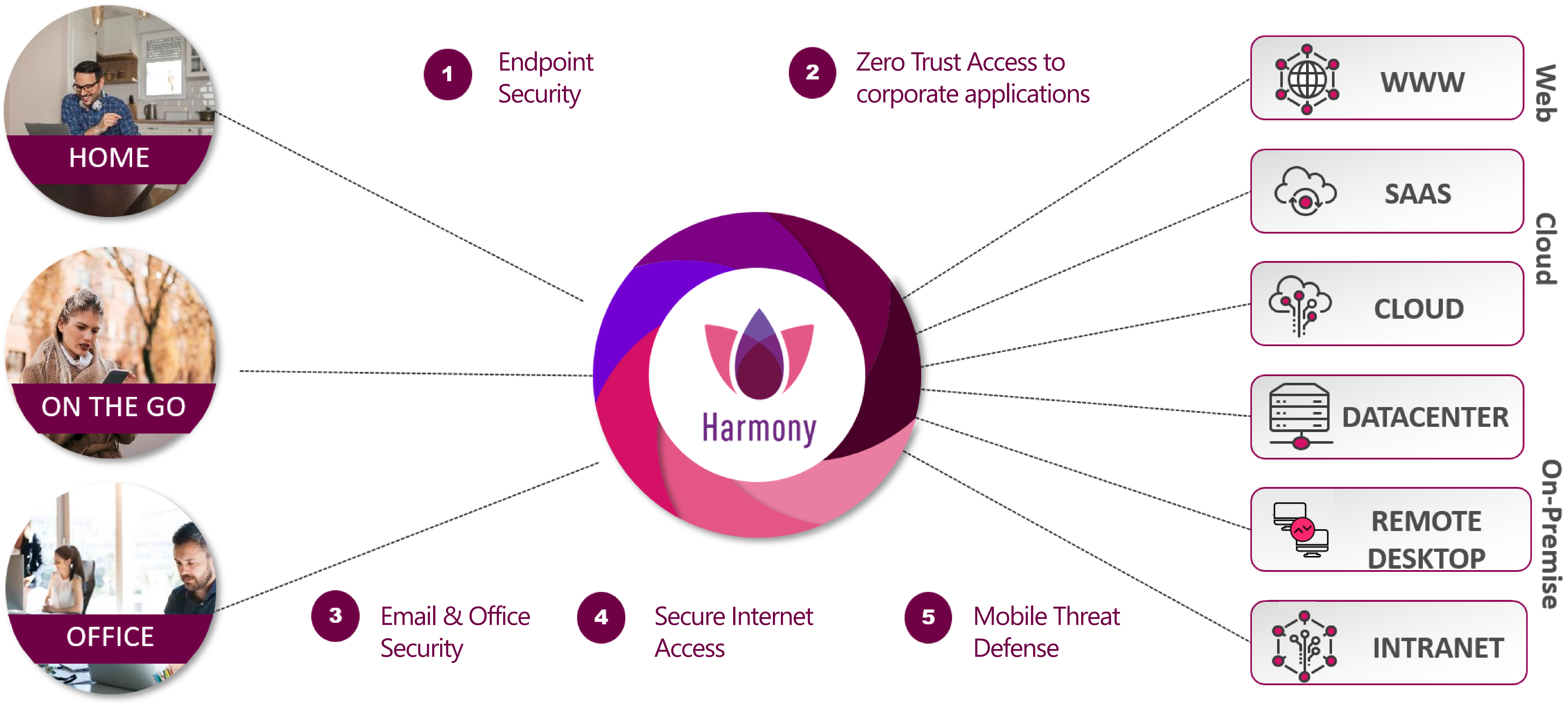


Figure 2:
Check Point Harmony delivers the 5 must have protections for remote users in a single solution

Unified cloud-based management: deploy, configure, and manage from a single portal

Each of the Harmony products are integrated and managed through Check Point's Infinity Portal, which provides unified policy management, and event management dashboard. All logs and security events are stored in the Infinity Portal's cloud-native big data platform, enabling vast amounts of data to be quickly searched and analyzed, providing unified visibility of malicious activity across Harmony solutions.

Easy to buy, deploy, and manage

Harmony offers an alternative that saves the overhead as security is increased. By consolidating six security products for complete user and access protection it is easy to use.

With unified and intuitive cloud-based management and by enabling user-centric security policies to be applied across the organizations' environments, it is easy to manage. And it is easy to buy with a simple and all-inclusive per-user subscription pricing model.

Powered by Check Point's ThreatCloud

Harmony is powered by Check Point's ThreatCloud, which delivers real-time threat intelligence that is derived from hundreds of millions of sensors worldwide. This intelligence is enriched with AI-based engines and exclusive research data from the Check Point Research Team.

ThreatCloud detects 2,000 attacks daily by unknown threats previously undiscovered and enables zero-day protection, delivering up-to-minute information on the newest attack vectors and hacking techniques.

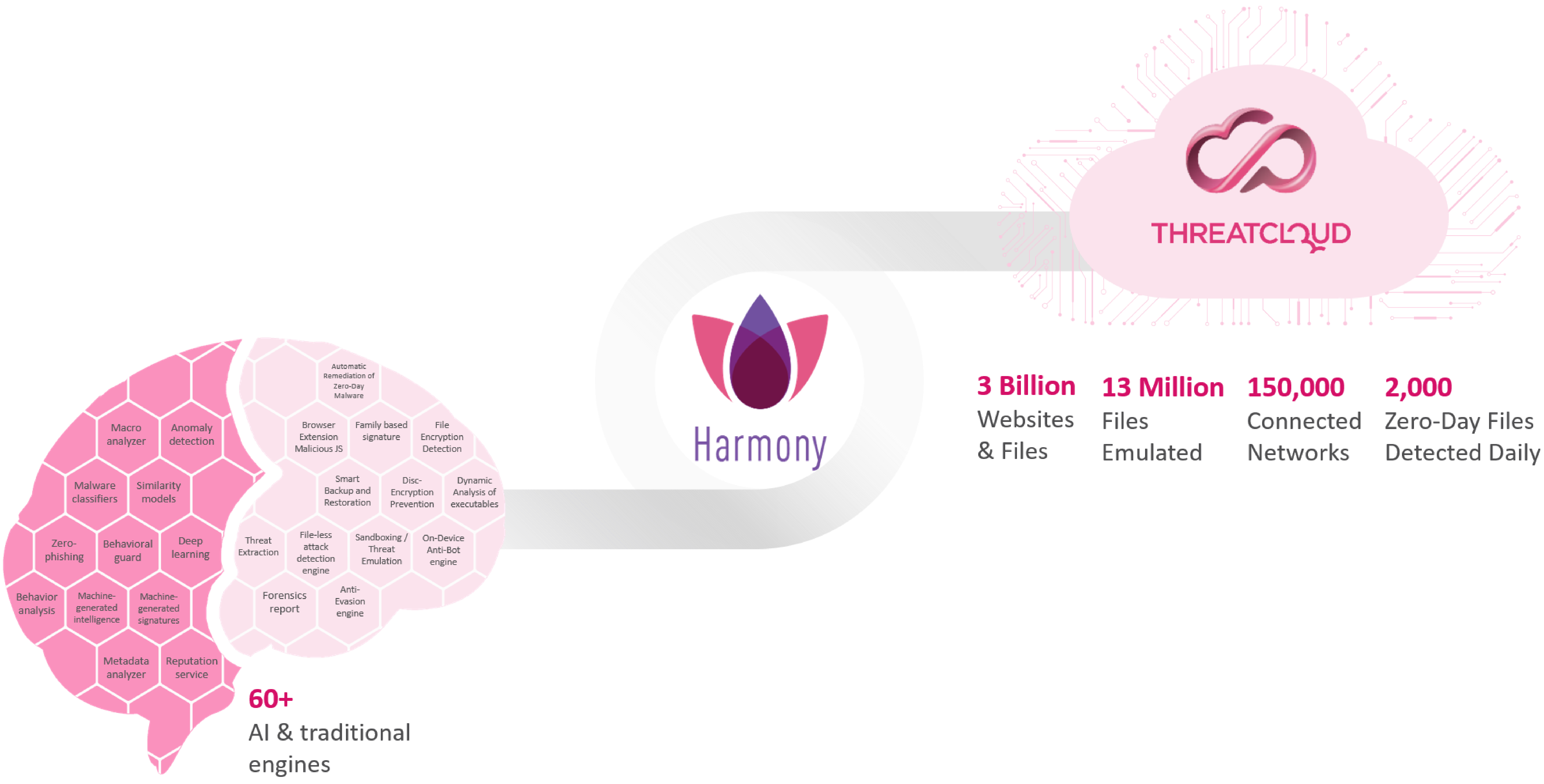
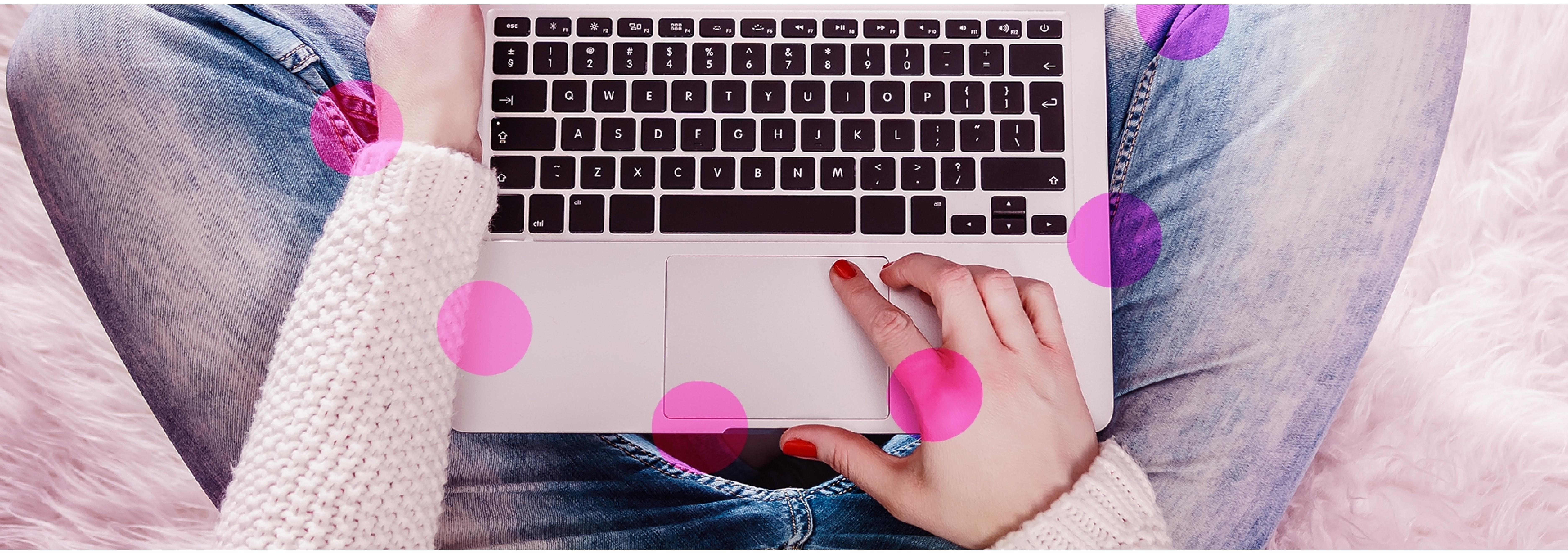

THREATCLOUD
Harmony
3 Billion Websites & Files
13 Million Files Emulated
150,000 Connected Networks
2,000 Zero-Day Files Detected Daily
Automatic Remediation of Zero-Day Malware
Macro analyzer
Anomaly detection
Browser Extension Malicious JS
Family based signature
File Encryption Detection
Malware classifiers
Similarity models
Smart Backup and Restoration
Disc-Encryption Prevention
Dynamic Analysis of executables
Zero-phishing
Behavioral guard
Deep learning
Threat Extraction
File-less attack detection engine
Sandboxing / Threat Emulation
On-Device Anti-Bot engine
Behavior analysis
Machine-generated intelligence
Machine-generated signatures
Forensics report
Anti-Evasion engine
Metadata analyzer
Reputation service
60+ AI & traditional engines

Figure 3:
Check Point Harmony provides the industry's best zero-day protection powered by the world's most powerful treat intelligence and 60+ security engines.

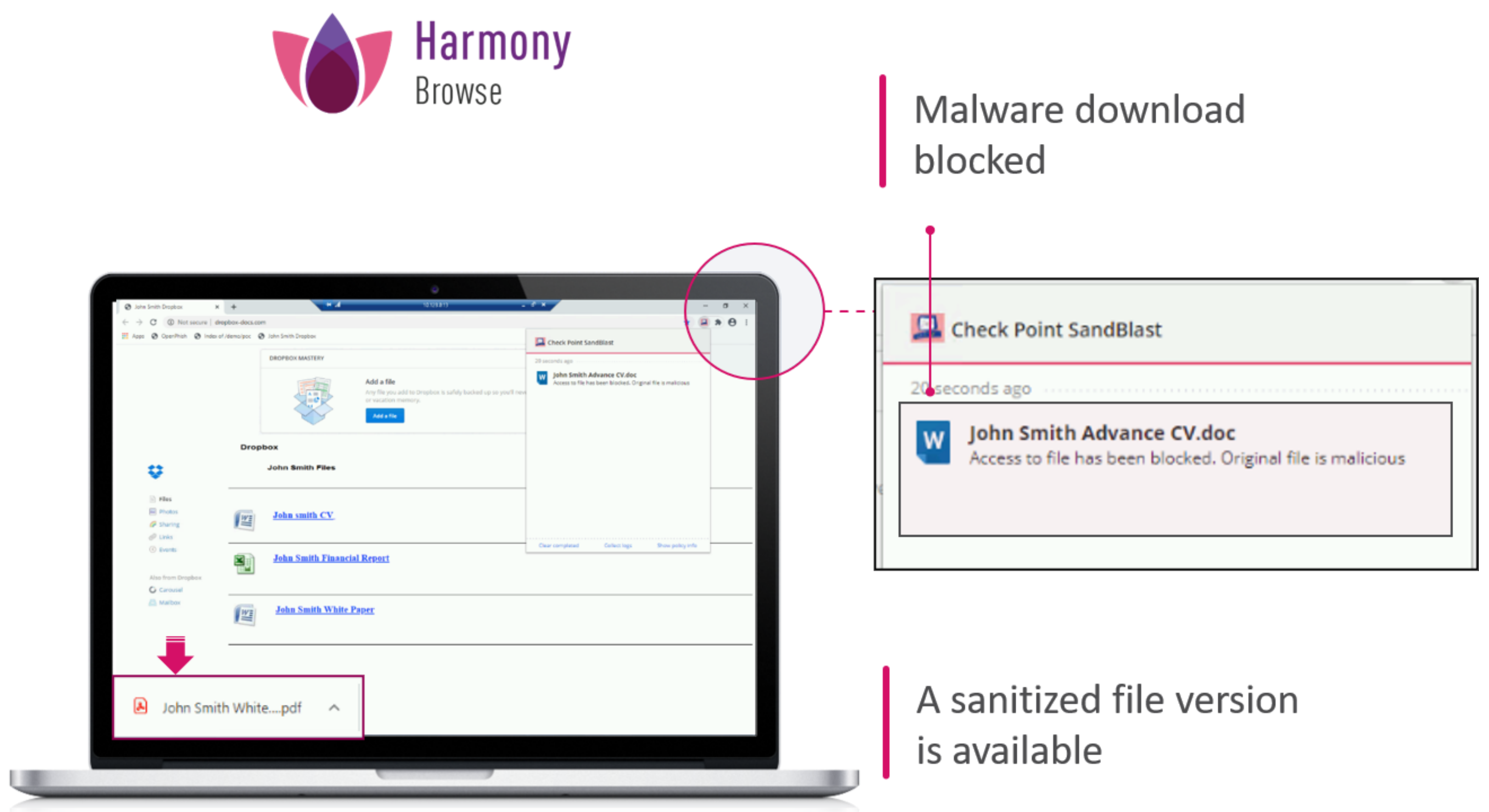


CHECK POINT HARMONY IN ACTION

360° malware protection

> **Since we deployed Harmony Endpoint, we have not had a single advanced malware or ransomware incident in almost a year.**
>
> Russell Walker, Chief Technology Officer, Mississippi Secretary of State

Users often access malicious files containing malware masquerading as seemingly legitimate and harmless files. For example, the file could be one that was uploaded to the organization's jobs section on its website, appearing to be the resume of an applicant.



Check Point SandBlast

20 seconds ago

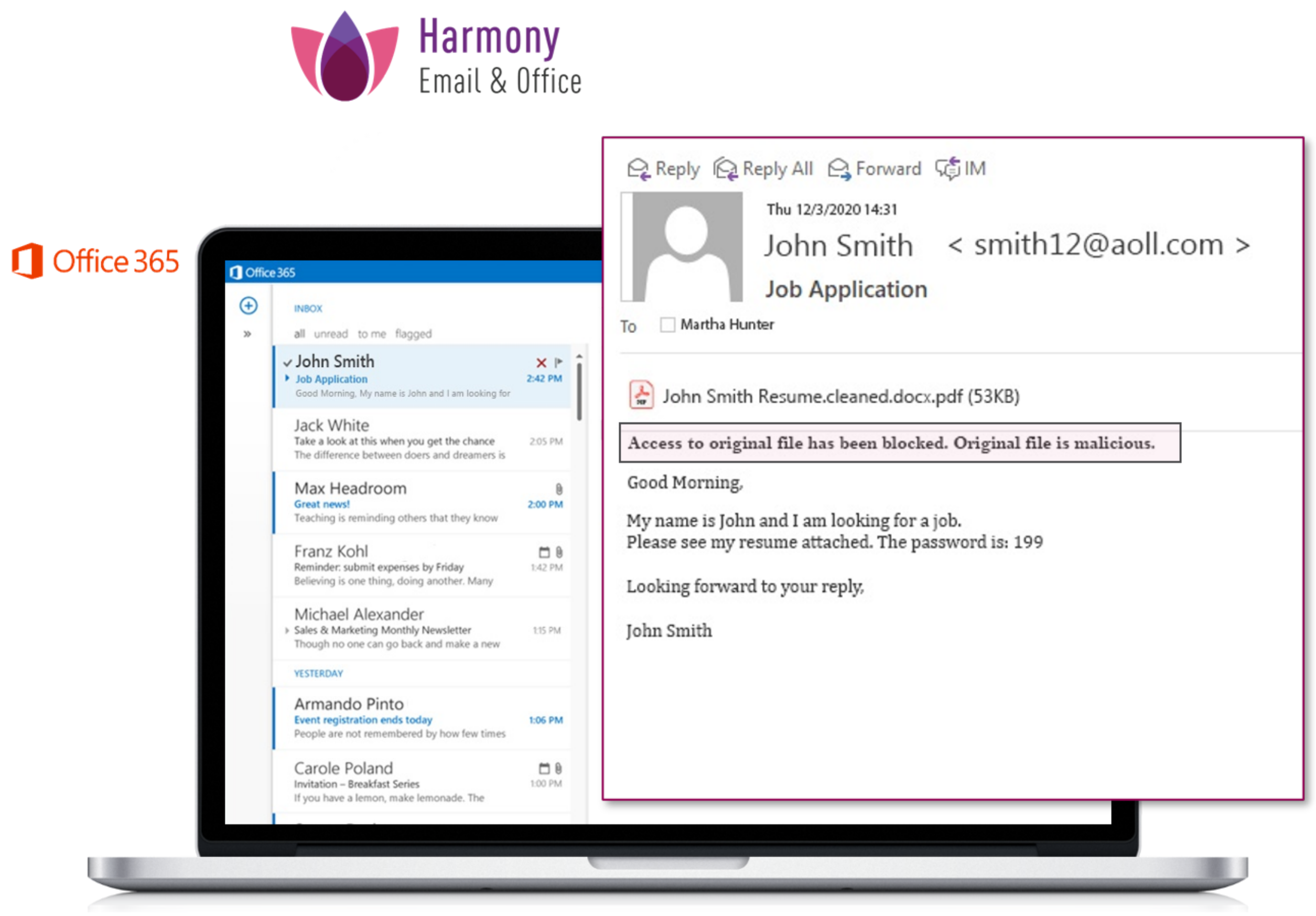
John Smith Advance CV.doc

Access to file has been blocked. Original file is malicious

In such cases, **Harmony Browse**, which uses the industry-leading Content Disarm and Reconstruction (CDR) technology, delivers a sanitized version of web-downloaded files in seconds.

In parallel, SandBlast, Check Point's sandboxing technology, analyzes the file in a virtual environment to proactively prevent the zero-day, never seen before malicious file from reaching a talent acquisition team member.

At the same time, this same malicious file may arrive at a talent acquisition professional's Office 365 mailbox. In this case, **Harmony Email & Office** also leverages SandBlast to block the malicious content before it even reaches the targeted mailbox. Instead, the solution provides a sanitized version of the email attachment within two seconds, eliminating any potential threat.



Thu 12/3/2020 14:31

John Smith < smith12@aoll.com >

Job Application

To □ Martha Hunter

John Smith Resume.cleaned.docx.pdf (53KB)

Access to original file has been blocked. Original file is malicious.

Good Morning,

My name is John and I am looking for a job.
Please see my resume attached. The password is: 199

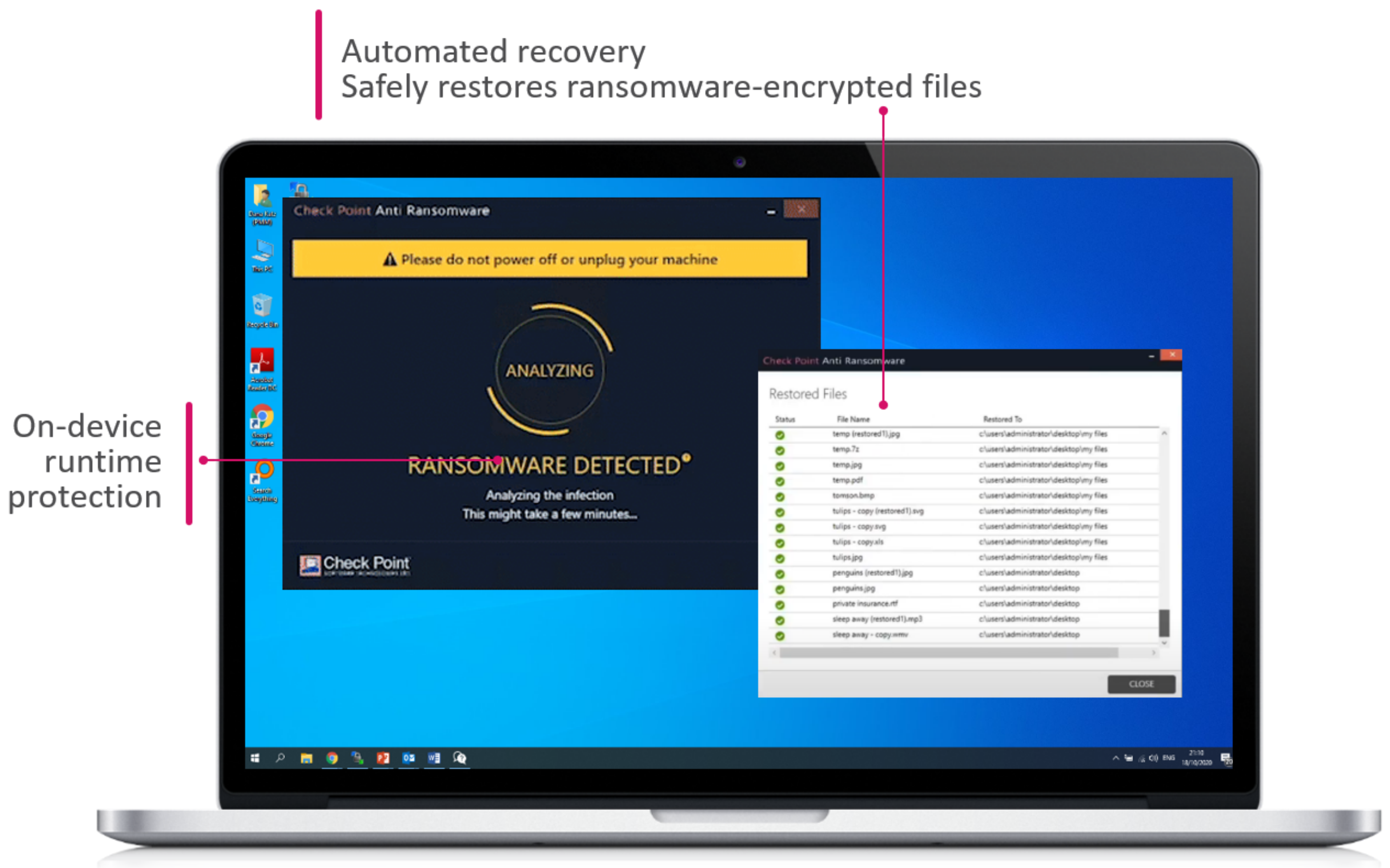
Looking forward to your reply,

John Smith

Should a particularly evasive zero-day malware make it through to a user's device, **Harmony Endpoint** provides runtime protection against ransomware and malware with post breach detection and response and instant and automated remediation, even in offline mode.

Once an anomaly or malicious behavior is detected, Check Point's Endpoint Behavioral Guard blocks and remediates the full attack chain without leaving malicious traces. Furthermore, anti-ransomware capabilities identify ransomware behaviors such as files encrypting or attempts to compromise OS backups, and safely and automatically restores ransomware-encrypted files.

Harmony Endpoint



Automated recovery
Safely restores ransomware-encrypted files

On-device runtime protection

Check Point Anti Ransomware

⚠ Please do not power off or unplug your machine

ANALYZING

RANSOMWARE DETECTED

Analyzing the infection
This might take a few minutes...

Check Point

Check Point Anti Ransomware

Restored Files

Status	File Name	Restored To
✓	temp (restored1).jpg	c:\users\administrator\desktop\my files
✓	temp.7z	c:\users\administrator\desktop\my files
✓	temp.jpg	c:\users\administrator\desktop\my files
✓	temp.pdf	c:\users\administrator\desktop\my files
✓	tomson.bmp	c:\users\administrator\desktop\my files
✓	tulips - copy (restored1).svg	c:\users\administrator\desktop\my files
✓	tulips - copy.svg	c:\users\administrator\desktop\my files
✓	tulips - copy.xls	c:\users\administrator\desktop\my files
✓	tulips.jpg	c:\users\administrator\desktop\my files
✓	penguins (restored1).jpg	c:\users\administrator\desktop
✓	penguins.jpg	c:\users\administrator\desktop
✓	private insurance.rtf	c:\users\administrator\desktop
✓	sleep away (restored1).mp3	c:\users\administrator\desktop
✓	sleep away - copy.wmv	c:\users\administrator\desktop

Furthermore, **Harmony Mobile** prevents users from downloading malicious apps onto their mobile device, and **Harmony Connect** enables the organization to define and enforce a zero-trust policy with granular rules for all users and all applications, to ensure that users gain access only to the apps they are authorized to use, and that malicious lateral movement is prevented.

360° phishing protection

Properly securing remote users and valuable corporate data against phishing can be extremely challenging, with attacks being multi-layered and ever evolving. But with 90% of cyberattacks starting with a phishing campaign, no organization can afford not to take on the challenge.

With Check Point Harmony, remote users are protected against the risks of phishing, including phishing websites, social engineering attacks through emails or collaboration apps, and phishing SMS (smishing).

Harmony phishing protection is driven by:

Harmony Endpoint

Which identifies and blocks the use of phishing sites in real time. Sites are inspected and if found malicious, the user is blocked from entering their credentials. Zero-phishing even protects against previously unknown phishing sites and corporate credential re-use.

Harmony Email & Office

Which protects users from advanced phishing and other social engineering attacks on cloud and on-prem mailboxes, as well as collaboration apps such as Teams, OneDrive, SharePoint, and Google Drive.

Harmony Mobile

Which keeps corporate data safe by securing employees' mobile devices across all attack vectors, including apps, network, and OS, blocking access to phishing sites, even those never seen before.

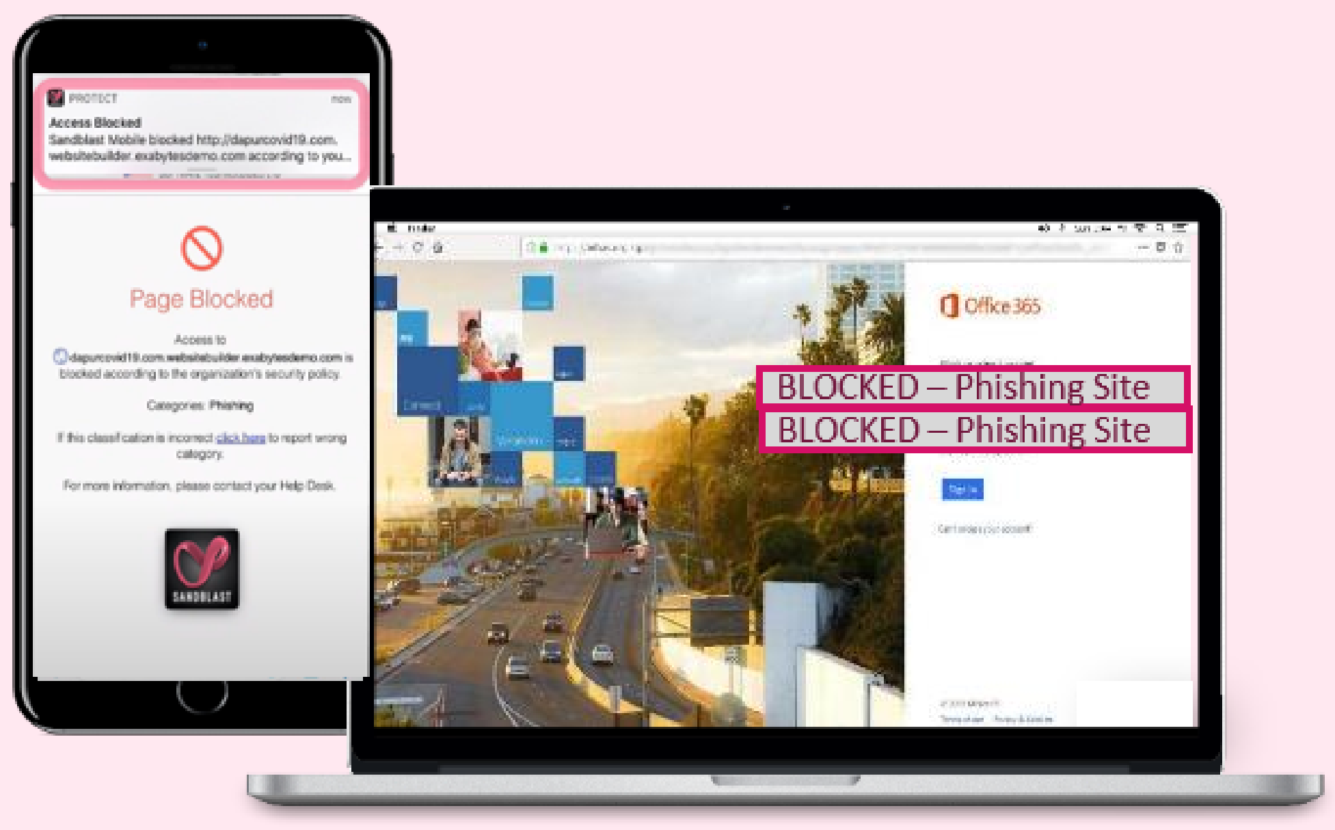
Harmony Browse

Which provides secure, fast, and private web browsing by inspecting all SSL traffic directly on the endpoint, blocking access to phishing websites and preventing the reuse of corporate passwords.

Harmony Connect Internet Access

For enabling secure access to the internet for remote users and branch offices, without impacting the browsing experience.

Prevent access to phishing sites
Even those never seen before



PROTECT now
Access Blocked
Sandblast Mobile blocked http://dapurcovid19.com.websitebuilder.exabytesdemo.com according to you...

Page Blocked

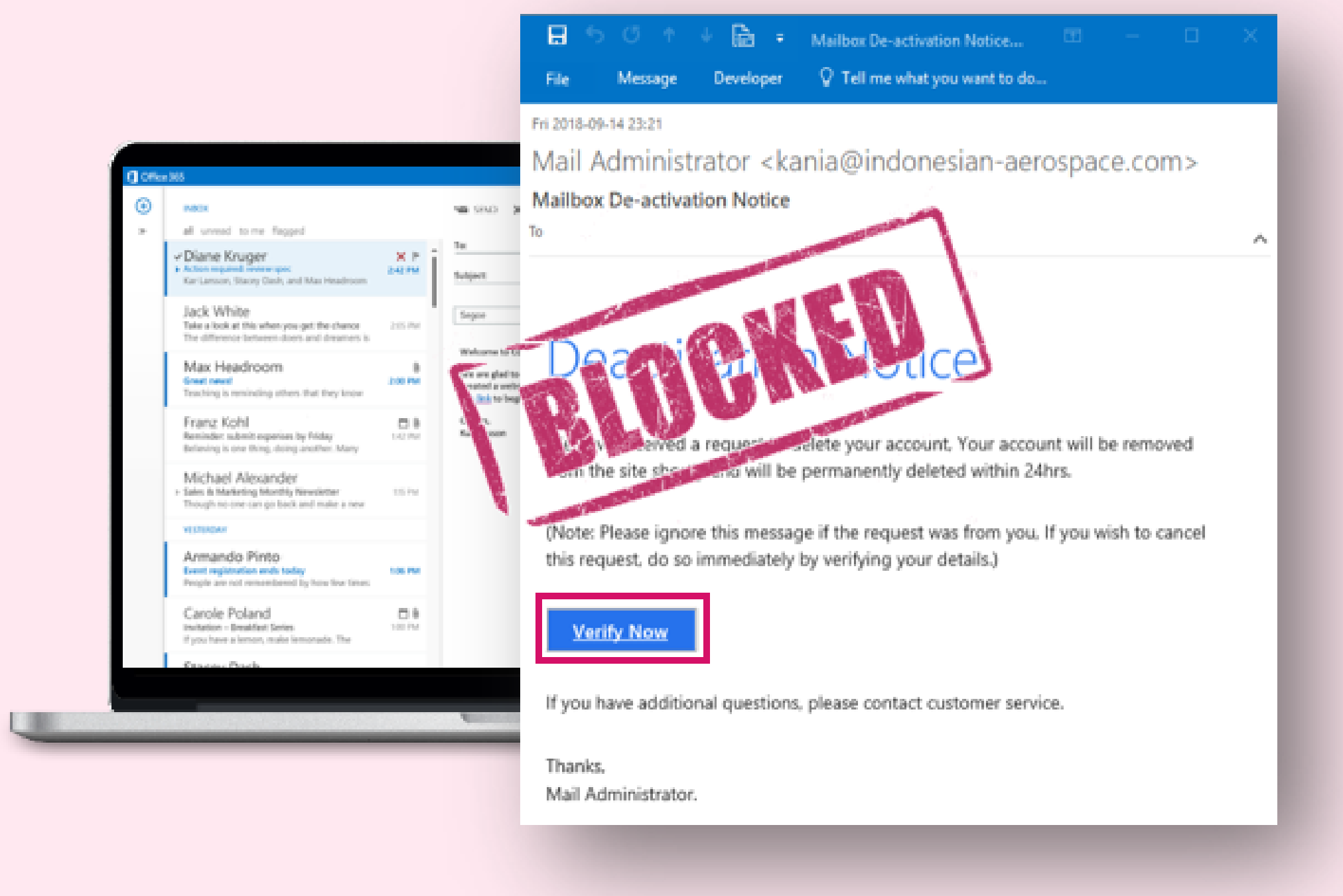
Access to dapurcovid19.com.websitebuilder.exabytesdemo.com is blocked according to the organization's security policy.

Categories: Phishing

If this classification is incorrect click here to report wrong category.

For more information, please contact your Help Desk.

Block phishing emails before they reach users



Mailbox De-activation Notice...

Fri 2018-09-14 23:21
Mail Administrator <kania@indonesian-aerospace.com>
Mailbox De-activation Notice
To

De[illegible] Notice

[illegible]ved a reque[illegible]elete your account. Your account will be removed [illegible] the site sh[illegible] will be permanently deleted within 24hrs.

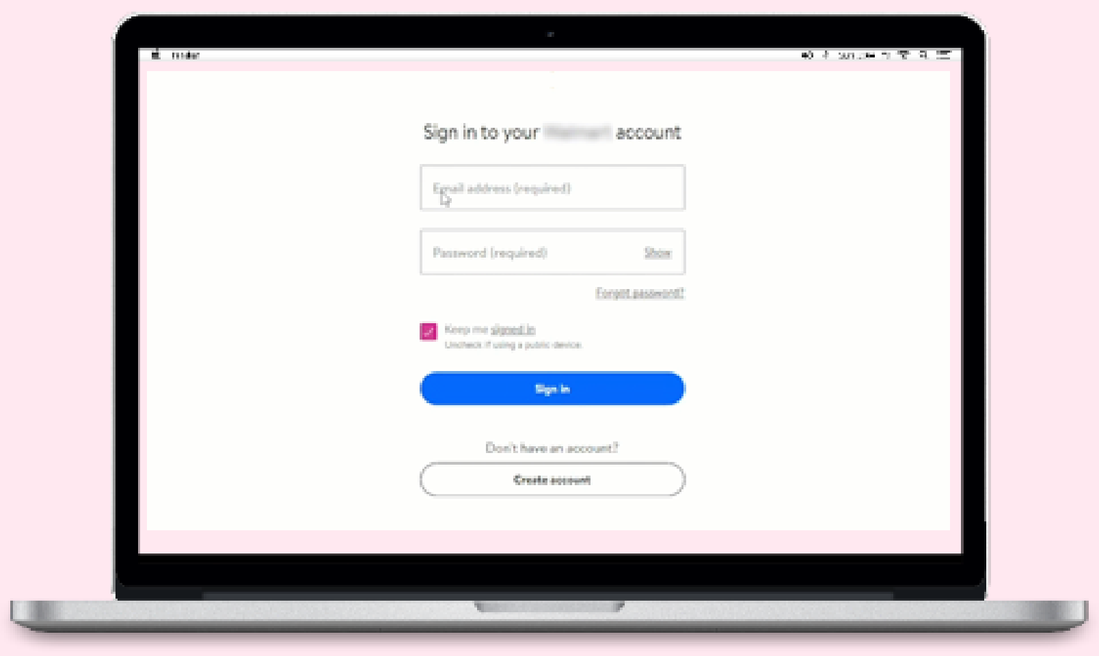
(Note: Please ignore this message if the request was from you. If you wish to cancel this request, do so immediately by verifying your details.)

Verify Now

If you have additional questions, please contact customer service.

Thanks,
Mail Administrator.

Prevent corporate password exposure



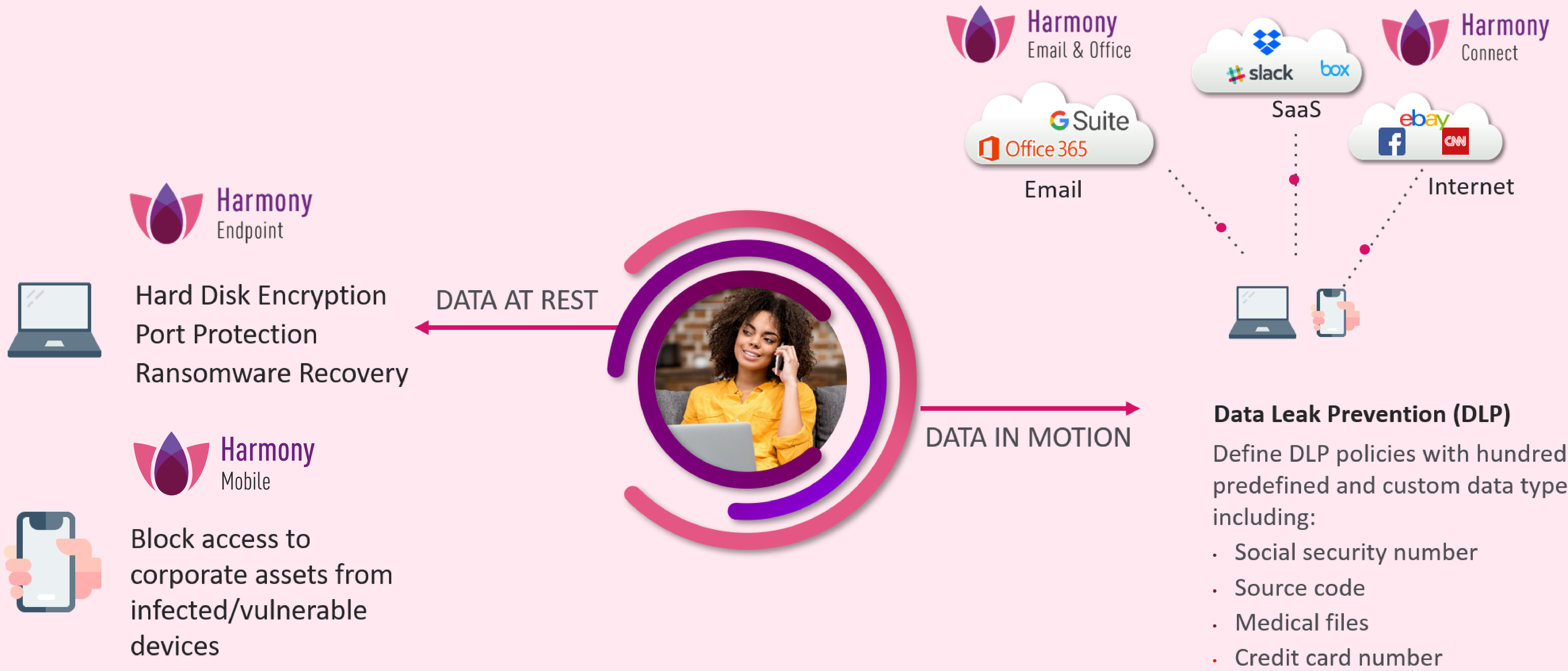
360° data protection

Harmony offers 360-degree data protection of sensitive data wherever it resides, regardless of whether it is at rest or in motion.

When data is at rest, i.e., on the device Harmony Endpoint minimizes the attack surface with full disk encryption and port protection. It also immediately recovers ransomware-encrypted data. And Harmony Mobile blocks any access to corporate assets should the device be vulnerable or is infected.

When it comes to data in motion, Harmony Email & Office prevents data loss with a data loss prevention for Office 365 and Google Workspace. And Harmony Connect prevents users from unintentionally leaking sensitive business data while they are browsing or using SaaS applications.

Harmony Connect also protects against shadow IT by identifying whether users are using unauthorized SaaS accounts, such as Slack, Teams, or Gmail, and blocks them from sending sensitive data over these applications.



Data Leak Prevention (DLP)

Define DLP policies with hundreds of predefined and custom data types, including:

- Social security number
- Source code
- Medical files
- Credit card number
- Bank account

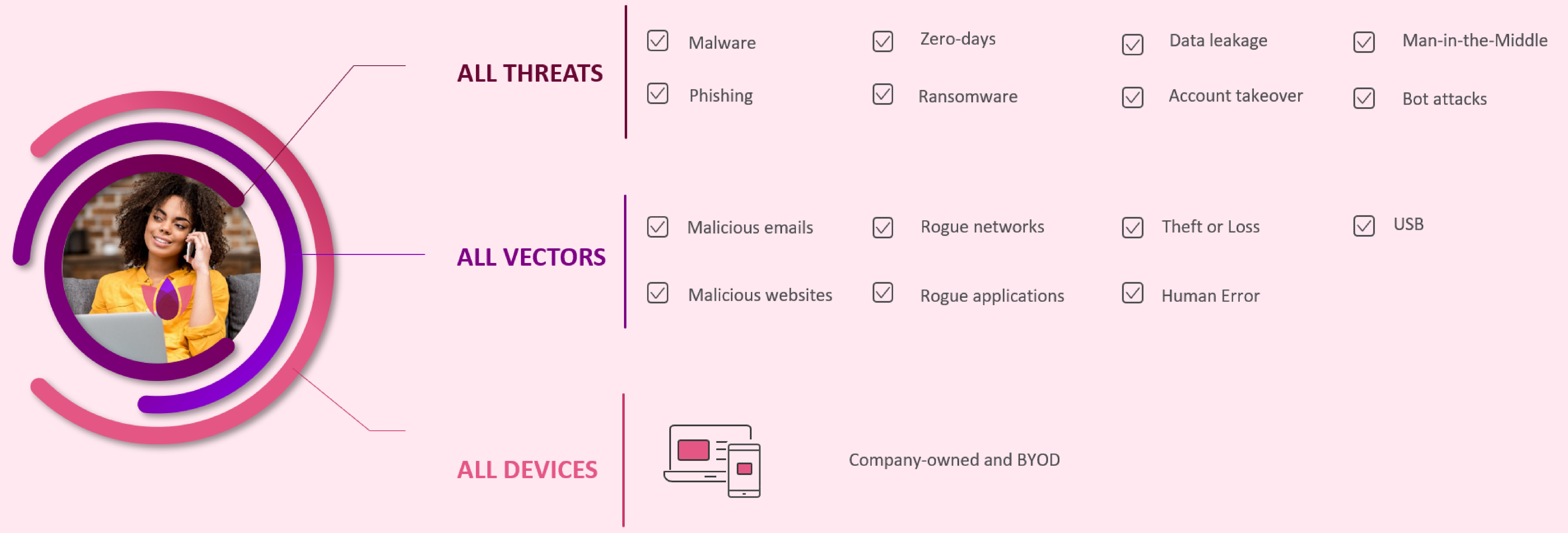
IN CONCLUSION

Remote work is here to stay and so are the threats to remote users. Protecting today's hyper-distributed workspace can be very challenging, requiring endless security functions across user devices, applications, and networks.

Check Point Harmony overcomes the challenge by offering the industry's first unified security solution for users, devices, and access. By consolidating the five must-have remote user protections, the solution is simple to buy, use, and manage. And most importantly, wherever they connect from, whatever users connect to, and however they connect, their home, devices, and privacy, as well as the organization's data are all secured and protected against phishing attempts, malicious email attachments, zero-day ransomware, and any other cyber threats.

Experience the new harmonious, hybrid workspace yourself. To get started, learn more about Harmony, or sign up for a first hand look.

Take a 5-minute security assessment to find out how secure is your remote workforce.



ALL THREATS

☑ Malware
☑ Phishing
☑ Zero-days
☑ Ransomware
☑ Data leakage
☑ Account takeover
☑ Man-in-the-Middle
☑ Bot attacks

ALL VECTORS

☑ Malicious emails
☑ Malicious websites
☑ Rogue networks
☑ Rogue applications
☑ Theft or Loss
☑ Human Error
☑ USB

ALL DEVICES

Company-owned and BYOD

Figure 4: Check Point Harmony
360° user protection against known and zero-days threats

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Check Point Infinity´s portfolio of solutions protects enterprises and public organizations from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other threats. Infinity comprises three core pillars delivering uncompromised security and generation V threat prevention across enterprise environments: Check Point Harmony, for remote users; Check Point CloudGuard, to automatically secure clouds; and Check Point Quantum, to protect network perimeters and datacenters, all controlled by the industry's most comprehensive, intuitive unified security management. Check Point protects over 100,000 of all sizes.