CHECK POINT

OTD BİLİŞİM
GLOBAL VAD

Products & Security Platform Overview

YOU DESERVE THE BEST SECURITY

Agenda

Check Point Platform Vision

Check Point Product Families

Use Cases

OTD BİLİŞİM
GLOBAL VAD

CEO priorities for 2024

McKinsey & Company

1. **Gen AI: The start of something big**
2. Outcompeting with technology
3. The energy transition
4. What's your superpower?
5. **Learn to love middle managers**
6. Geopolitics: beating the odds
7. Navigating the road to courageous growth
8. A new lens on the macroeconomy

Most important business risks for 2024

Allianz

1. **Cyber incidents**
2. Business interruptions
3. Natural catastrophes
4. Changes in legislation and regulation
5. Macroeconomic developments
6. Fire, explosion
7. Climate change
8. Political risks and violence
9. Market developments
10. Shortage of skilled workforce

OTD BİLİŞİM
GLOBAL VAD

Immediate impact of AI on cyber security

Who will AI help?

Attackers	**55.9%**
Both	35.1%
Defenders	8.9%

OTD BİLİŞİM
GLOBAL VAD

AI requires cyber security investment

Infra-structure Security	Identity and Access Mgmt	Data Security	Application Security	Logging and Monitoring	AI Security
Posture	MFA	Encryption at Rest	Architecture Review	Cloud Audit Logs	24x7 SOC Monitoring
Workload	RBAC	Encryption in Transit	Threat Modeling	Collect Logs and Event Management	Appropriate Staffing
Vulnerability	Least Privilege	DLP	Application Security Testing		Threat Hunting
Virtual Network	Human and service accounts	Secret/Key Management	PEN Testing		Forensics
Host Security					
Firewall					

Platform: THE cyber security priority

Cyber leaders should:

- Simplify and rationalize cyber security
- Establish the **PLATFORM** for seamless operations at speed

A platform for consolidation – that works

Collaborative, unified, best threat prevention

AI in action – TODAY!

Commercial flexibility and agility

Infinity

Platform

OTD BİLİŞİM
GLOBAL VAD

Check Point Infinity Platform

AI-Powered. Cloud-Delivered.

OTD BİLİŞİM
GLOBAL VAD

SECURE THE **ENTERPRISE**

AI-Powered. Cloud-Delivered.

Infinity Platform

SECURE THE **NETWORK**

Quantum

Maestro
Hyperscale Data Center

VPN
Virtual Private Remote Access

Gateways
Enterprise Firewalls

SD-WAN
Optimized Connectivity

Spark
SMB Suite

Rugged
ICS Security

DDoS Protector
Block DDoS Attacks

IoT Protect
IoT Security

Smart-1 Cloud
Security Management

SECURE THE **CLOUD**

CloudGuard

Network
Cloud Access Control and Prevention

WAF
Web Application Firewall

Cloud Native Application Protection (CNAPP)
Unified Security from Code to Cloud

Cloud Detection and Response
Contextual and Actionable Intelligence

SECURE THE **WORKSPACE**

Harmony

SASE
Internet Access Private Access

Email
Cloud Email and Collaboration Suite Security

SaaS
Threat Prevention for SaaS Applications

Endpoint
Protection & Posture Management

Mobile
Mobile Threat Defense

Web Browser
Prevent Internet Threats and Data Loss

COLLABORATIVE SECURITY **OPERATIONS & SERVICES**

Infinity Core Services

Security Operations and AI

XDR/XPR
Extended Prevention and Response

Playblocks
Orchestration and Automation

Events
Unified Events

ThreatCloud AI
AI-Powered Threat Intelligence

AI Copilot
Automating Security with AI

Global Services

MDR/MPR
Managed Prevention and Response

Incident Response
Keep Your Business Running

Consulting & Training
Leverage security architecture design experts

OTD BİLİŞİM
GLOBAL VAD

WHEN IT COMES TO CYBER SECURITY,

"SECOND BEST" WILL GET YOU BREACHED

The Check Point Ethos

PREVENTION NOT DETECTION

Once Malware is inside, it's already too late

OUR MISSION

Allow any organization to conduct their business on the internet with the highest level of security

OTD BİLİŞİM
GLOBAL VAD

ThreatCloud AI

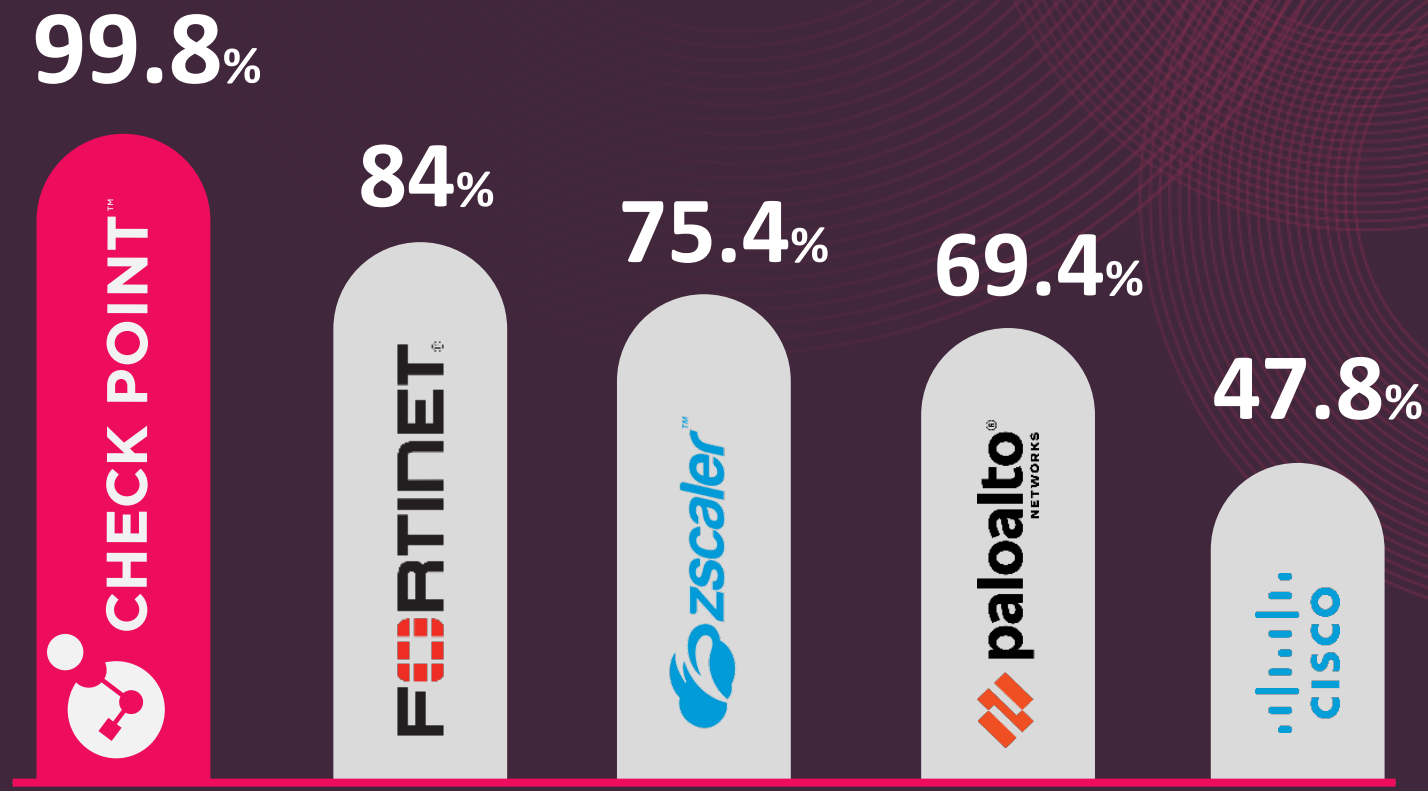
#1 Miercom
In Threat Prevention.
AGAIN

99.8%
Unknown Attacks
Prevented

100%
Zero Phishing Attacks
Prevented

2024 Security Benchmark Report

Zero+1 Malware Prevention Rate

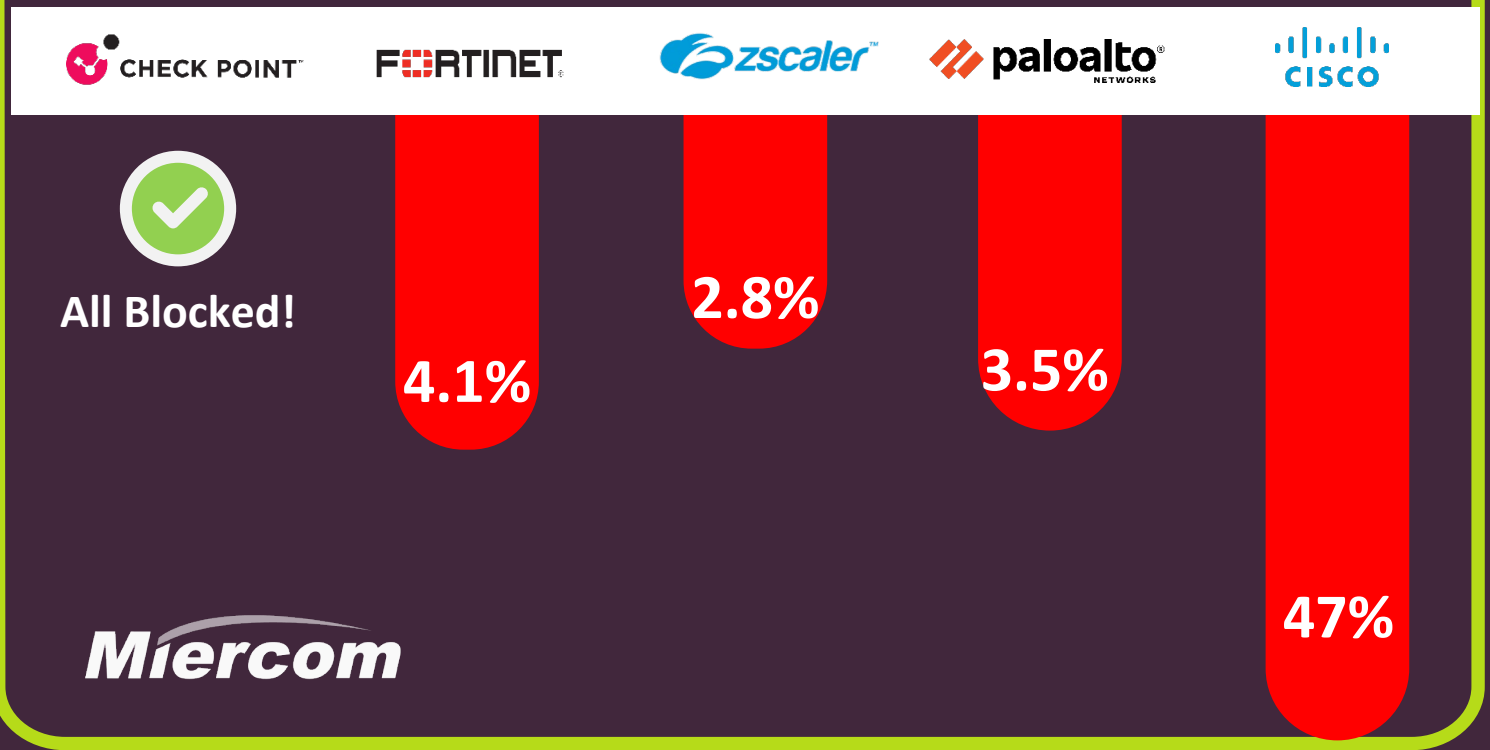


OTD BİLİŞİM
GLOBAL VAD

Zero Phishing 3rd party validation

WEB

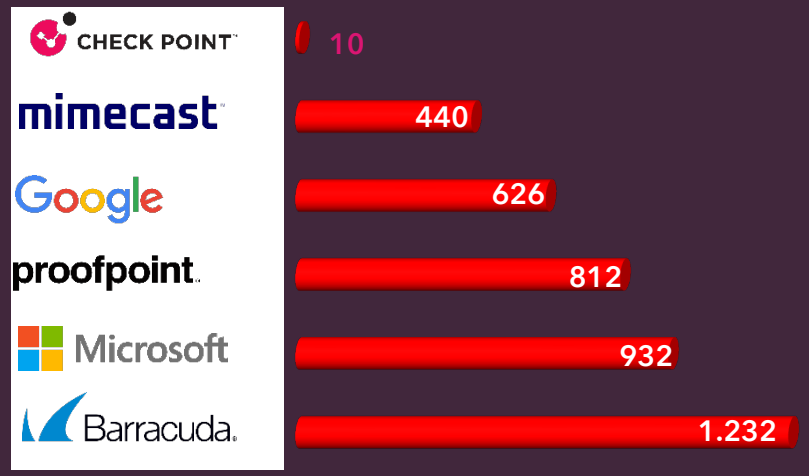
PHISHING LINKS MISSED (WEB BROWSING)



Miercom

EMAIL

PHISHING EMAIL/100K IN USER INBOX



Source: https://tiny.cc/unknown360

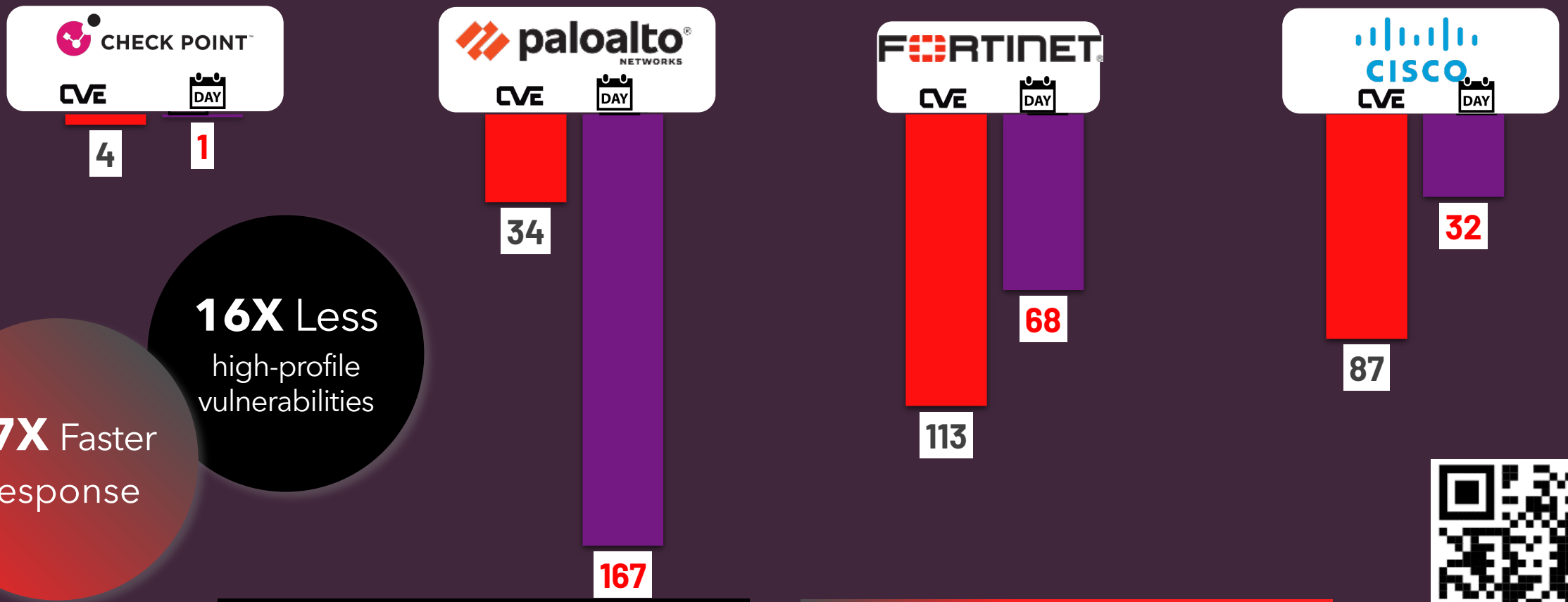
Check Point: The Best Security

OTD BİLİŞİM
GLOBAL VAD

Superior Resilience and a Strong Sense of Urgency

High & Critical Vulnerabilities

2021-2024



16X Less high-profile vulnerabilities

77X Faster Response

Number of Critical & High Vulnerabilities

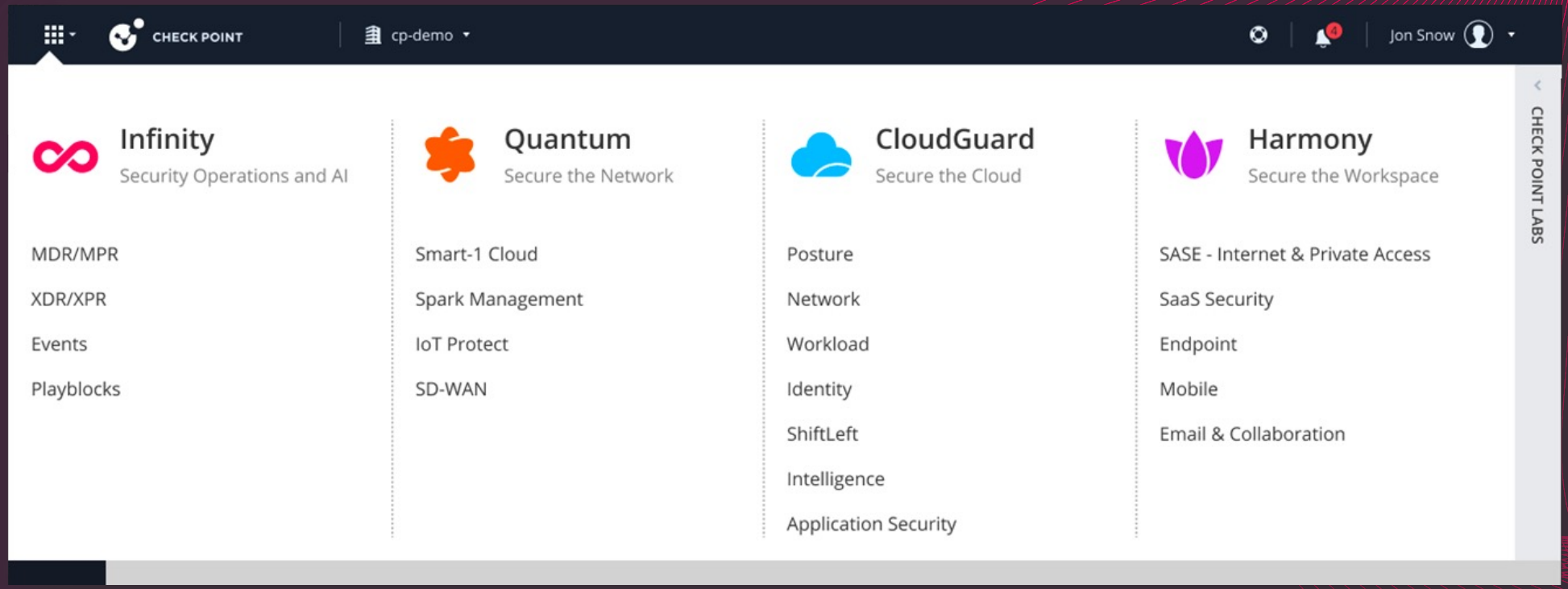
Average Number of days to fix Critical & High Vulnerabilities

Source: Vendors security advisories
Reference: http://tiny.cc/urgency

Updated Sep-01-2024

OTD BİLİŞİM
GLOBAL VAD

Unified Security Management, **Cloud-Delivered**



"Check Point sets the bar for centralized management and usability.

FORRESTER®

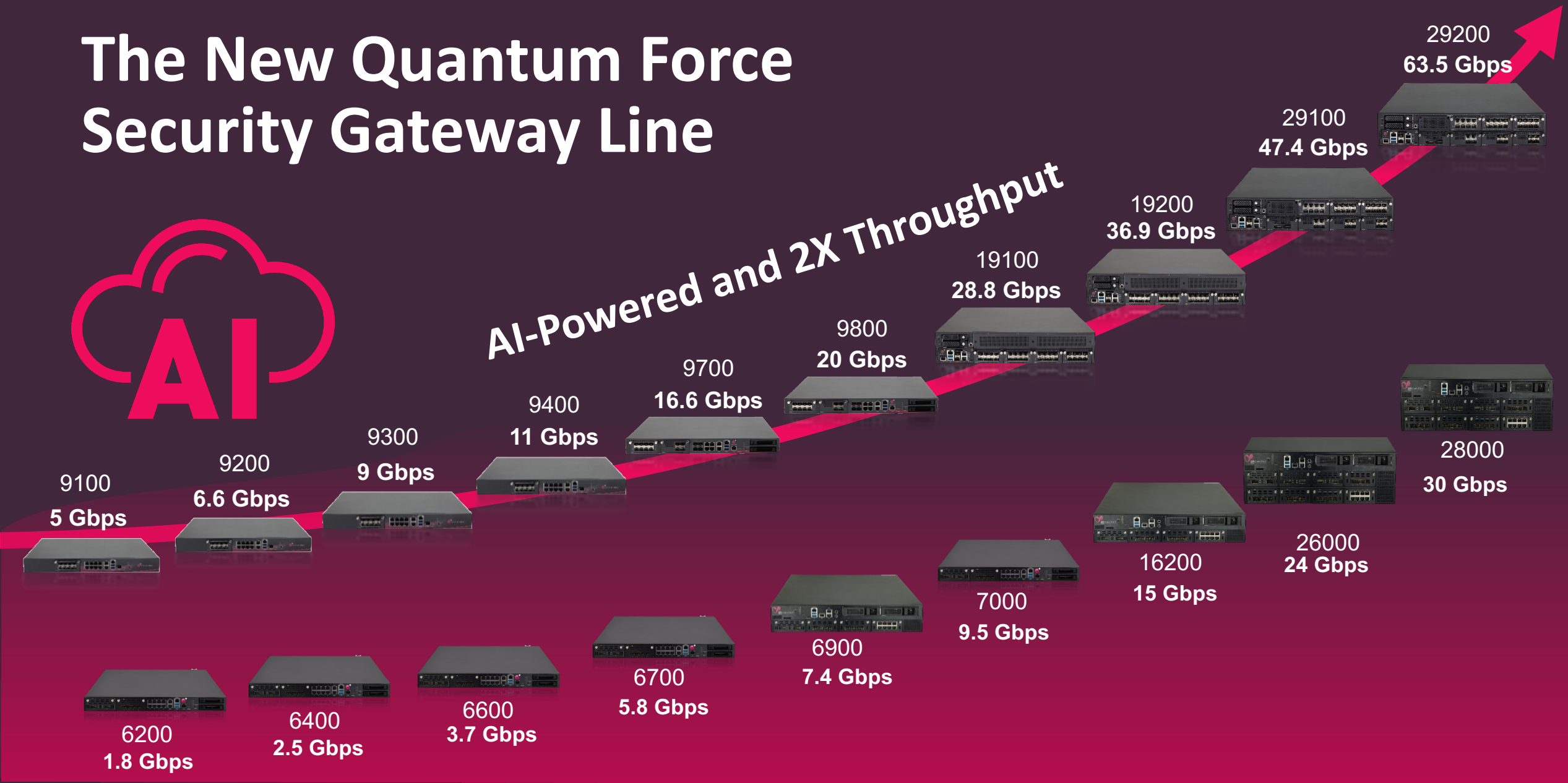
The Forrester Wave™: Zero Trust Platform Providers, Q3 2023

OTD BİLİŞİM
GLOBAL VAD

Quantum Product Family

CHECK POINT

The New Quantum Force Security Gateway Line

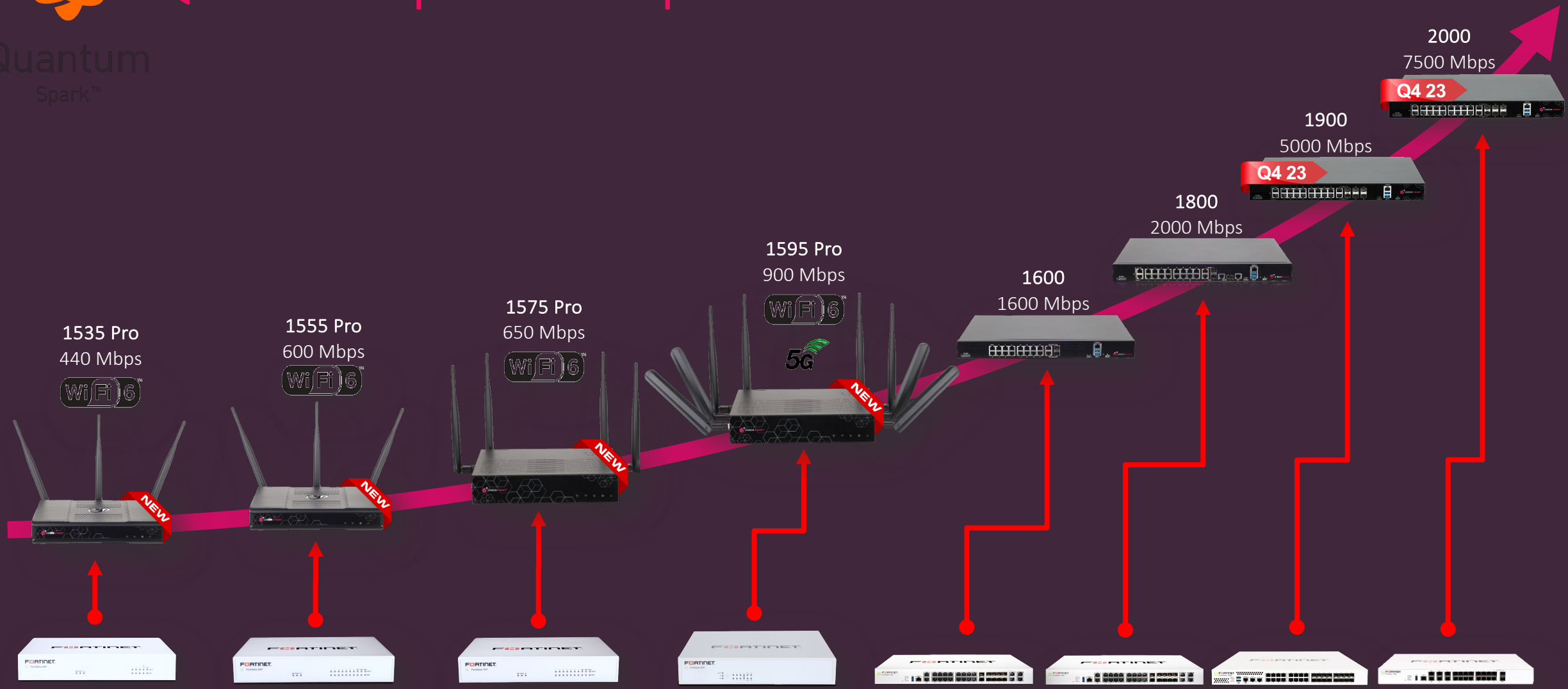


OTD BİLİŞİM
GLOBAL VAD

Gen-V Threat Prevention Throughput

Quantum Spark Lineup vs. Fortinet

Quantum
Spark™

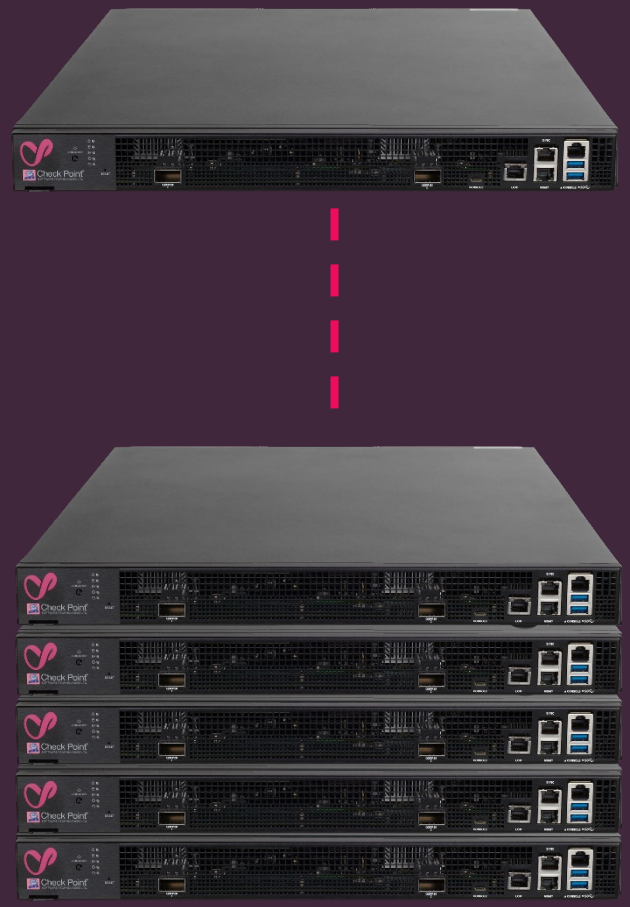


Quantum

Scalability has never been so easy!

OTD BİLİŞİM
GLOBAL VAD

MAESTRO
HYPERSCALE ORCHESTRATOR



16600HS Security Gateway

850 Gbps

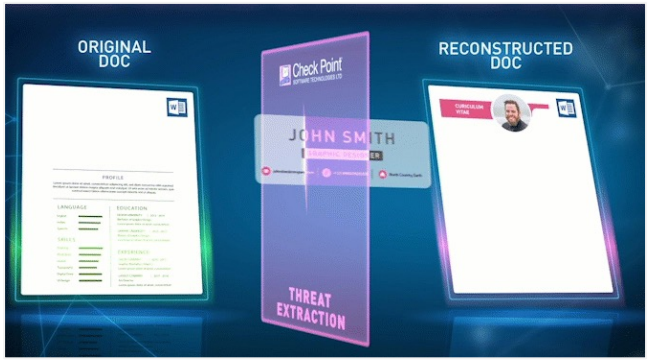
Up to 52 appliances

52.8 Gbps
35.2 Gbps
17.6 Gbps

Threat Prevention

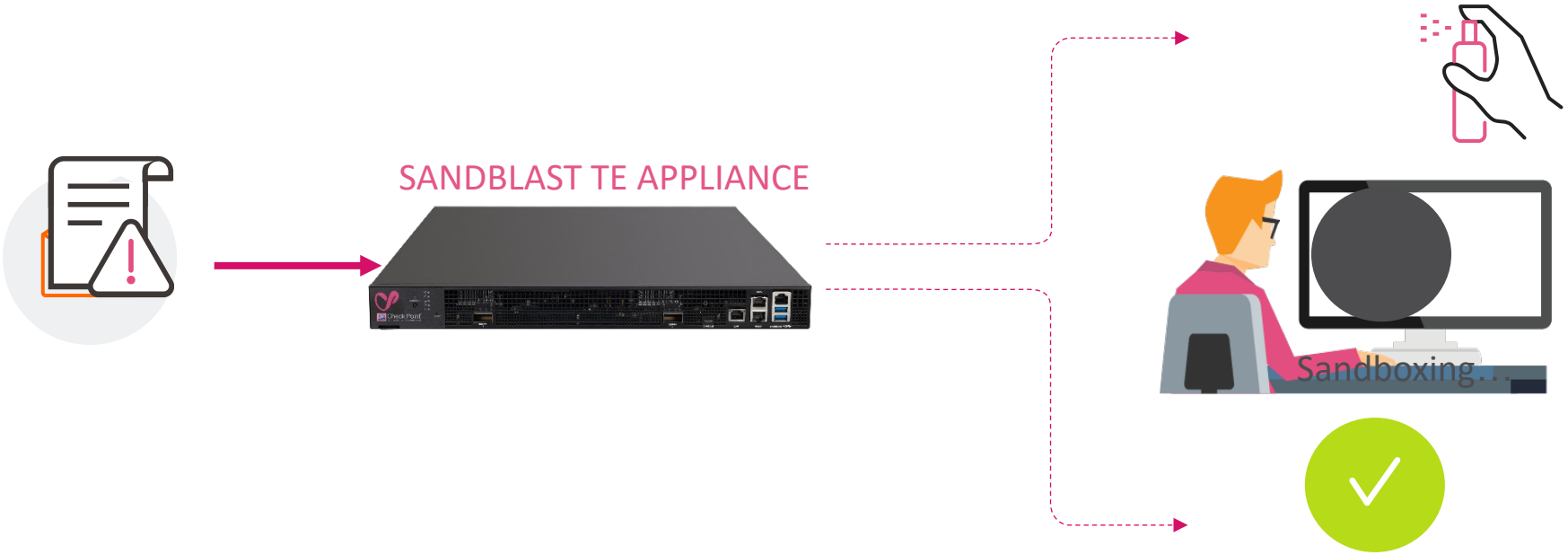
Fully Operational within 6 minutes

THREAT EMULATION / THREAT EXTRACTION



1 Create A Copy of File. Extract everything can be Malicious.

2 In the Background, Scan the File against Zeroday Attacks with Sandboxing.



✓ Users starts using cleaned files instantsly.

✓ If the file is clean, Users can download the original file.

OTD BİLİŞİM
GLOBAL VAD

Quantum Gateways

Next Generation Firewall

Firewall
VPN
Application-Control
IPS

Next Generation Threat Prevention

Next Generation Firewall +

Anti Virus
Anti Bot
URL Filtering
Anti Spam

Advanced DNS Security

Sandblast - Gen V Threat Prevention

Next Generation Threat Prevention +

Threat Emulation
Threat Extraction

Zero Phishing

R81.20 required

Quantum IoT

IoT discovery
IoT threat prevention

R81.20 required

Quantum SD-WAN

Application prioritization
Connectivity monitoring
Automated link failover
Bandwidth aggregation

R81.10 required

12 Blades – Best Security

IoT

SD-WAN

CHECK POINT

OTD BİLİŞİM
GLOBAL VAD

Harmony Product Family

CHECK POINT

OTD BİLİŞİM
GLOBAL VAD

Protect Your Workspace

Layered Security for Users, Devices, Apps and Access

XDR

Mobile

Endpoint

Browser

Email

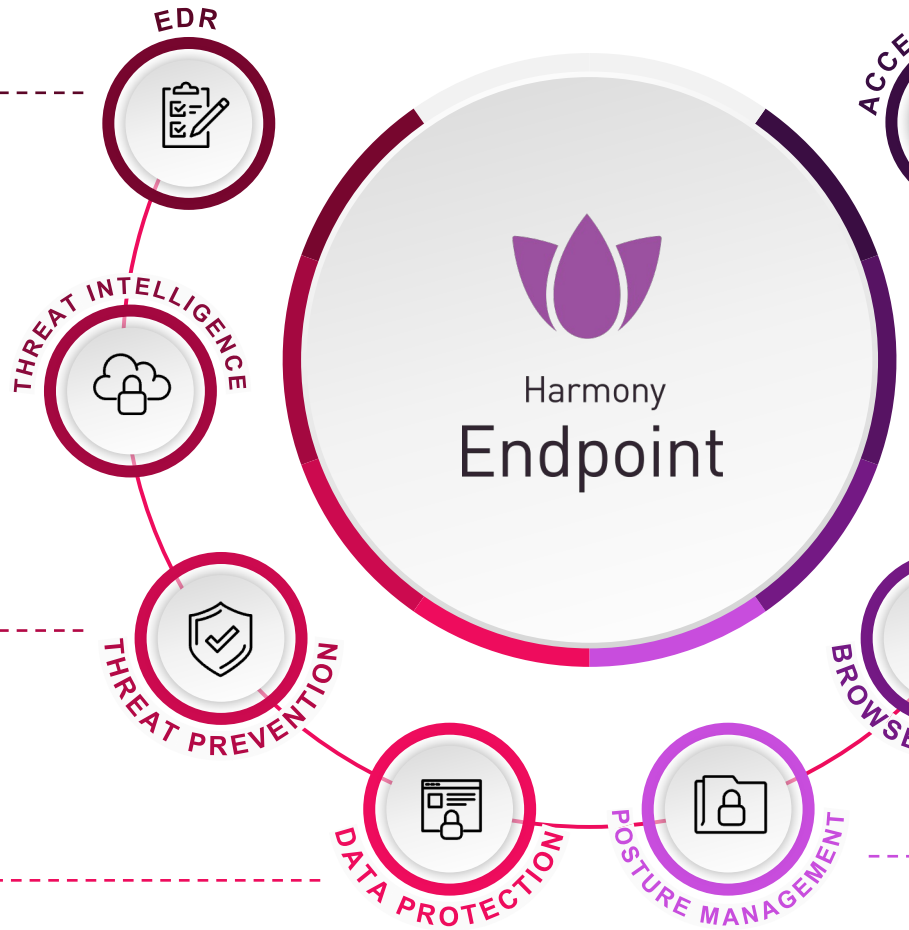
Apps

SASE

- Phishing
- Malware
- Data Leakage
- Vulnerabilities

OTD BİLİŞİM
GLOBAL VAD

360° Endpoint Security



NEW
- **Incident Management**
- **Research Intelligence**

- **Monitoring & Incident Handling**
- **Deployment & Policy Handling**

NEW
- **Threat Hunting**
- Forensic Report
- MITRE Mapping

- **Remote Access VPN**
- Firewall
- Application Control
- Endpoint Compliance

- **ThreatCloud**
- IOC Management

- **Threat Emulation**
- **Threat Extraction**

- **Anti-Ransomware & Intel TDT**
- **Anti-Bot**
- Anti-Malware
- Anti-Exploit
- Behavioral Guard
- Port Protection

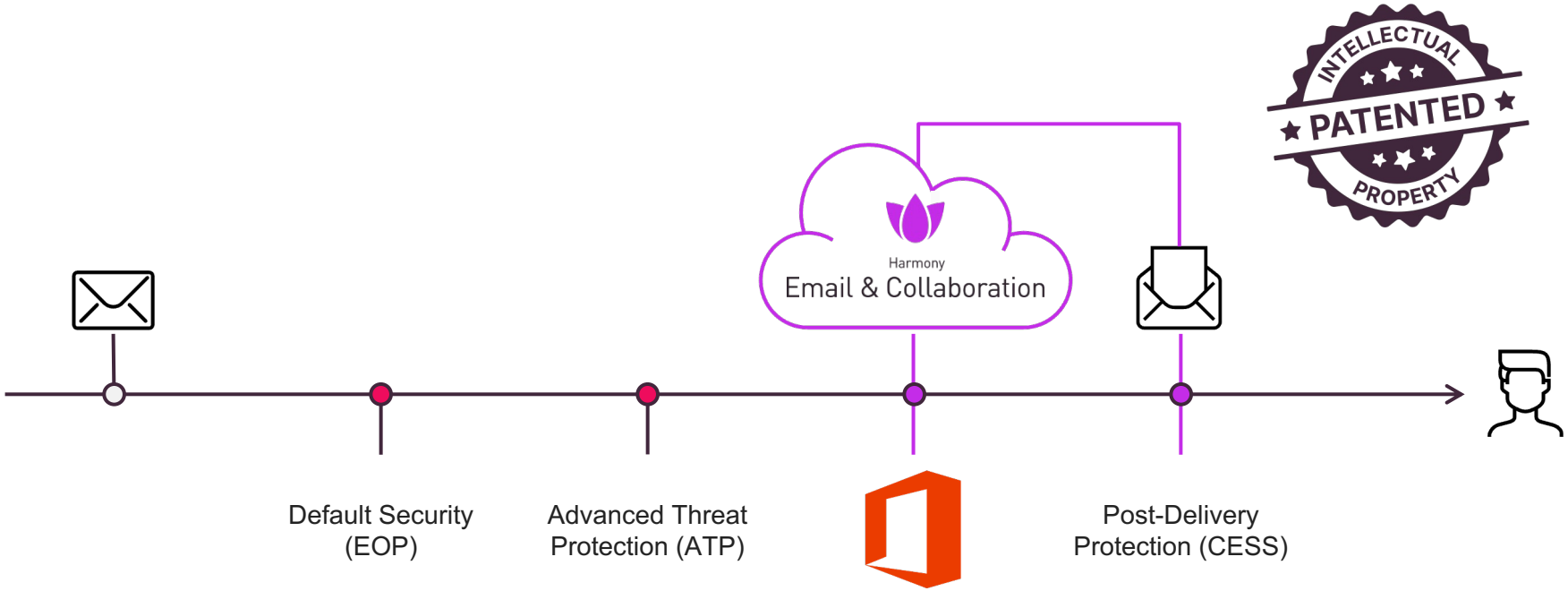
NEW
- **Zero-day Phishing**
- **DLP (Data Loss Prevention)**
- URL Filtering
- Corporate Password Reuse
- Safe Search

- **Full Disk Encryption**
- Media Encryption

NEW
- **Vulnerability Management**
- **Patch Management**
- Inventory Management

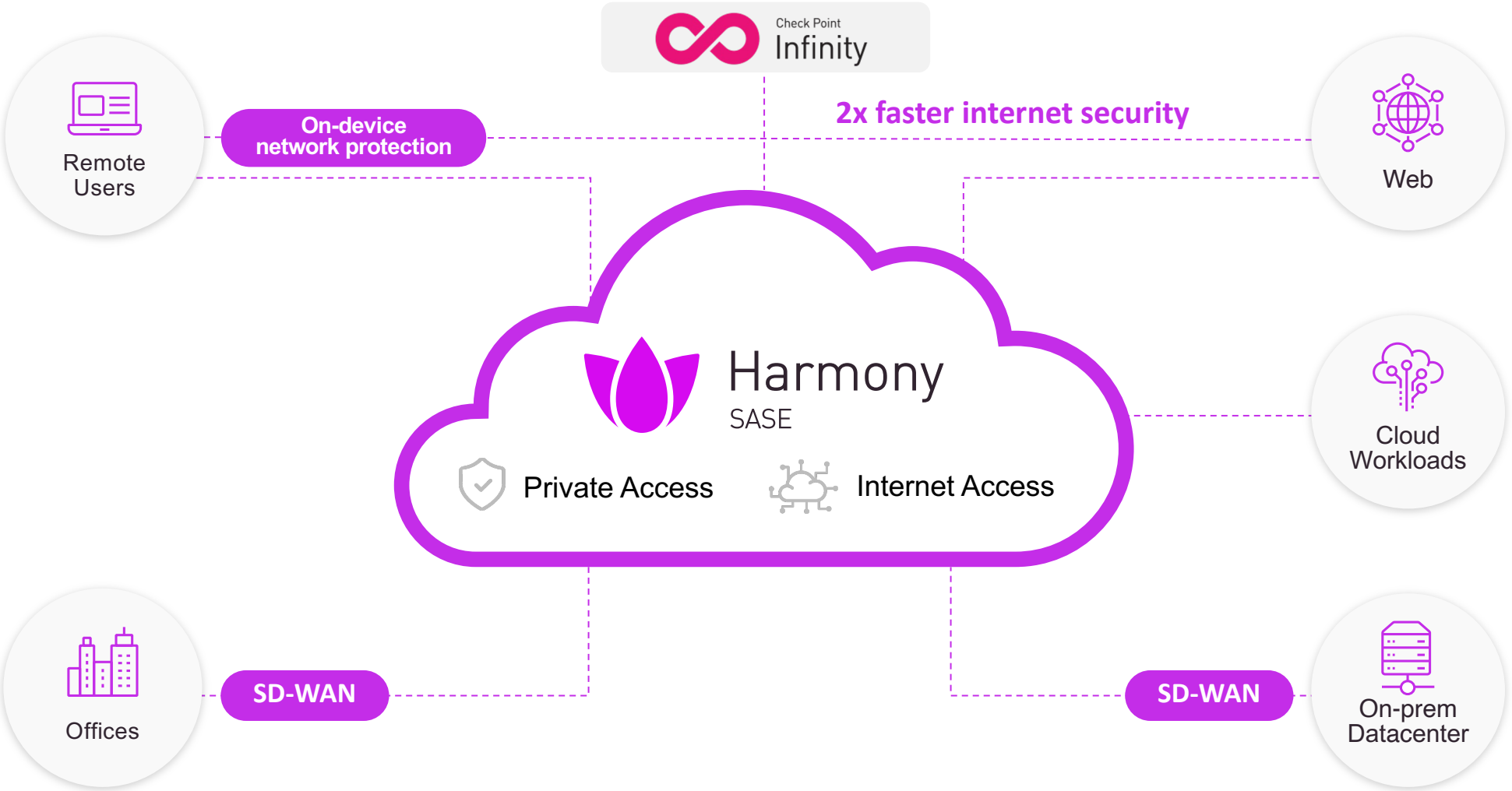
CHECK POINT

Prevention First Email Security

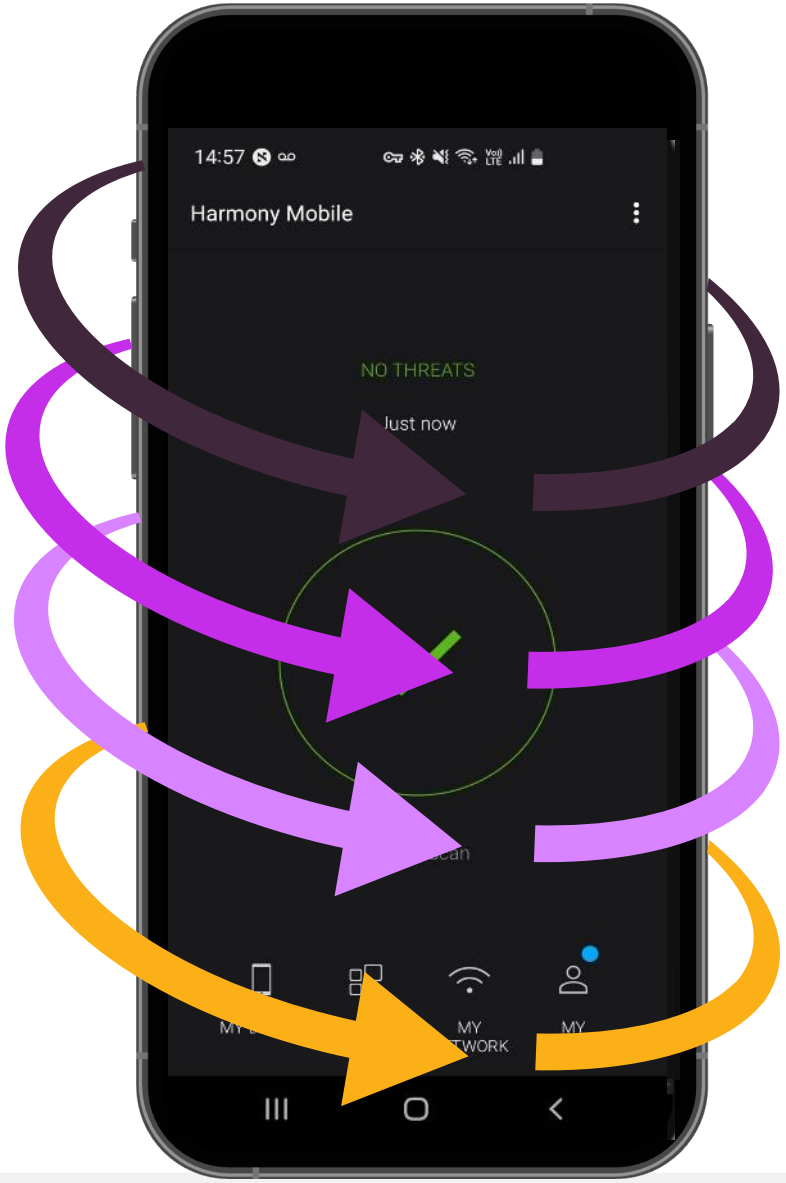


- BEC / anti-phishing
- NLP & stylometry
- Impersonation
- Anti-spam
- Notice/alert
- Account compromise
- Malware AV/Sandboxing
- Encrypted Attachments
- Malware Threat Extraction (CDR)
- Link Reputation / Threat-Intel
- Link Sandboxing
- Link Click-time Protection
- DLP
- Encryption

The Only Hybrid SASE with On-Device Protection



Harmony Mobile - Complete Protection



01
APPLICATIONS

- Real-time analysis Malicious side-loading prevention

02
NETWORK

- Anti-phishing / Zero-phishing
- Safe browsing
- Conditional access
- Anti-bot
- URL filtering
- Protected DNS
- Wi-Fi network security (MiTM)
- Risky download prevention

03
DEVICE & OS VULNERABILITY

- OS vulnerabilities
- Device-level exploits
- Risky configurations
- Advanced rooting
- Jailbreak detection

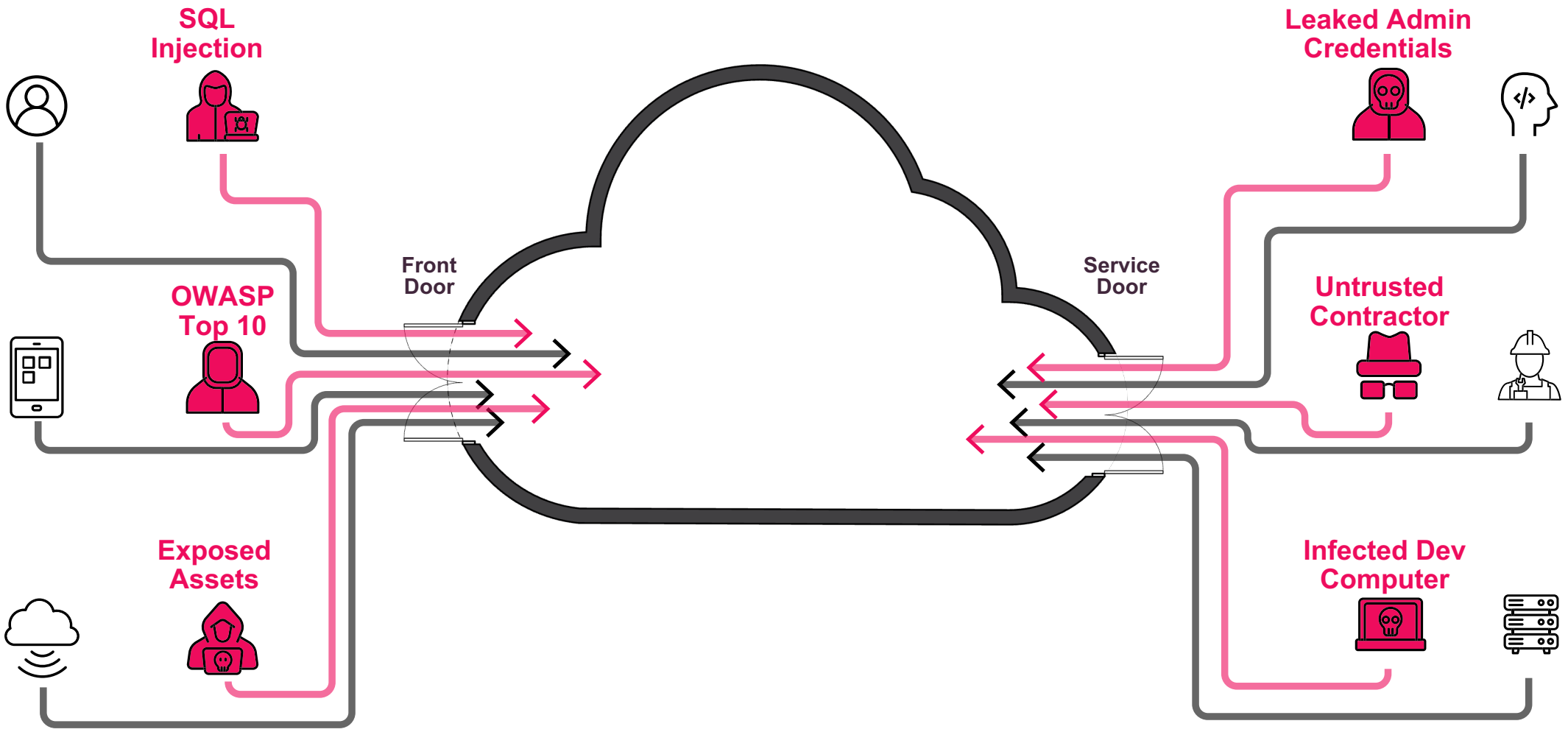
04
FILES

- Download prevention
- Storage scanning
- Zero-day file emulation (Sandboxing)

OTD BİLİŞİM
GLOBAL VAD

CloudGuard Product Family

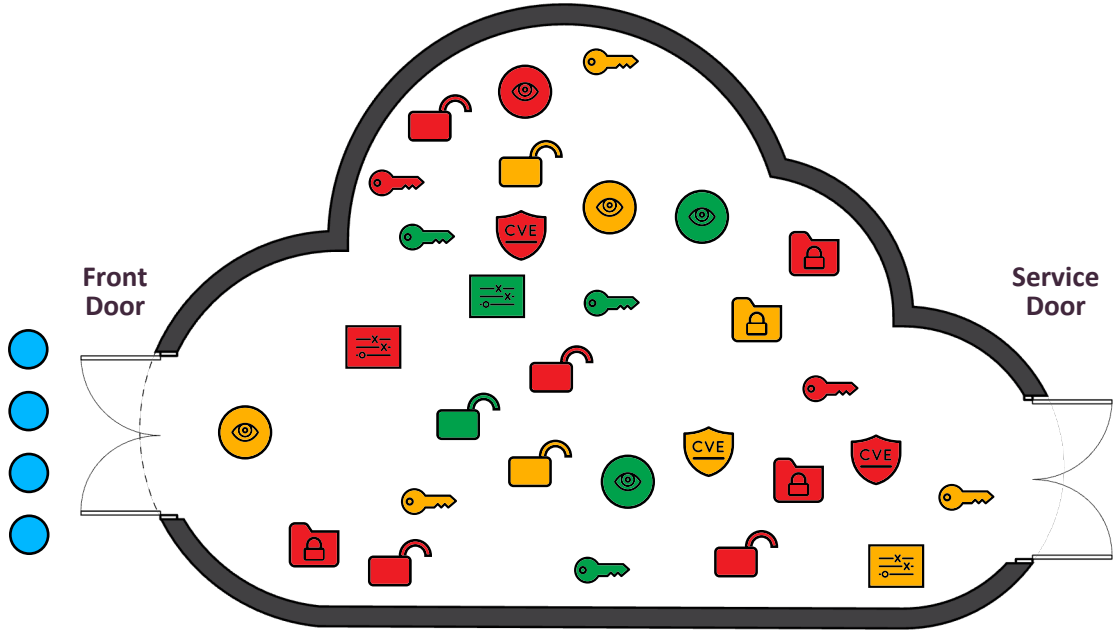
CHECK POINT



Attackers Enter The Cloud Through The Front Door

Or Through The Service Door

CloudGuard WAF



Use Case	CloudGuard WAF	Cloud Native WAF
Zero Day Prevention	✓ **Immediate**	× **Avg. 40 days***
Signature Updates	✓ **AI**	× **Signature**
Accuracy	✓ **Highest 97%**	× **87%***
API Prevention	✓ **Yes**	× **Not Provided**
Multi-Cloud Support	✓ **Yes**	× **Single Cloud**

Unmatched AI-Based WAF Prevention

Comprehensive Application Self-Protection

Cloud Native WAF

Stop application layer attacks including OWASP Top 10 and much more

API Security

Protect APIs; shield applications from exploits like XML, REST, GrpahQL, and JSON payload processing and API usage thresholds

Bot Prevention

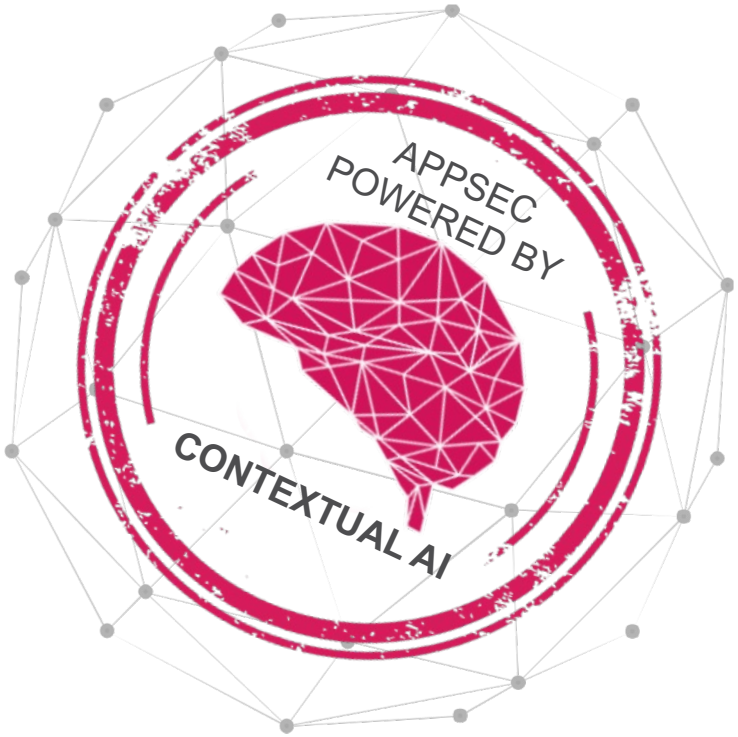
Stop automated attacks, Inclusive of user credential abuse

Rate Limit

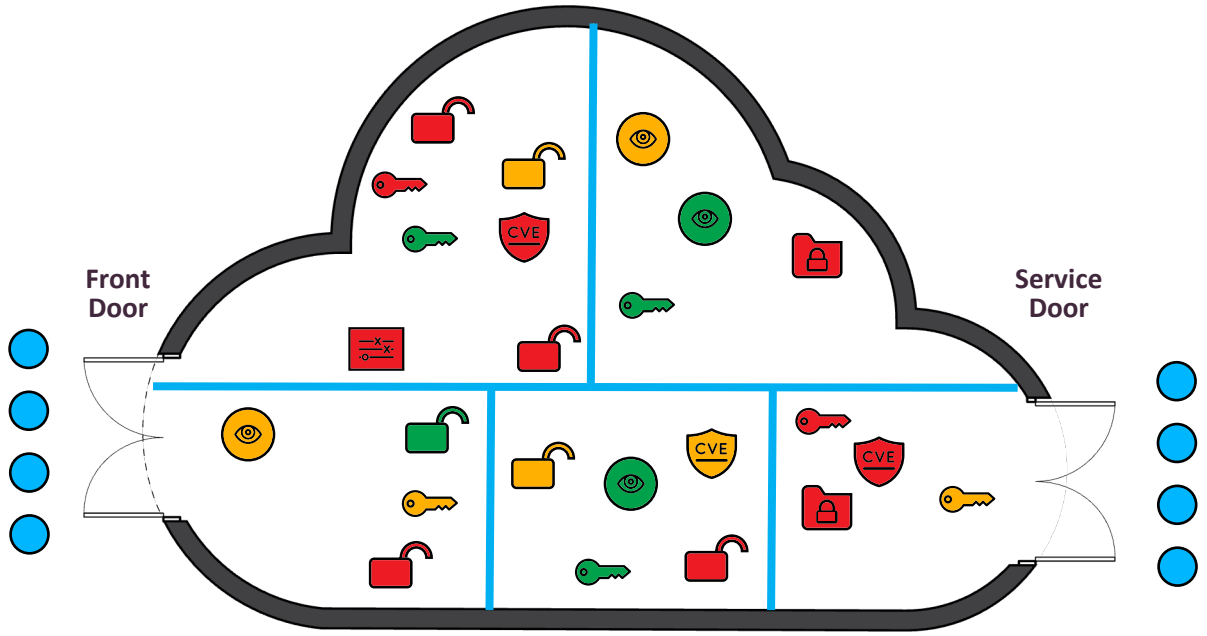
Limit the number of requests to an API/App resource within a configured time, scope to block DDoS/DoS attack

File Security

Analyze any files uploaded and consult Check Point's Threat Cloud regarding the file's reputation.



CloudGuard Network



CloudGuard Network

Use Case	CloudGuard Network Security	Cloud Native FW
Threat Prevention	✓ Best Security	× Limited IPS
Hybrid-Cloud Support	✓ Yes	× No On-Prem. Support
Multi-Cloud Support	✓ Yes	× Single Cloud
ROI	✓ High 169%	× Low <40%

Unmatched Cloud Network Security

CloudGuard
CNAPP

OTD BİLİŞİM
GLOBAL VAD

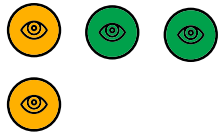
#3 Use CNAPP with Prevention To Remediate The Remaining Risks

CHECK POINT

CNAPP

Workload Protection

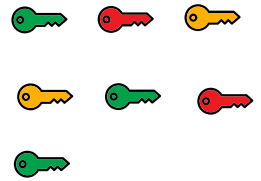
Detection & Response



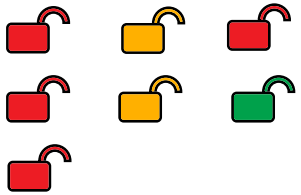
Posture Mgmt.

Data Posture

Identity Mgmt.



Code Security



Classify Your Cloud Risks Powered by 6 CNAPP Modules

CloudGuard: Complete CNAPP Platform With Prevention

OTD BİLİŞİM GLOBAL VAD

8 Modules & 52 Engines

Network Security
- IPS Protection
- Threat Emulation & Extraction
- Hybrid Cloud VPN
- Cloud Native WAN Integration
- Hub & Spoke Segmentation
- Bot Protection, DLP, TP
- IaC deployment

WAF
- ML-based Threat Prevention
- API discovery and security
- Bot Prevention
- API Schema Validation
- File Security
- Intrusion Prevention (IPS)
- IaC deployment

CSPM
- Service Inventory
- Out-of-the-box Rulesets
- Best Practice Rulesets
- Compliance Standards Rulesets
- Custom Rules

CWPP
- Container Vulnerability
- Malware Scanning
- Runtime Threat Detection
- Behavior Anomalies
- Function Self Protect (Serverless)
- Agent & Agentless

CIEM
- Graph Visualization
- Effective Permissions Calculation
- Overprivileged Identities Detection
- Inactive Identities Detection
- Behavior Anomalies
- Best Practice Violations

CDR
- Network Log Analysis
- Kubernetes Network Log Analysis
- Account Activity Log Analysis
- Threat Identification
- Behavioral Analysis
- Anomaly Detection

DSPM
- Coverage of Azure & AWS
- Cloud Native Classification Engine:
- Amazon Macie & Microsoft Purview
- Identify PII, PCI, PHI
- Indicated as a risk factor

Code Security
- Code & IaC Scanning
- IaC, Secret, & CI/CD Detectors
- Custom Detectors
- Offline & Online Scanning
- Software Composition Analysis (SCA)
- Repos, Local, & Pipeline Scan

CloudGuard Unified Platform

- **Unified Findings & Asset Mgmt.**
- **Risk Mgmt.**
- **Remediation (Guidelines/Automatic/1-Click)**
- **1-Click Agentless Onboarding**

OTD BİLİŞİM
GLOBAL VAD

Infinity Core Services

CHECK POINT

AI is Powering Better Security

AI-Powered Threat Prevention

AI-Powered Assistant for Admins & Security Analysts

Protect AI Servers

Enable Safe GenAI usage

ThreatCloud AI

50+ Threat Prevention Engines for 99.8% malware catch rate
Real-time Threat Intelligence

AI Copilot

Saves up to 90% of the time needed to perform common administration tasks
Accelerates SecOps threat hunting, analysis and automated response.

Copilot for Quantum – GA
Copilot for XDR - GA

AI Cloud Protect

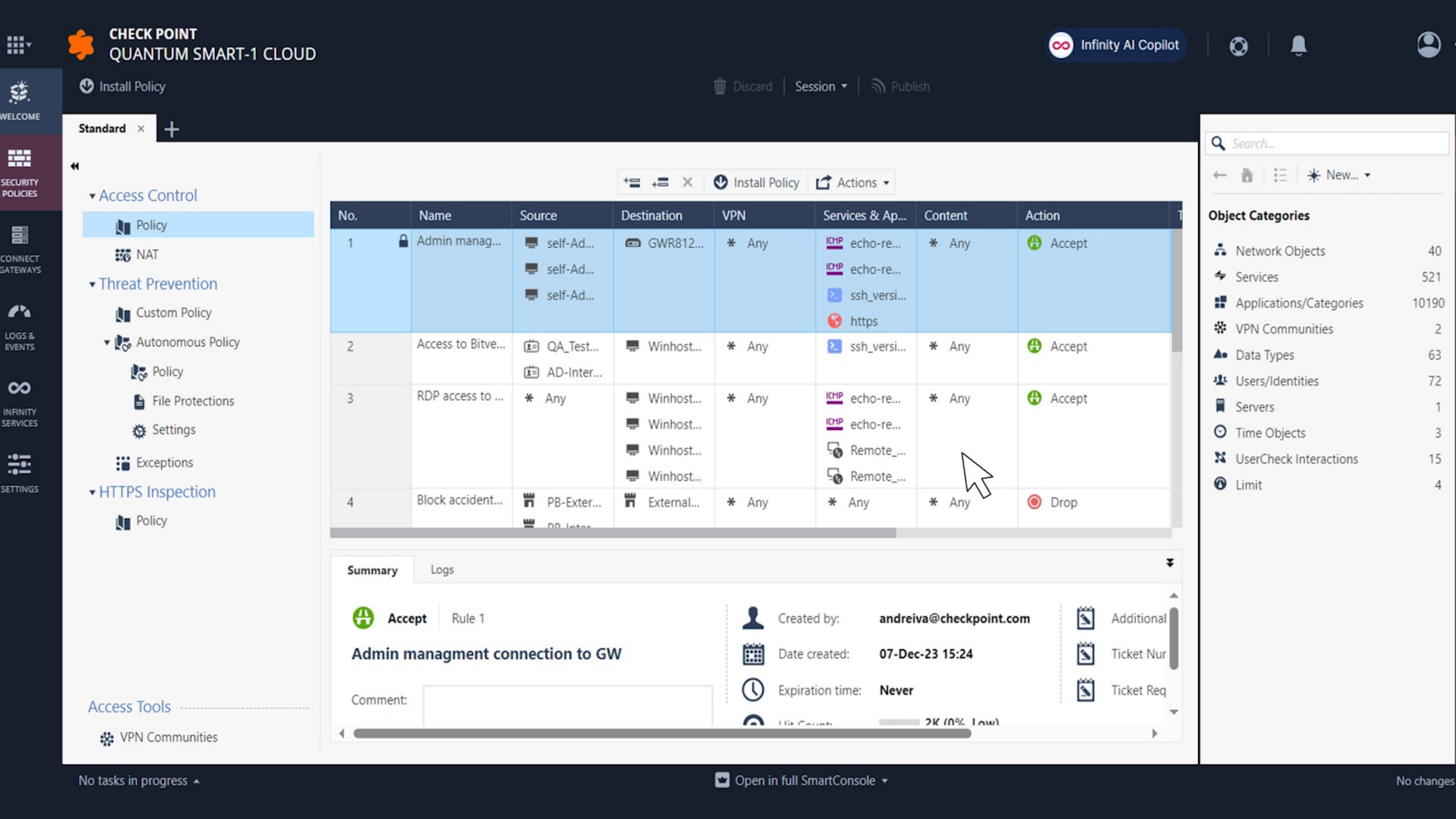
Nvidia partnership to protect AI cloud infrastructure used by enterprises for their own AI apps

Preview

GenAI Security

Enables safe adoption of GenAI in the enterprise; delivers discovery, risk insights, data protection in real time

Preview


CHECK POINT
QUANTUM SMART-1 CLOUD
Infinity AI Copilot
Install Policy
Discard
Session
Publish
WELCOME
SECURITY POLICIES
CONNECT GATEWAYS
LOGS & EVENTS
INFINITY SERVICES
SETTINGS
Standard
Access Control
Policy
NAT
Threat Prevention
Custom Policy
Autonomous Policy
Policy
File Protections
Settings
Exceptions
HTTPS Inspection
Policy
Access Tools
VPN Communities
Install Policy
Actions
No. Name Source Destination VPN Services & Ap... Content Action
1 Admin manag... self-Ad... self-Ad... self-Ad... GWR812... Any echo-re... echo-re... ssh_versi... https Any Accept
2 Access to Bitve... QA_Test... AD-Inter... Winhost... Any ssh_versi... Any Accept
3 RDP access to ... Any Winhost... Winhost... Winhost... Winhost... Any echo-re... echo-re... Remote_... Remote_... Any Accept
4 Block accident... PB-Exter... External... Any Any Any Drop
Summary
Logs
Accept
Rule 1
Admin managment connection to GW
Comment:
Created by: andreiva@checkpoint.com
Date created: 07-Dec-23 15:24
Expiration time: Never
Additional
Ticket Nur
Ticket Req
Search...
New...
Object Categories
Network Objects 40
Services 521
Applications/Categories 10190
VPN Communities 2
Data Types 63
Users/Identities 72
Servers 1
Time Objects 3
UserCheck Interactions 15
Limit 4
No tasks in progress
Open in full SmartConsole
No changes

Infinity
AI Copilot

Hi Gil, what can I do for you today?

Just now

Documentation How can I create a new policy?

Logs Can you give me a list of malware families that was detected in the last 7 ...

Configuration Display the configured gateways

Policy Show my policies

Troubleshooting Am I protected from CVE-2019-0708 ?

Emily Johns can't access SAP-server-America, please suggest allowing her access

Emily Johns can't access SAP-server-America, please suggest allowing her access

18:24

The logs show that Emily Johns attempts to access the SAP-server-America (IP: 192.168.19.1) were dropped by the rule 6.3 named "Production Farm Cleanup rule". This happened multiple times, last time on 2024-01-03 at 13:59:41.

Just now

Would you like to add Emily Johns to access role 'Sales_North_America' that can access SAP-server-America

Yes (Add to access role) No

18:24

Emily Johns added to access role 'Sales_North_America'

Just now

Would you like to Install Policy

Yes (Install Policy) No

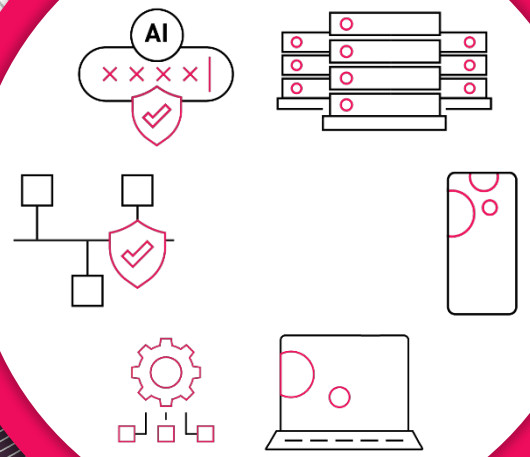
How can I help you today?

Inifinity XDR / XPR

Infinity XDR/XPR

Bank, EMEA

Correlation



Detection

High Severity Breach is Active on 3 Endpoints compromised 1 User

Comprehensive Prevention

- Isolated Infected endpoints
- Blocked Malicious URLs
- Removed Reset Password for user
- Processes from devices

Quantum

Harmony

CloudGuard

Infinity External Risk Management

OTD BİLİŞİM
GLOBAL VAD

Attacks Surface Monitoring	Targeted Threat Intelligence	Global Threat Intelligence	Brand Protection	Supply Chain Intelligence
Shadow IT & Asset Discovery	Dark web Monitoring & Actor Chatter	Ransomware watch & Threat landscape	Brand & Phishing Protection	Vendors & Technology Detection
Vulnerabilities & Exposure Detection	Credentials and Account Takeover	Enriched IoC Feeds	Social Media Impersonation	3rd party Risk Management
CVE Intelligence	Fraud & Data leakage	Intelligence Knowledgebase	Mobile App Impersonation	Alerting on Critical Risks and Breaches

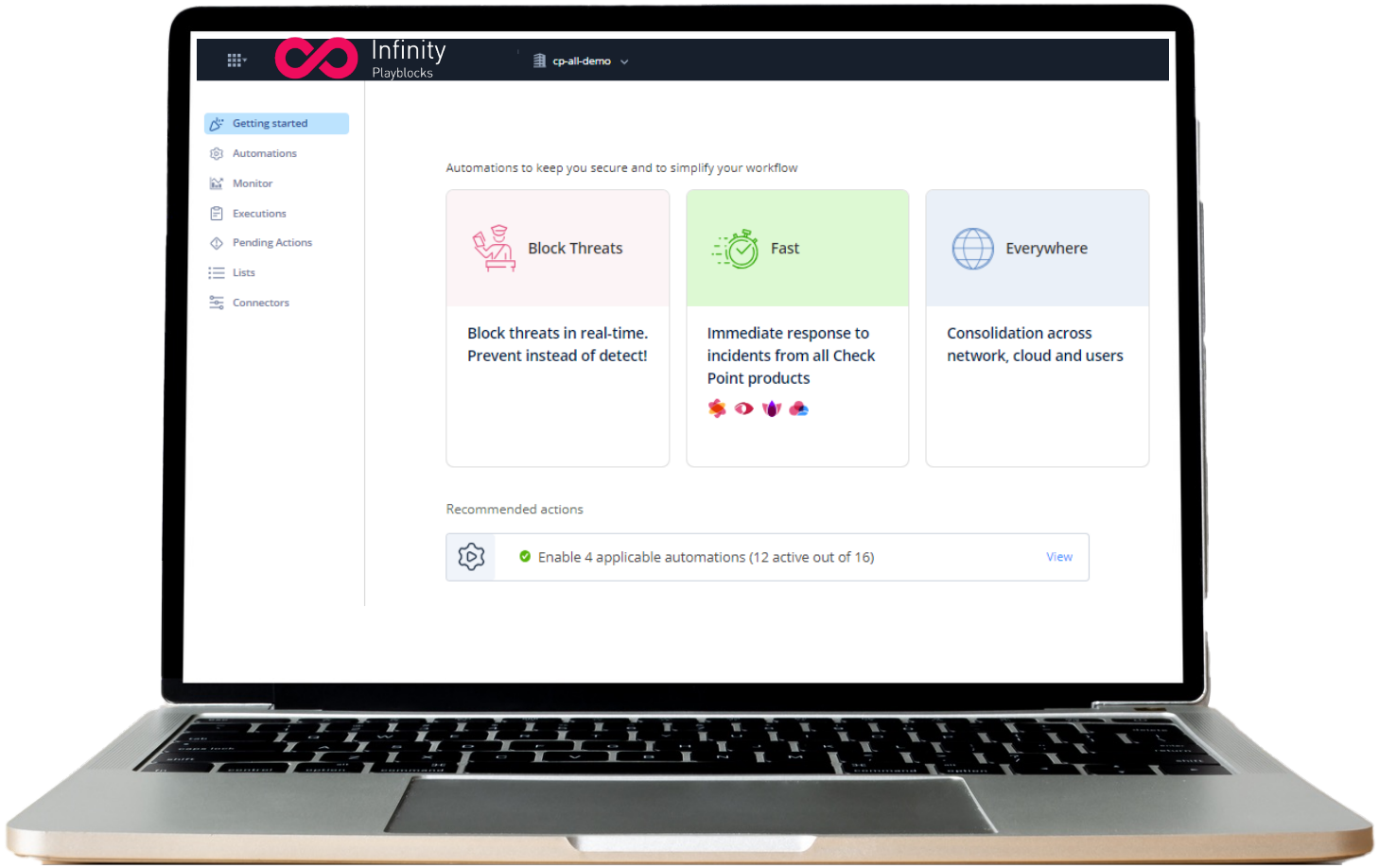
Remediation

Fast & Effective Takedowns | 3rd Party Integrations

Expert Threat Intelligence

Triage & Contextualization Of Alerts | Virtual HUMINT | Custom Investigations & Threat Actor Profiling

Infinity Playblocks - SOAR



Infinity
Playblocks

- +70 out-of-the-box Playblocks
- 2-minute deployment
- Available as cloud service

PHISHING I
RANSOMWARE I
DATA LEAKAGE I
VULNERABILITIES

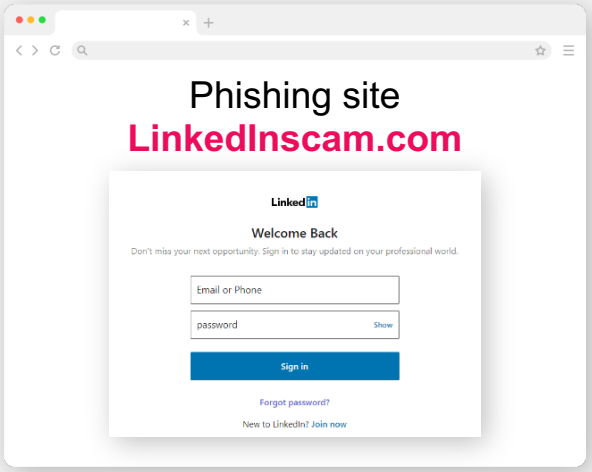
360° Threat Prevention

Examples

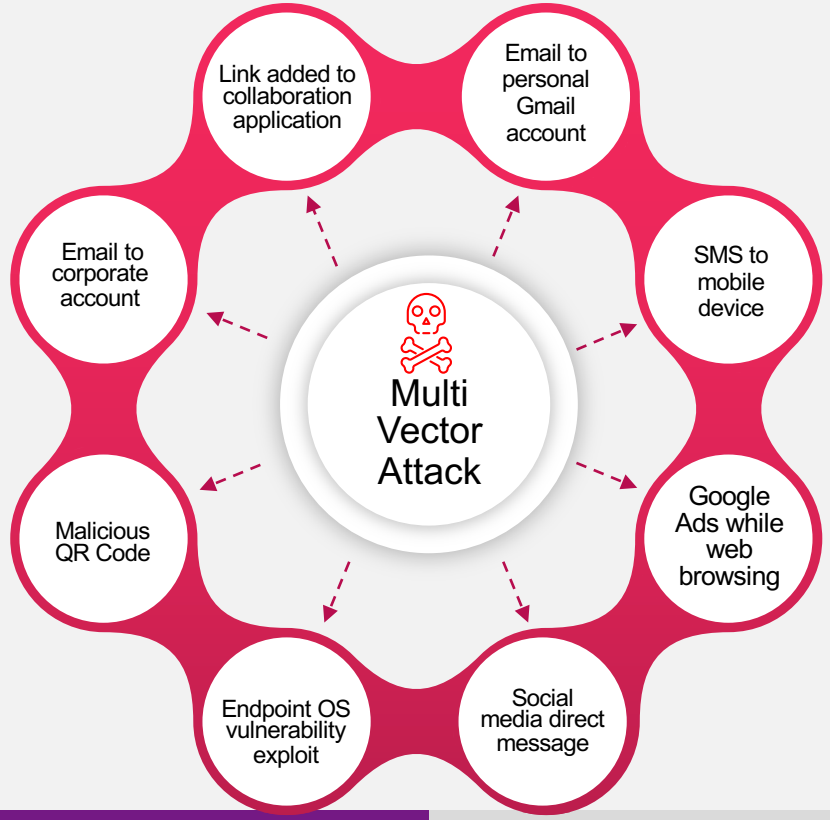
Example: Phishing Attack

PHISHING

Phishing site created



Distributing the attack



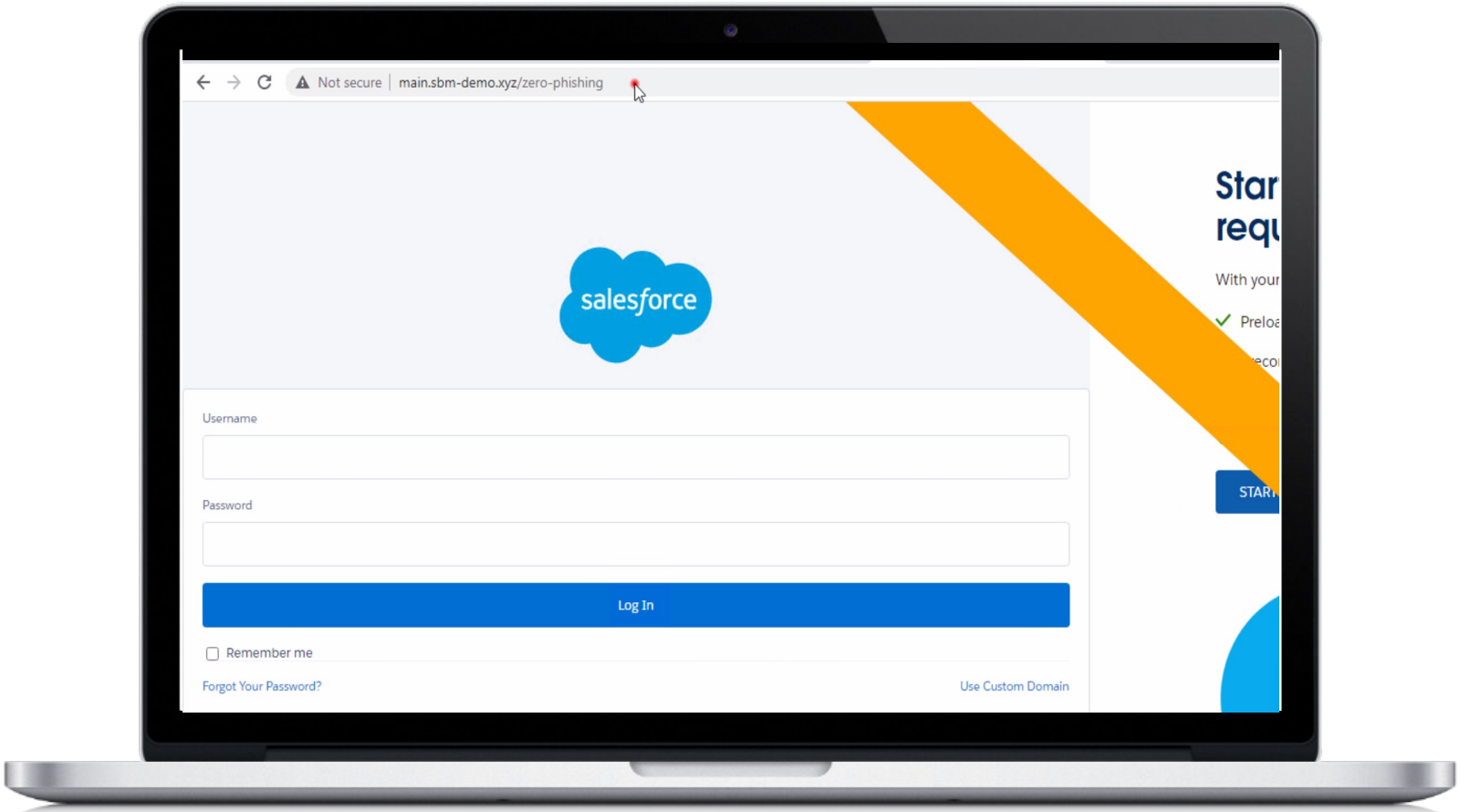
360° ZERO DAY PHISHING PROTECTION

Anti Phishing

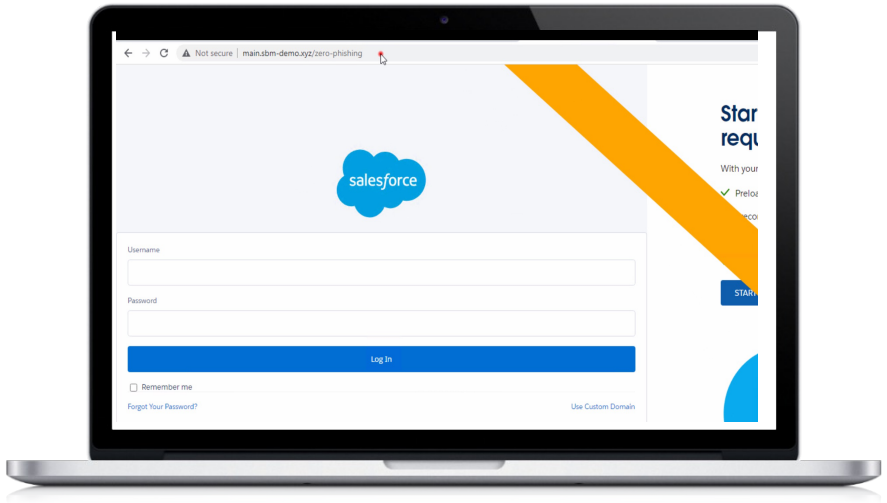
PHISHING

Endpoint Protection

- **Blocks zero-day phishing** sites designed to steal user credentials
- Prevents **re-use of corporate passwords**
- **Real-time analysis** of threat indicators including domain reputation, links, IP, and similarity to legitimate web pages



Anti Phishing



PHISHING

Firewall Protection

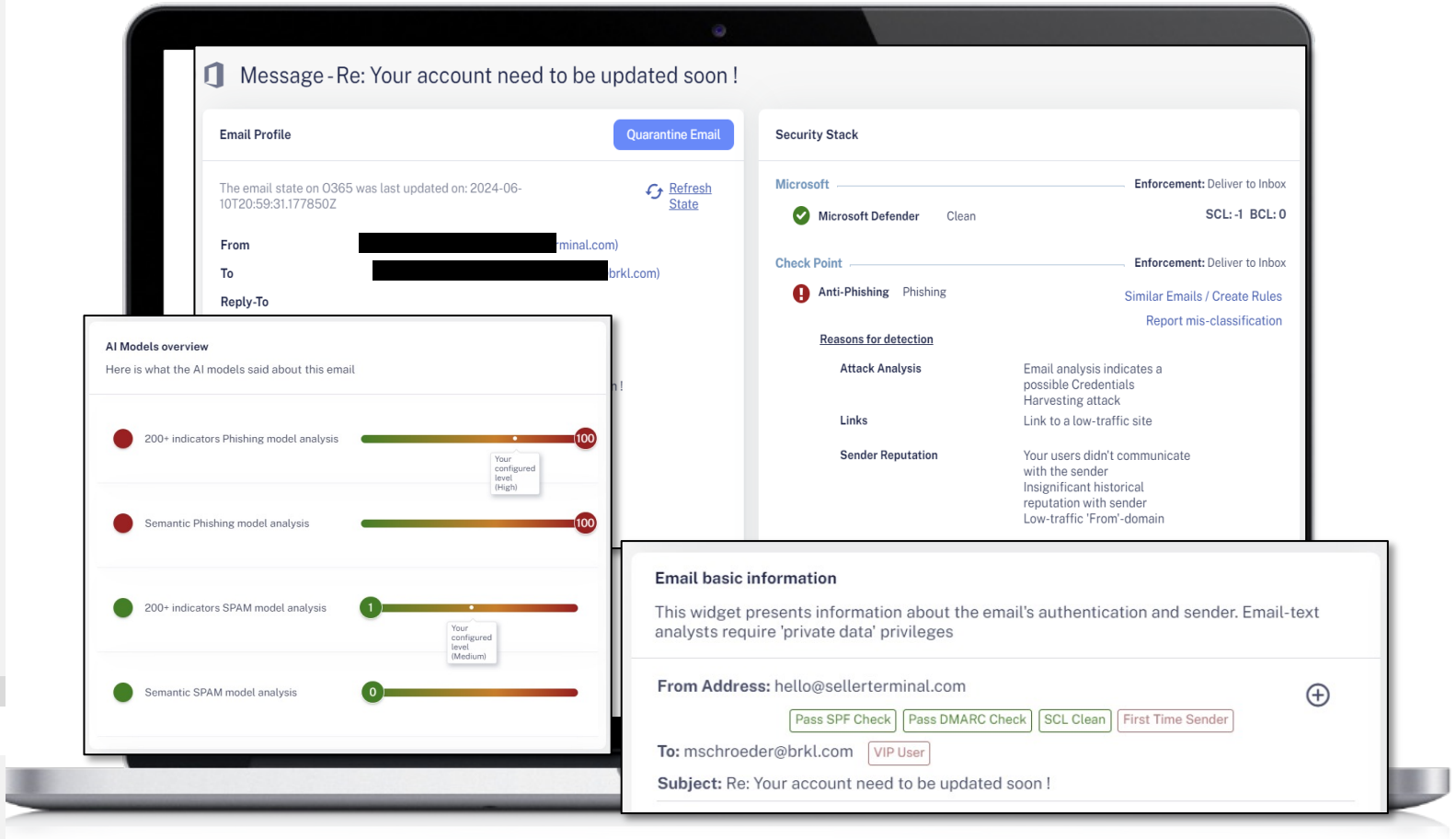
- **Blocks zero-day phishing** sites designed to steal user credentials
- **Real-time analysis** of threat indicators including domain reputation, links, IP, and similarity to legitimate web pages

Anti Phishing

PHISHING

Email Protection

- AI for deep analysis and low false positive!
- Superior NLP for email's subject and body
- Full Malware Analysis for any file attached or discovered at URL destination



G Suite Office 365 Exchange

CHECK POINT

OTD BİLİŞİM GLOBAL VAD

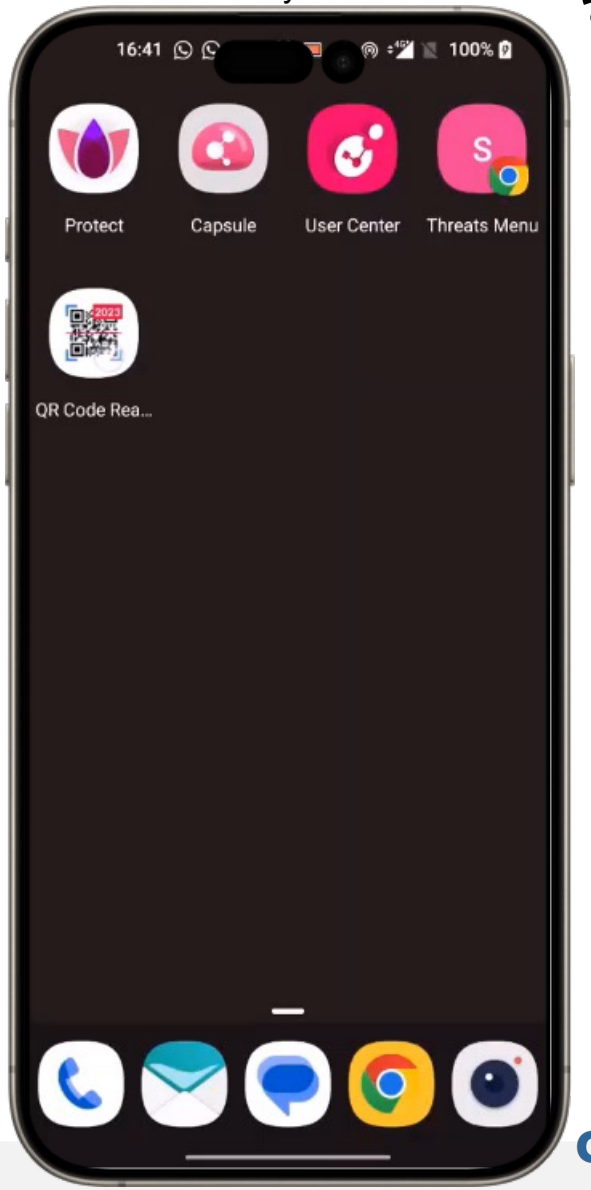
Anti SMishing & Qwishing

Mobile Protection

- Anti-phishing engine instantly inspects the link
- Unknown sites analyzed in real-time with Zero-phishing
- URL identified as malicious phishing and blocked

Competition

Harmony Mobile



PHISHING

Multi-layered protection

Email

Firewall

Browser

Mobile

0 DAY ATTACKS

PHISHING

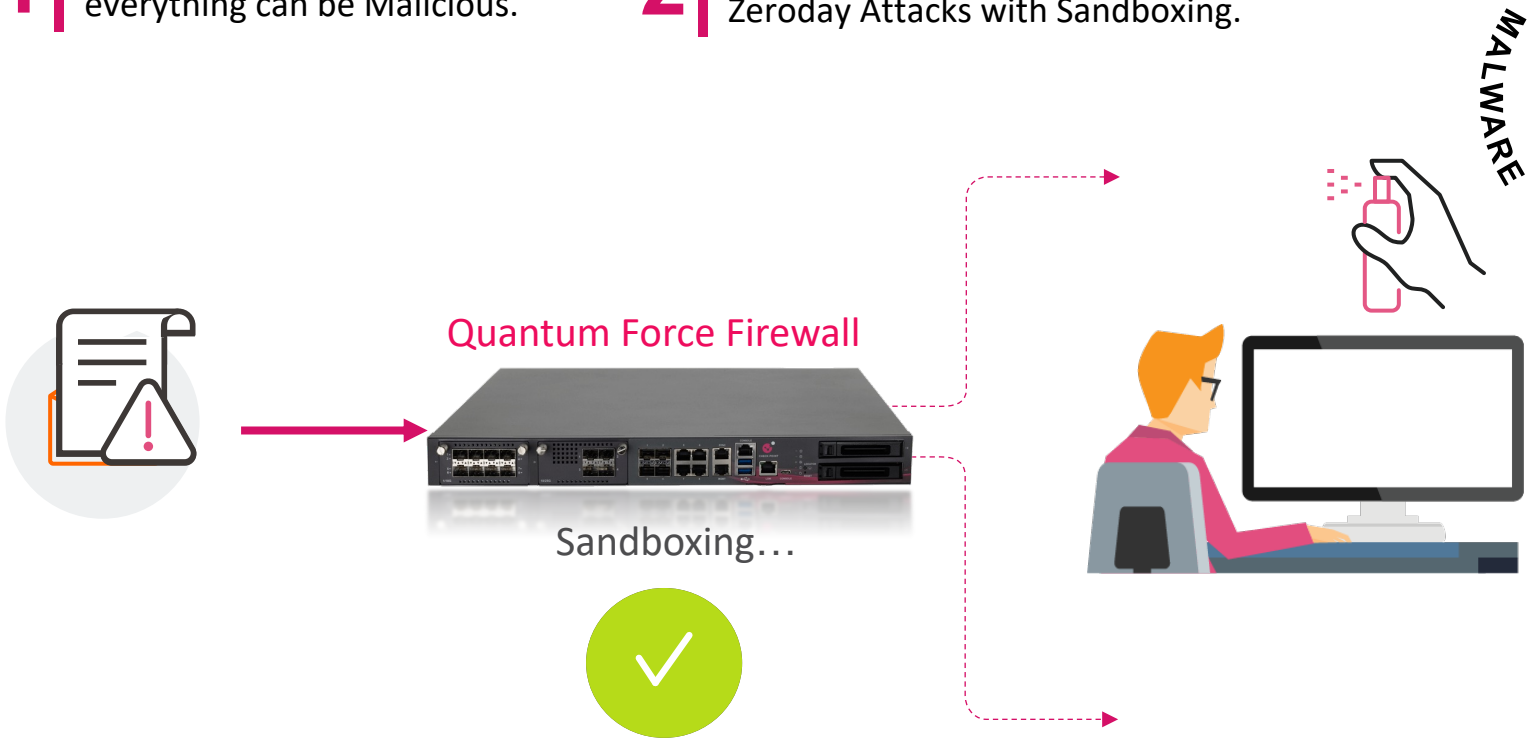
File Protection

Web downloads - Firewall

- Sanitized version available in 1.5 seconds
- Embedded CDR & sandboxing
- Once proven non-malicious, the original file can be downloaded

1 Create A Copy of File. Extract everything can be Malicious.

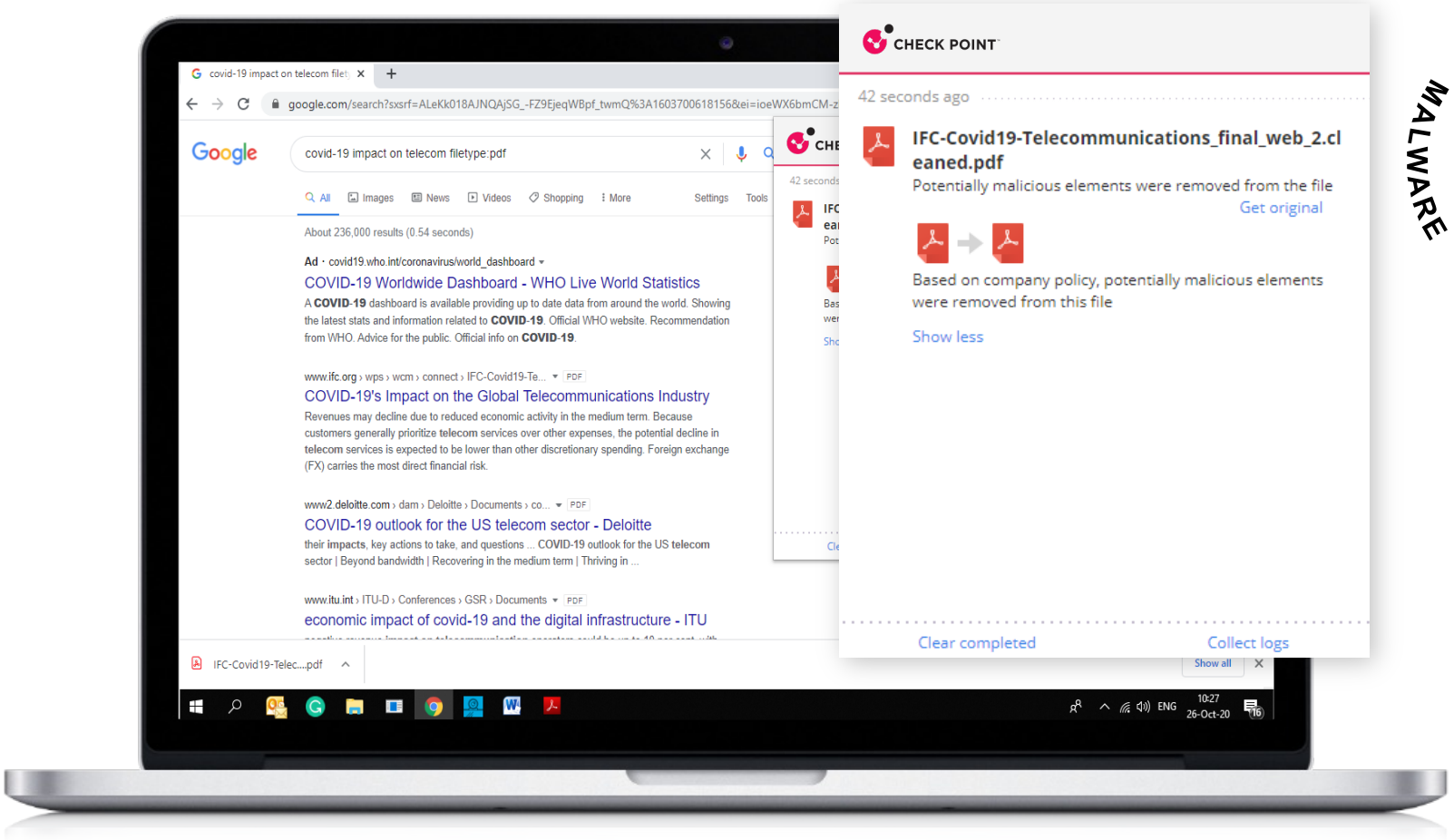
2 In the Background, Scan the File against Zeroday Attacks with Sandboxing.



File Protection

Web downloads - Endpoint

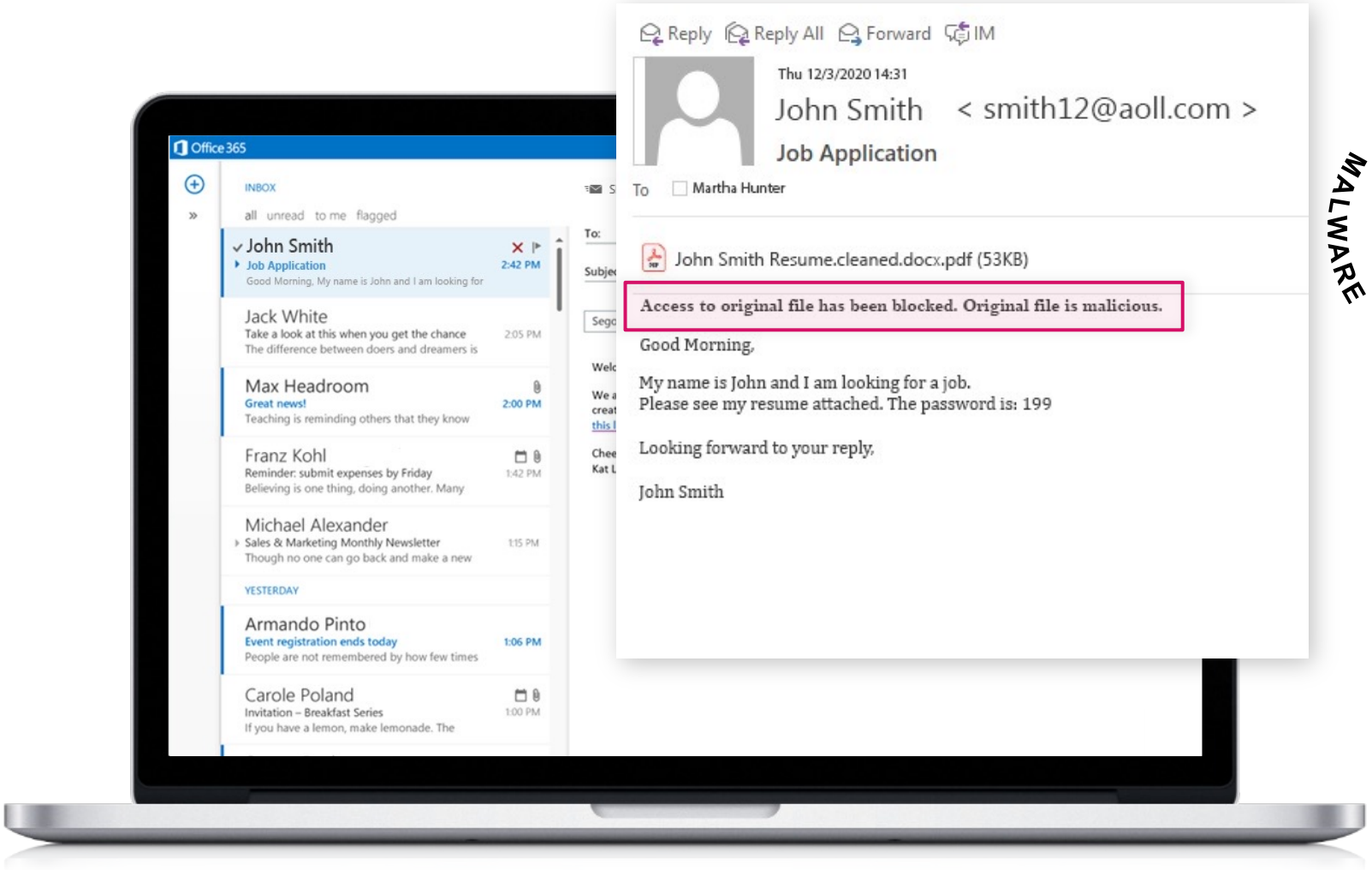
- Sanitized version available in 1.5 seconds
- Embedded CDR & sandboxing
- Once proven non-malicious, the original file can be downloaded



File Protection

Email attachments

- Sanitized version available in 1.5 seconds
- Original file scanned in sandbox for threats
- Once proven non-malicious, the original file can be downloaded



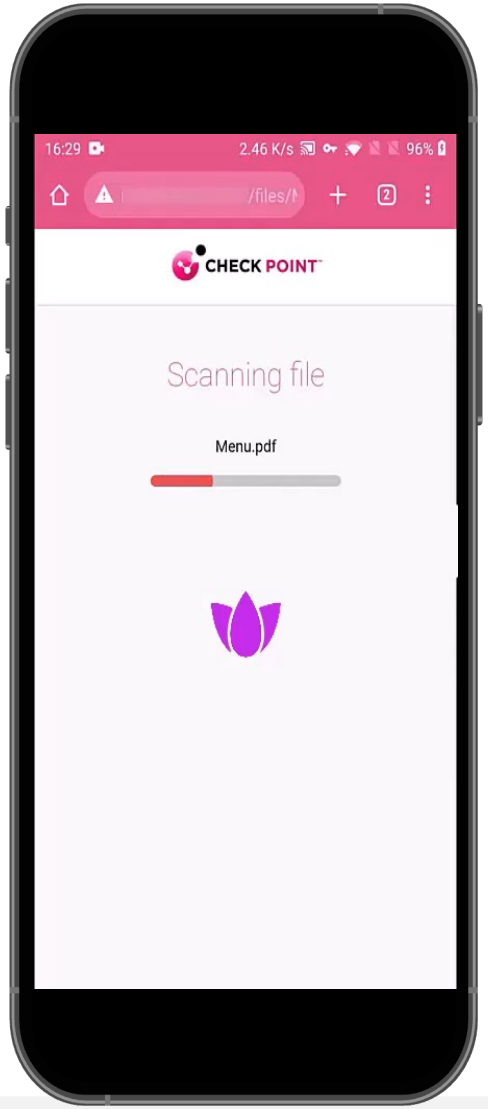
MALWARE

G Suite Office 365 Exchange

File Protection

Mobile downloads

- Supports all file types
- File emulation & sandboxing
- Leveraging ThreatCloud threat intelligence
- Potentially malicious files are blocked

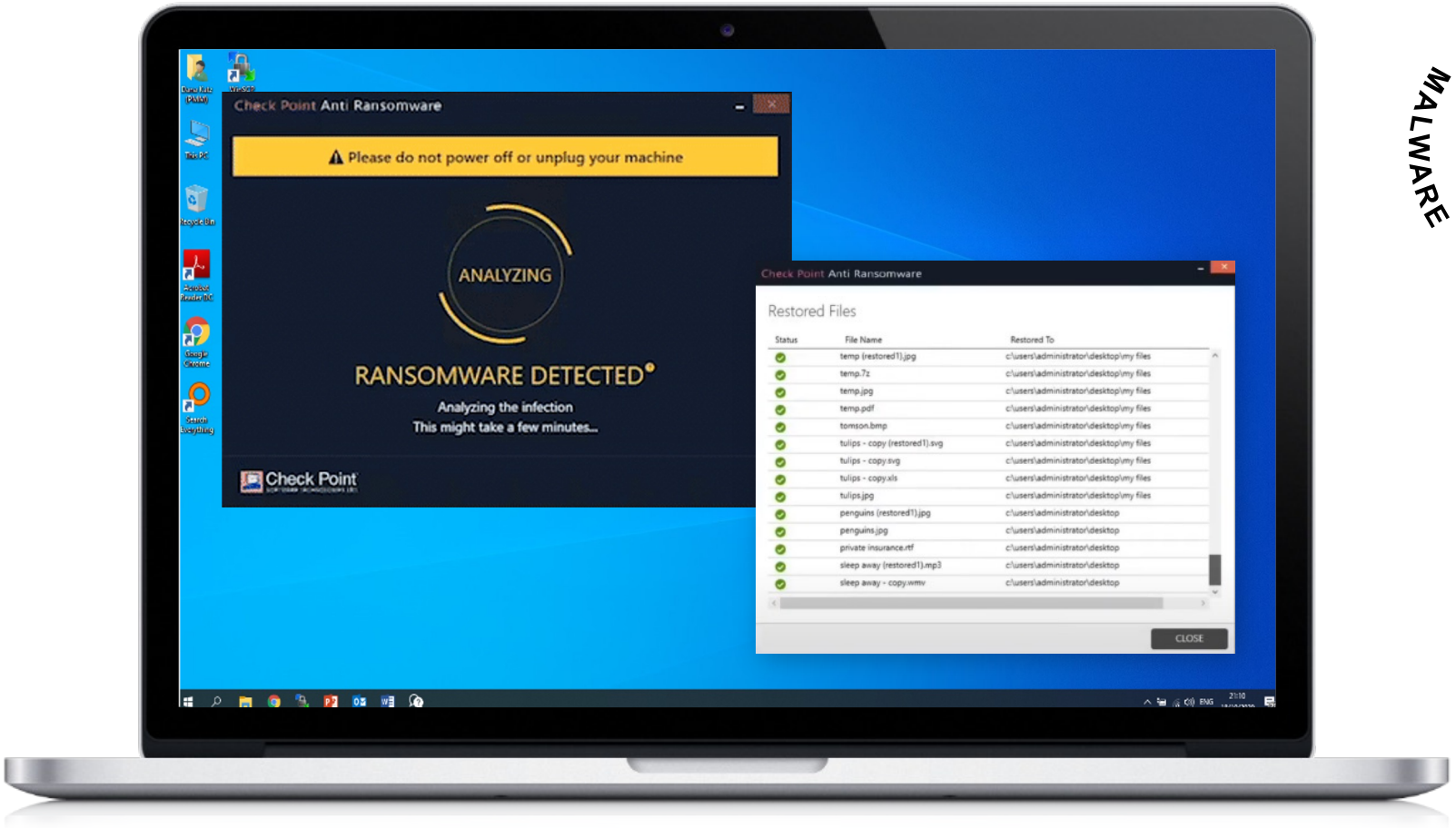


MALWARE

Anti-Ransomware

Run-time protection

- Immediately prevent attacks with behavioral modeling and chip-level protection using Intel TDT
- On-device attack detection & prevention even in offline mode
- Auto recovery safely restores ransomware-encrypted files

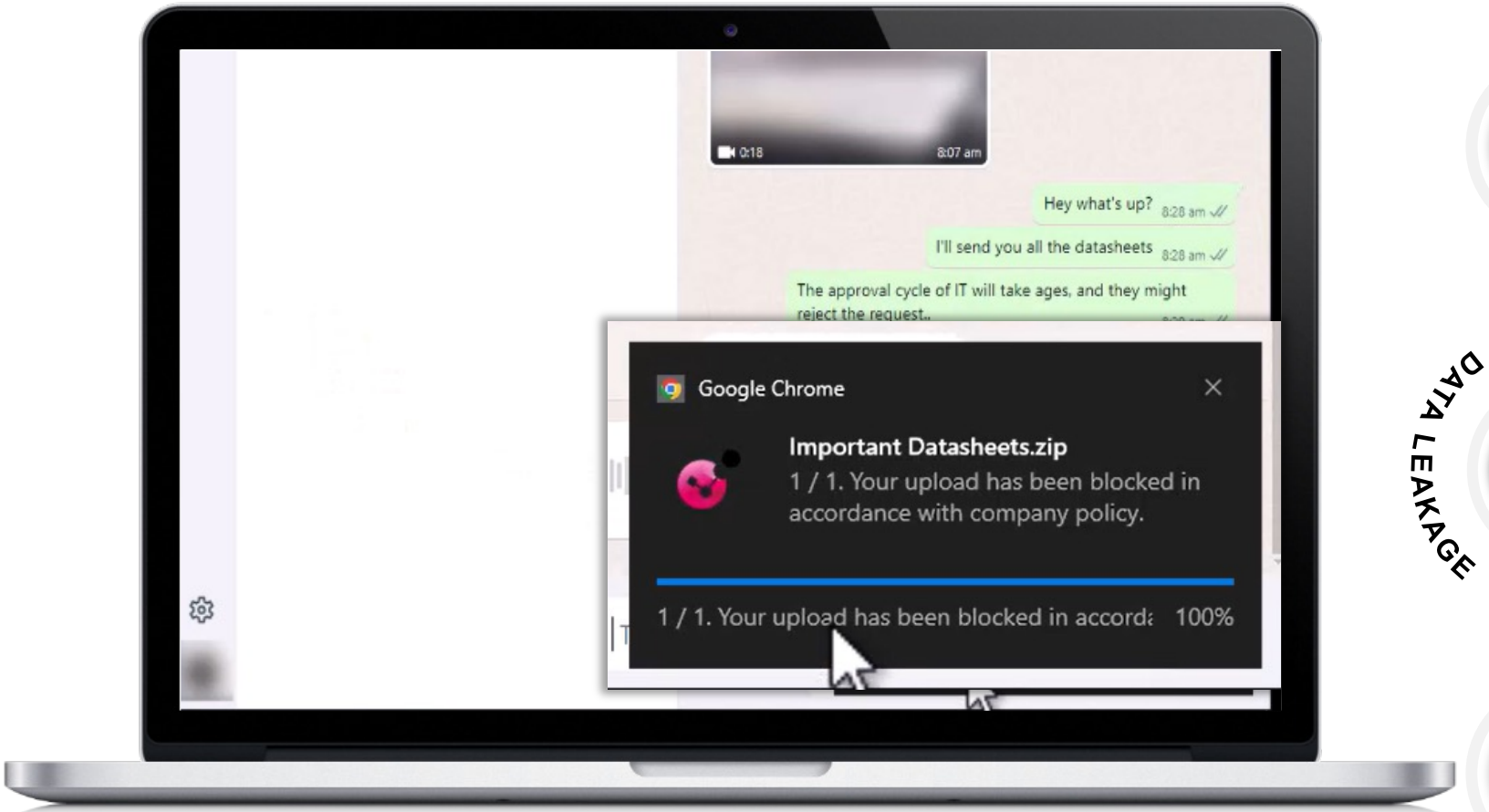


MALWARE

360° Data Loss Prevention

Manage & Protect Data by Policy

- Out of the box pre-defined data types
- Create custom data types & groups
- Define security thresholds

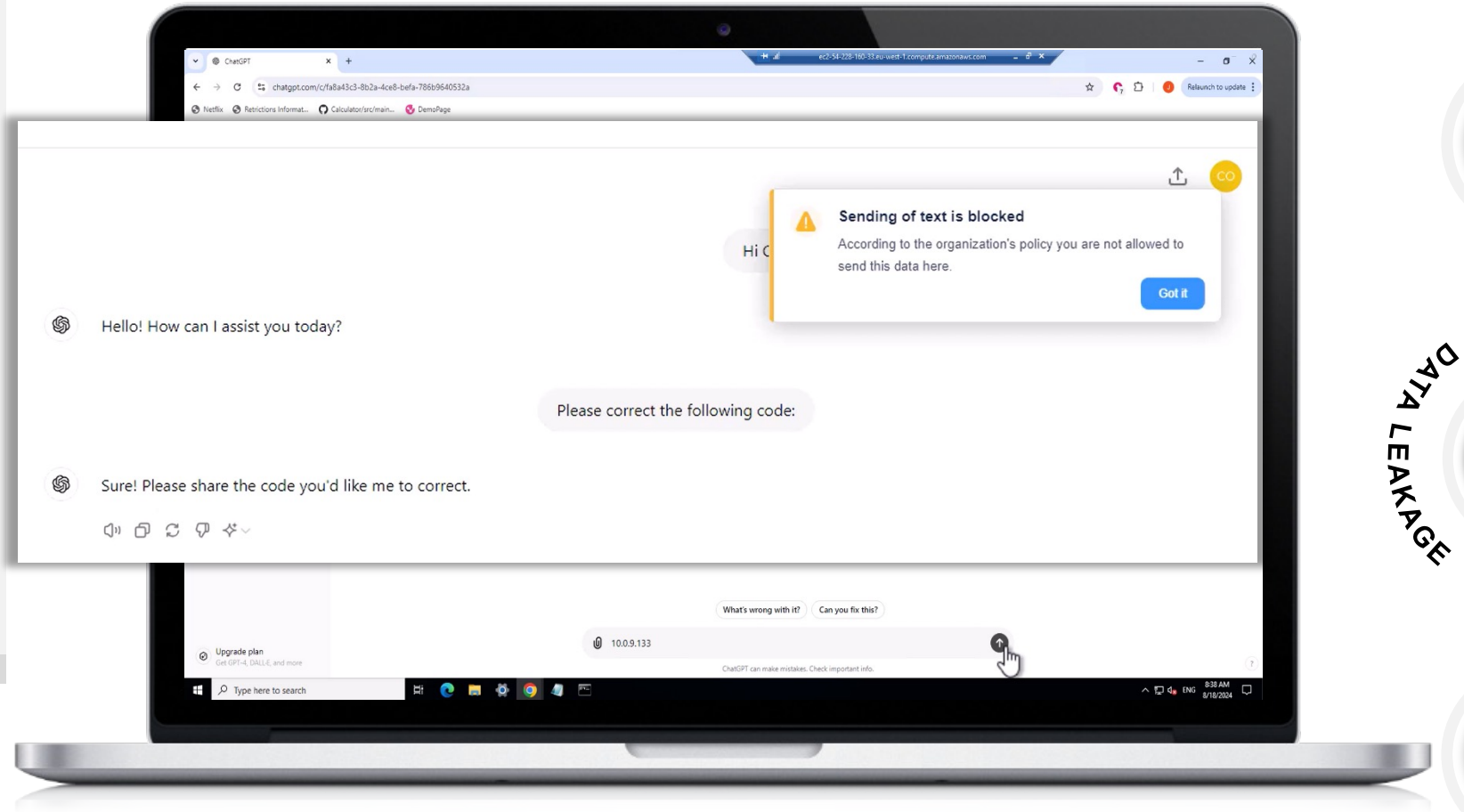


DATA LEAKAGE

360° Data Loss Prevention

Generative AI Security

- Discover generative AI applications & risks
- Real time DLP
- Ensure regulatory compliance

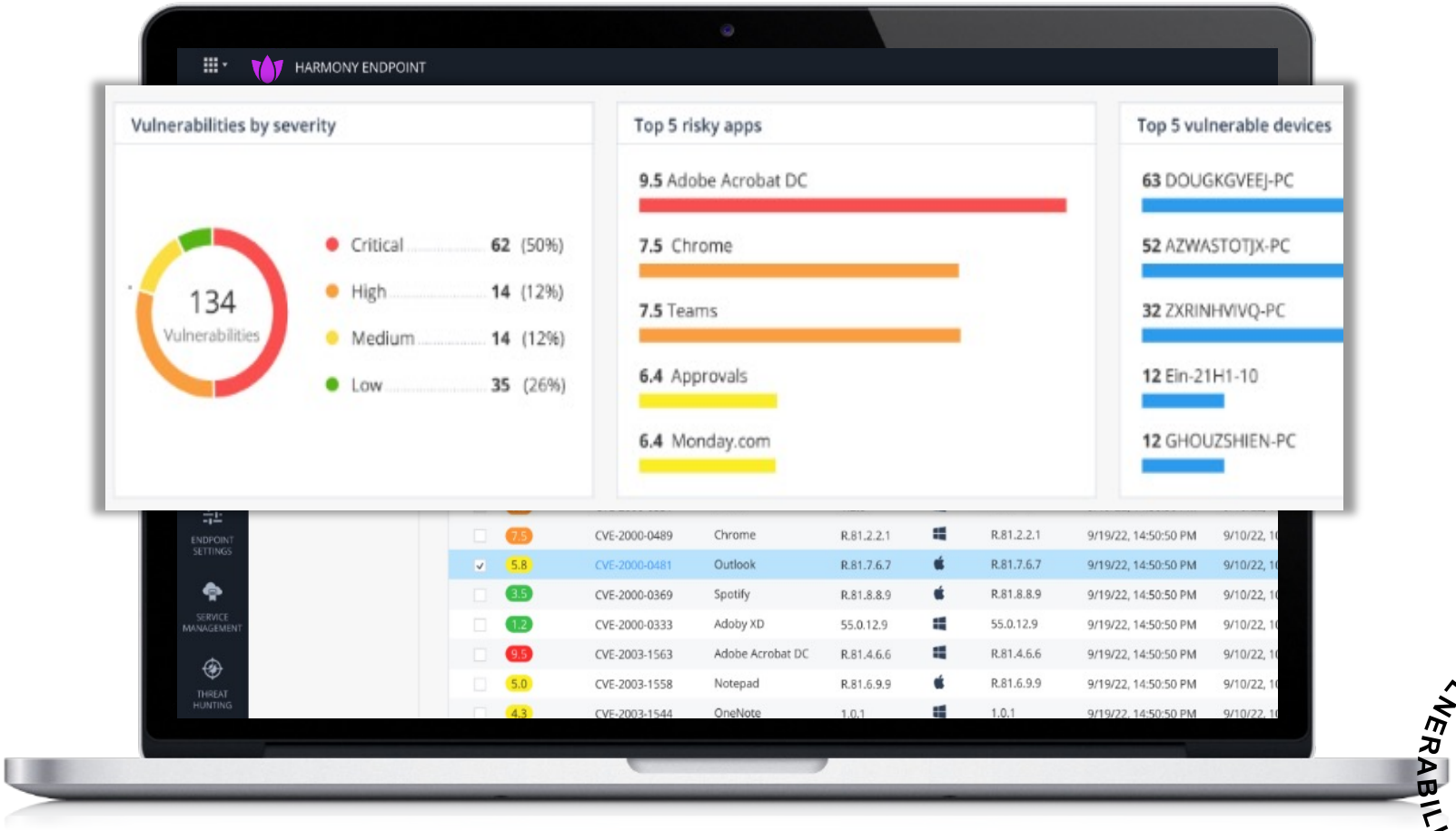


DATA LEAKAGE

Proactively Eliminate Vulnerabilities

On-device attack prevention

- Scan the work environment for vulnerabilities
- Focus on critical vulnerabilities
- Instant patch enforcement

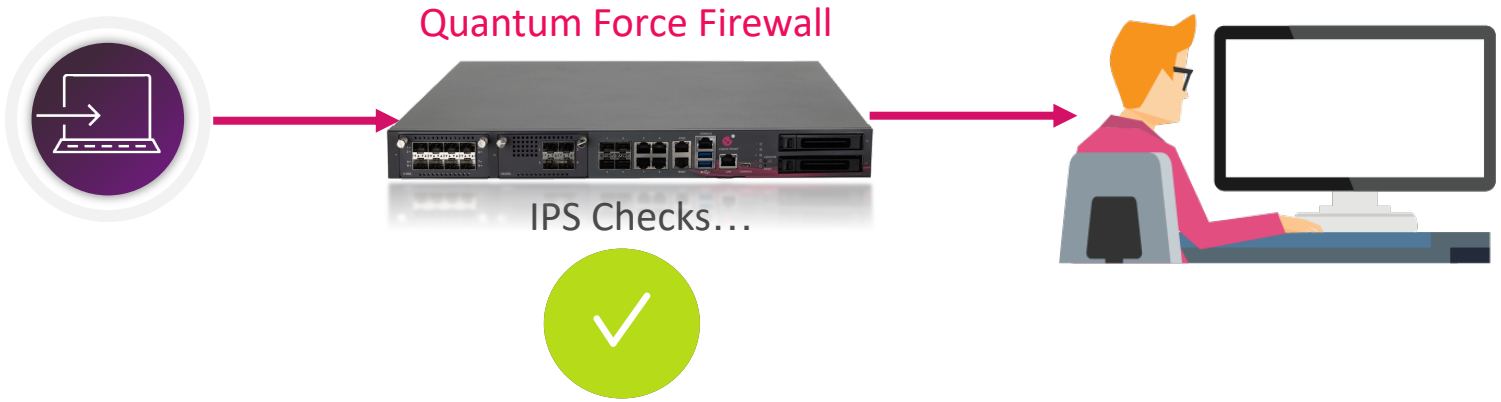


VULNERABILITIES

Actively Prevent Vulnerabilities

Firewall IPS Protection

- Scan the traffic on critical vulnerabilities
- Instant Prevention

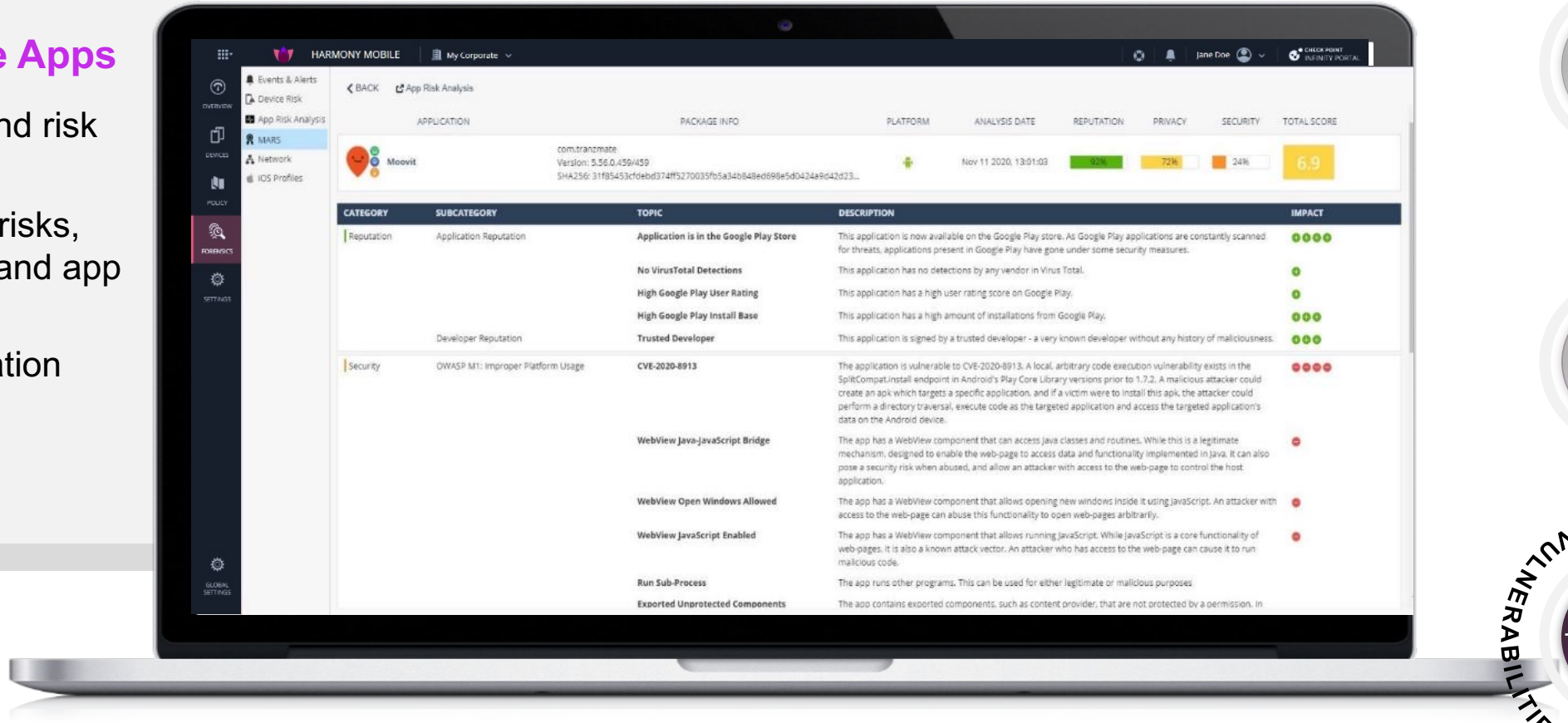


Identify Mobile Application Vulnerabilities

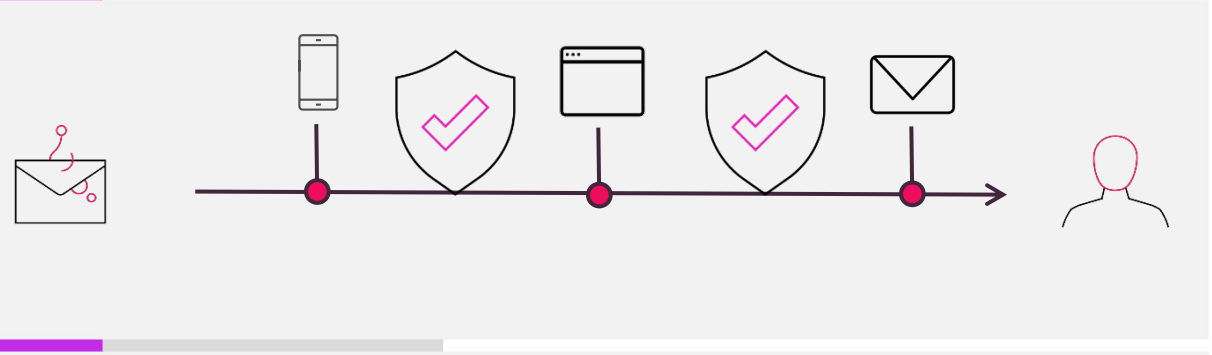
Analyze Mobile Apps

- App overview and risk score
- Identify privacy risks, security issues and app reputation
- Detailed Application Analysis report

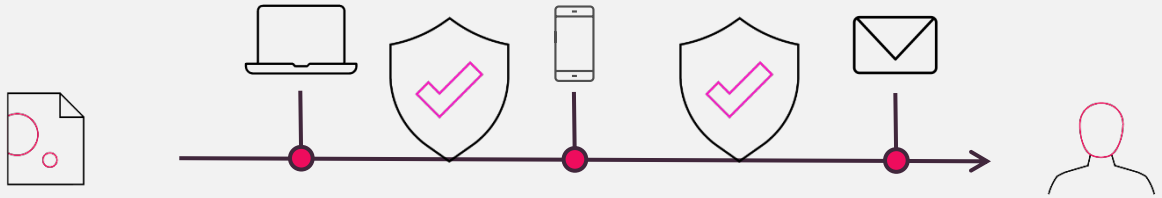
MARS (Mobile Application Reputation Service)



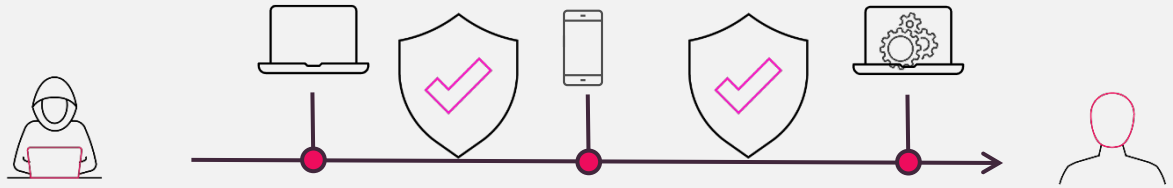
360° Threat Prevention In Action



PREVENT
Phishing Attacks



BLOCK
Malicious Files



STOP
Vulnerability Exploits

- Firewall
- XDR
- Mobile
- Endpoint
- Browser
- Email
- Web Applications
- SASE

Quantum

CloudGuard

Harmony

Check Point Infinity

CHECK POINT

OTD BİLİŞİM
GLOBAL VAD

Thank You!

YOU DESERVE THE BEST SECURITY