CHECK POINT™

Malware 2021 to Present Day

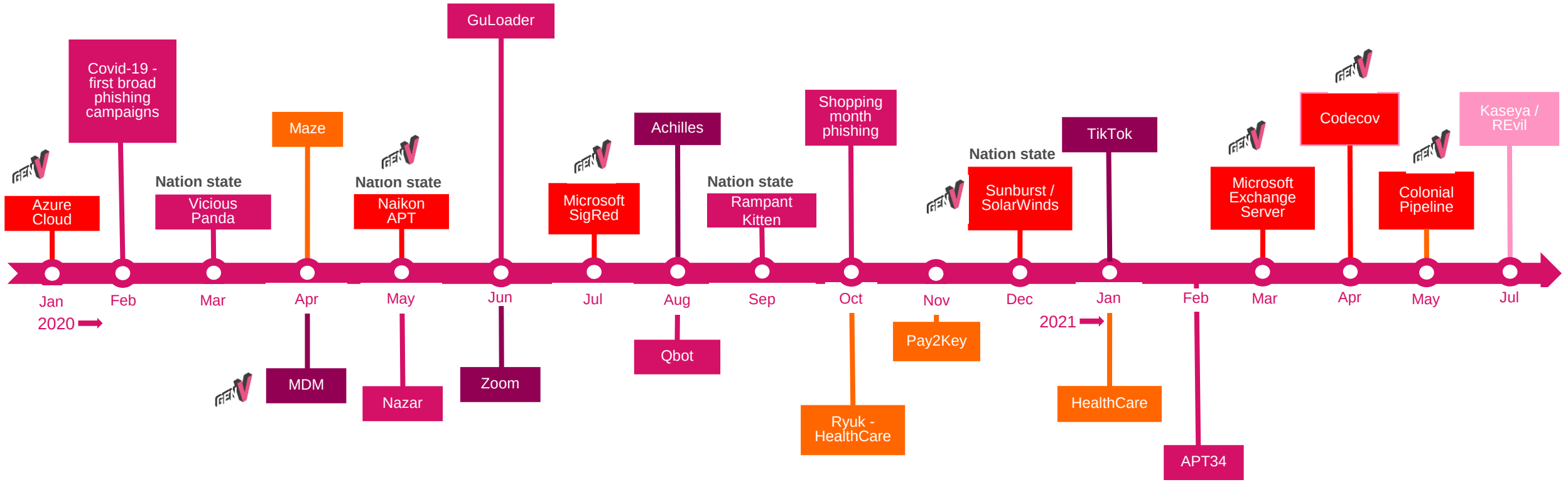
Building a Preventative Cyber Program

Mark Ostrowski | Office of the CTO | Head of Engineering East

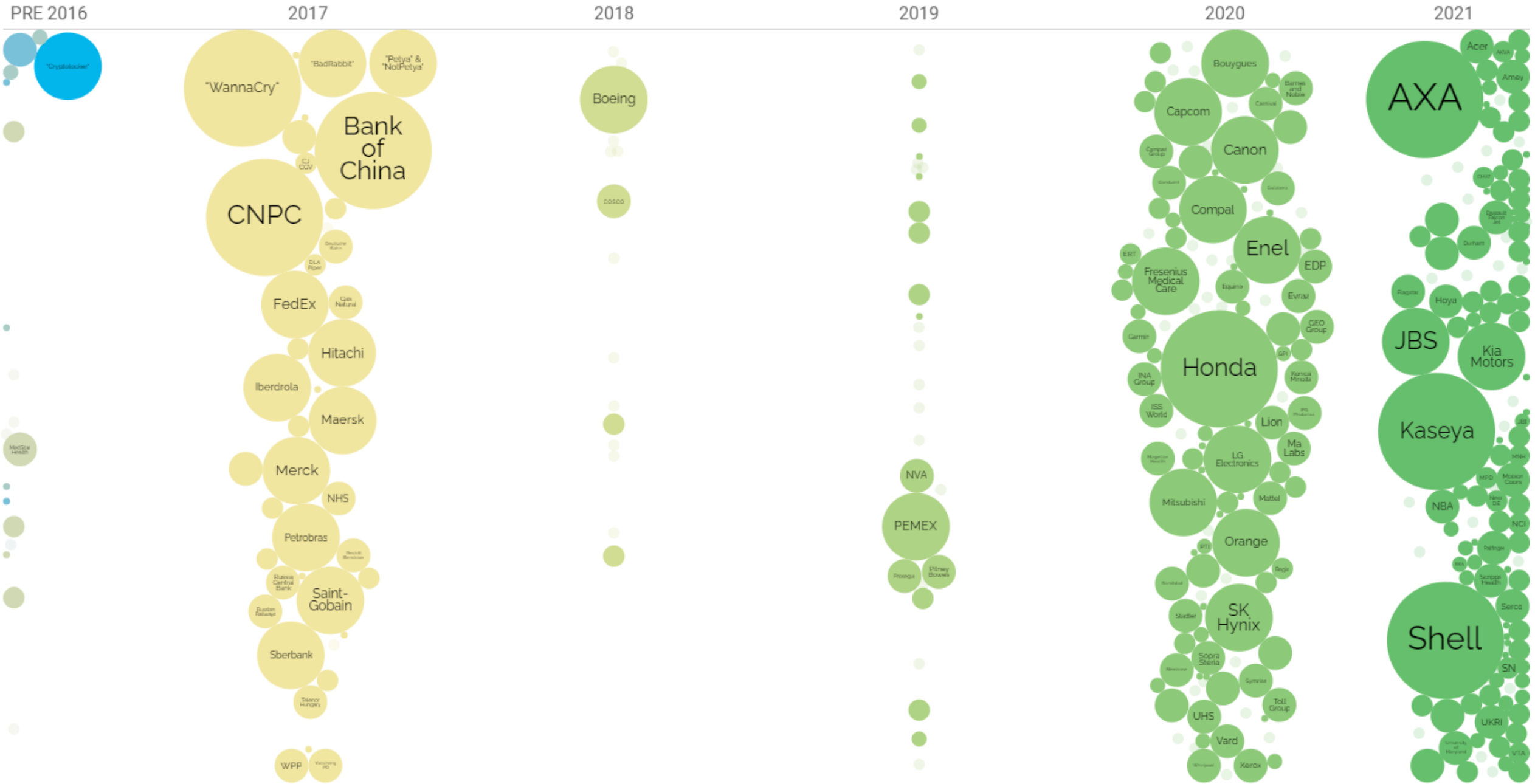
Check Point CHECKMATES

YOU DESERVE THE BEST SECURITY

Since 2020 the attack surface got wider…



Solar winds and the Surge in Gen5 sophisticated attacks


PRE 2016
2017
2018
2019
2020
2021
"Cryptolocker"
"WannaCry"
"BadRabbit"
"Petya" & "NotPetya"
Bank of China
CNPC
FedEx
Hitachi
Iberdrola
Maersk
Merck
NHS
Petrobras
Saint-Gobain
Sberbank
WPP
Boeing
COSCO
NVA
PEMEX
Bouygues
Capcom
Canon
Compal
Enel
Fresenius Medical Care
EDP
Honda
LG Electronics
Mitsubishi
Orange
SK Hynix
UHS
Vard
Xerox
Acer
AXA
JBS
Kia Motors
Kaseya
NBA
Shell
UKRI

Malware 2021

CHECK POINT™

YOU DESERVE THE BEST SECURITY

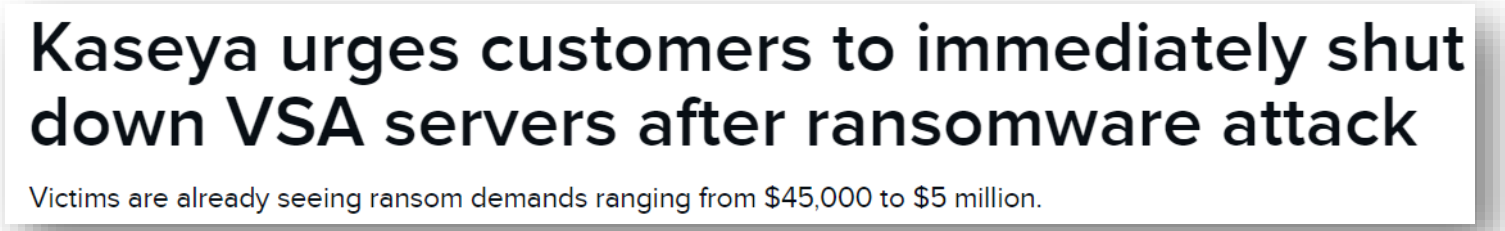
From SolarWinds to Log4j

Software supply chain attacks increased by up to 650% in 2021

- 66% of supply chain attacks leveraging unknown vulnerabilities
- 16% leveraging known software flaws

Most attacks targeted software code

- 82% of the companies provide access to third party vendors
- 76% of the companies provide roles that allow account takeover
- 90% of security teams were not aware such permissions were granted



Kaseya Attack Incident

MSP Solution provider, 1,500 companies were affected in supply chain attack

REvil Ransomware exploited a flaw affecting Kaseya's internet-facing VSA servers.

Luckily - less than 0.1% of the customers were accessed

From SolarWinds to Log4j

Advanced Persistent Threats

- Attack on South Korean software vendor
- Latvian IT attacked using new backdoor “Blindingcan”

Popular NPM package UA-Parser-JS poisoned with cryptomining, password-stealing malware

North Korea's Lazarus Group Turns to Supply Chain Attacks

State-backed group is among a growing number of threat actors looking at supply chain companies as an entry point into enterprise networks.

Ransomware

UNC2465 cybercrime group that is affiliated with the Darkside ransomware gang has infected with malware the website of a CCTV camera vendor.

Cyberattack Hits Multiple Greek Shipping Firms

NPM Package Compromised

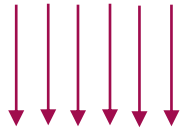
Threat actors NPM account takeover code injection NPM library Facebook, Microsoft, Amazon, Google, Slack affected

Malicious code inserted into three version of the NPM library – Linux and Windows devices infected with crypto miners and password stealers

From SolarWinds to Log4j

October 2021 Nobelium (SolarWinds Attacker) Resurfaces

- Focus on cloud resellers and tech service providers



Log4j Vulnerability

Suspected Russian Activity Targeting Government and Business Entities Around the Globe

Nobelium Espionage Campaign Persists, Service Providers in Crosshairs

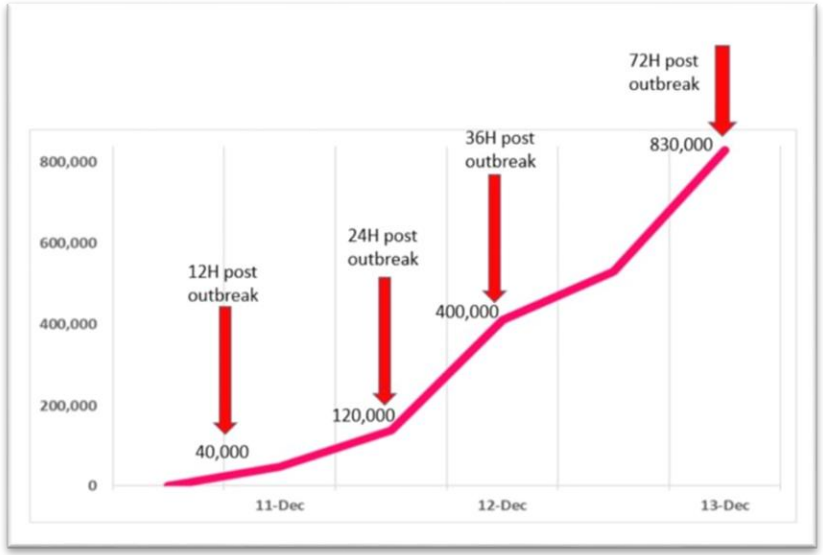
Nobelium compromises at least 14 resellers and IT service providers, Microsoft warns

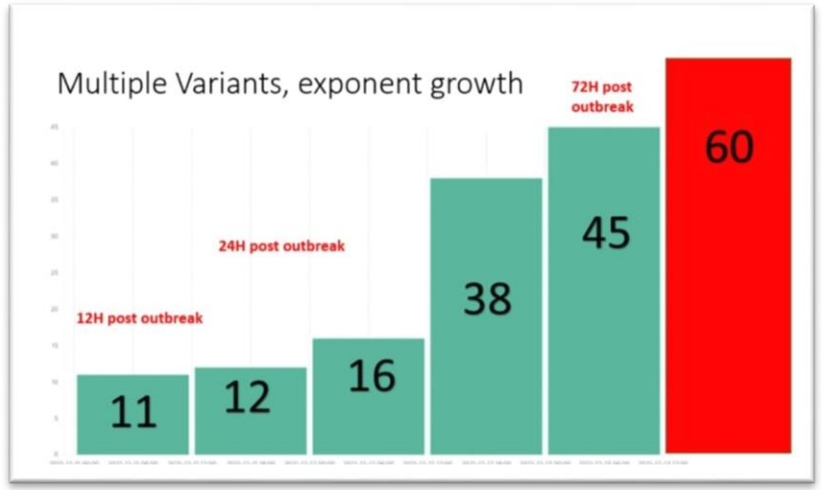
- Apache Log4j open-source Java-based logging package
- Used by millions of Java-based applications worldwide to log activity
- Dec 9th CRITICAL FLAW disclosed by Apache Foundation
- Enables attackers to compromise machines via a single string

LOG4J 2™

CP<R> closely monitored the log4j vulnerability and the attacks exploiting it

- Prevented over **4,300,000 attempts** to allocate the vulnerability
- **Over 46%** of those attempts were made by known malicious groups
- Attempted exploit of over 48% of corporate networks globally
- CPR are first to report how an Iranian APT is leveraging the vulnerability to target Israeli organizations
- **June 2022 – Impacting 43% and most commonly exploited**





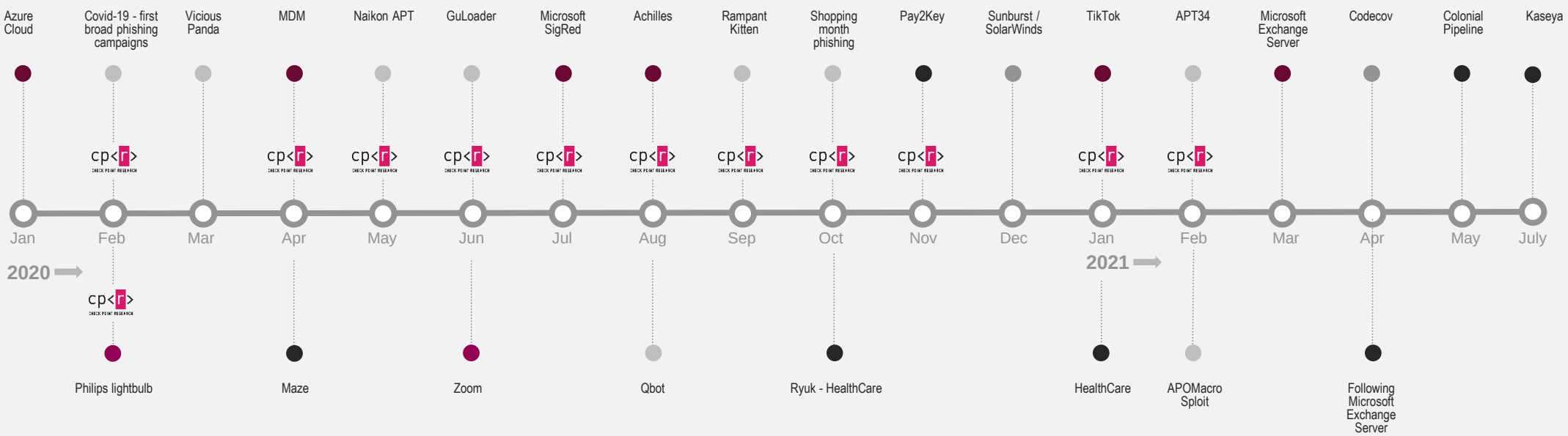
2021’s Threat Landscape Was Exceptionally Dangerous

Every month

10’s of millions of attacks

400K zero days*

- **APT**
- **Supply chain**
- **Ransomware**
- **SW vulnerabilities**



*According to ThreatCloud

TrickBot and Emotet (still most prevalent in 2022)

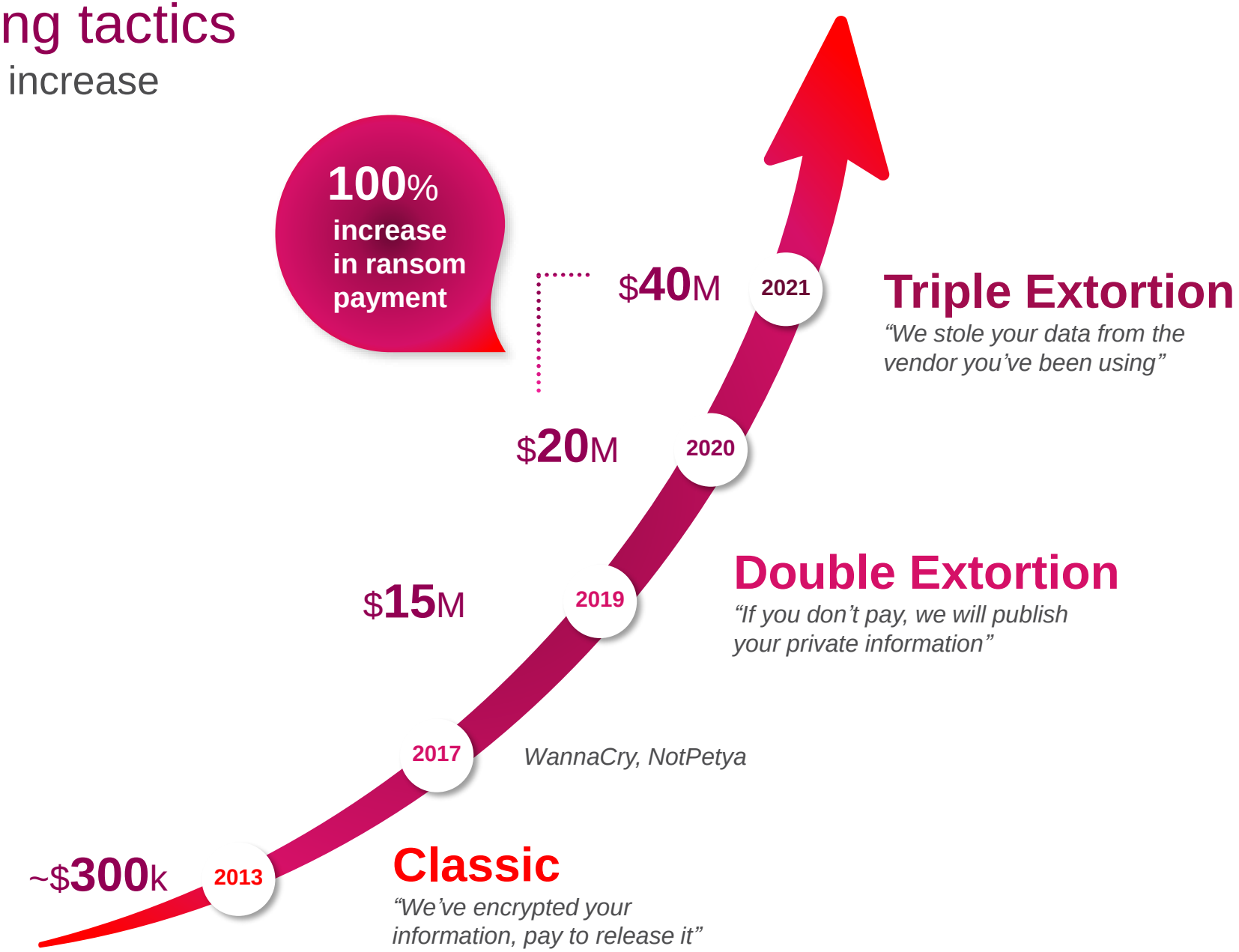
- **Emotet** was the #1 malware in 2020 with 19% global impact
- Takedown January 2021
- Comeback in November 2021
- Ranked #7 in November and #2 in December (after Trickbot)
- In 2021 ranked #4 with 4.9% global impact
- Emotet remains the most prevalent malware as late as March 2022, impacting 10% of organizations worldwide

Threat Actors Target Mobile

- 46% of organizations had at least one employee download a malicious mobile application
- Social Media leveraged for malware distribution
- CPR identifies critical flaw in MediaTek chip
- SMSishing on the rise
- Top mobile malware in 2021
  - Hiddad - 29%
  - xHelper - 17%
  - AlienBot - 13%
  - FluBot - 7% (taken down)
  - **AlienBot, Anubis, MaliBot now top 3 as of June 2022**

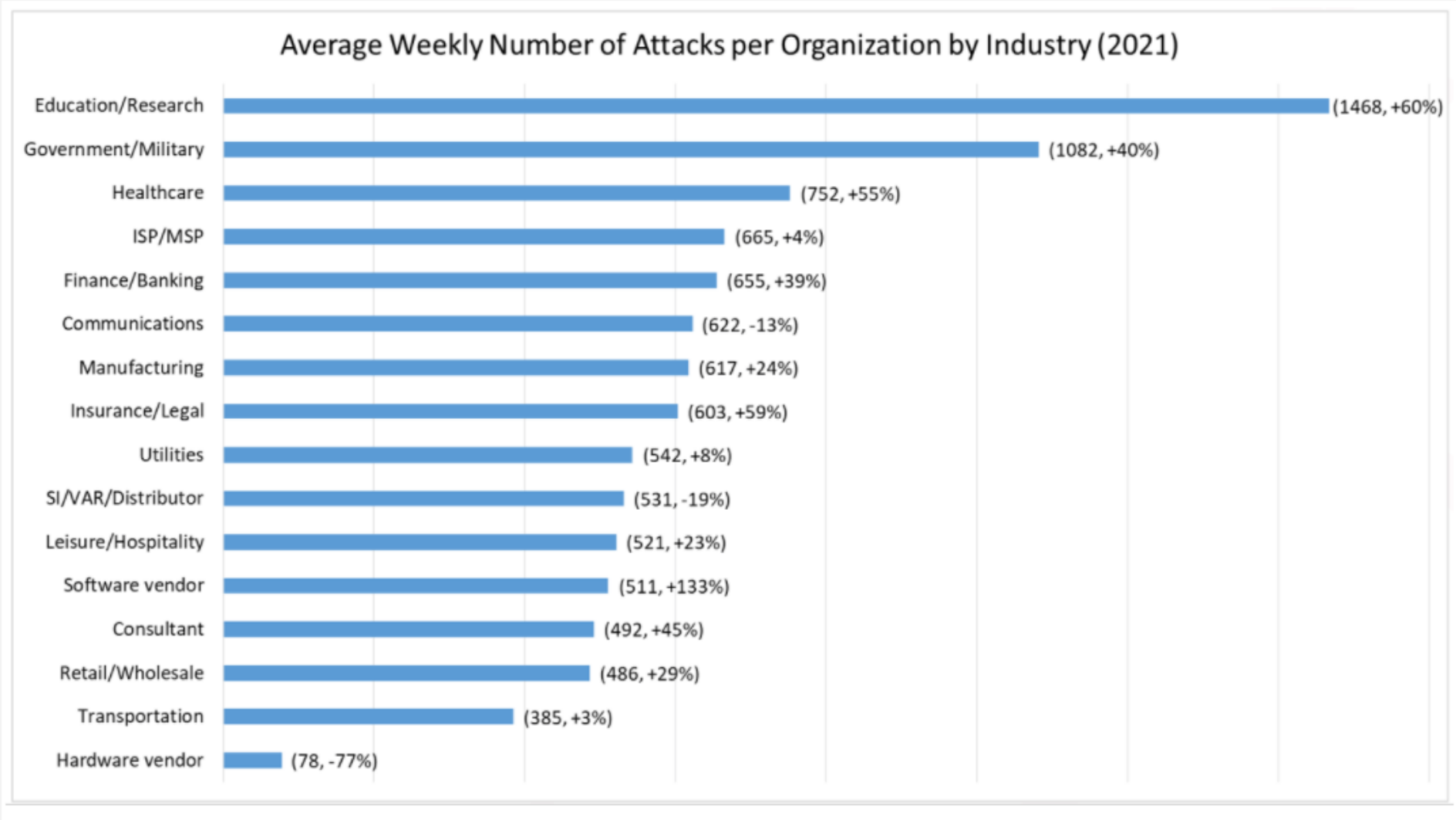
Ransomware evolving tactics

Attack sophistication & cost increase



*June 2020 – June 2021

Every Industry and Vertical Targeted



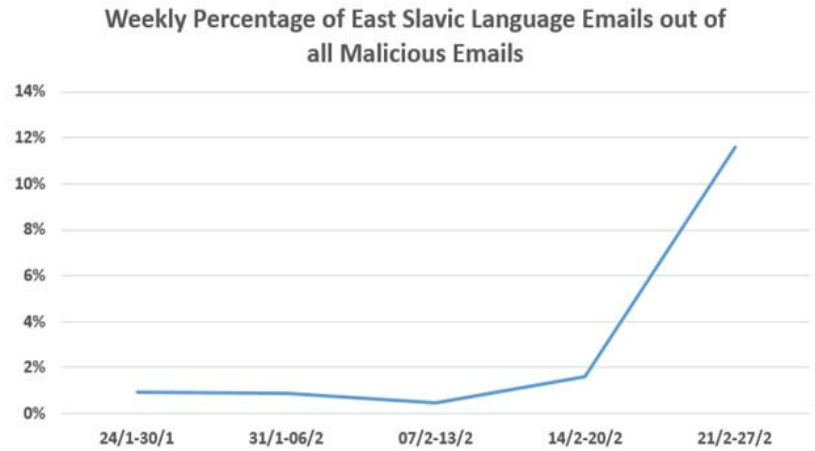
Malware 2022

CHECK POINT

YOU DESERVE THE BEST SECURITY

Cyber Attack Trends In The Midst Of Warfare: the numbers behind the conflict

- Cyber attacks on Ukraine's government and military sector surged by a staggering 196% in the first three days of combat
- Cyber attacks on Russian organizations increased by 4%
- Phishing emails in the East Slavic languages increased 7-fold
- Both Russia and Ukraine saw increases in cyber-attacks of 10% and 17% respectively

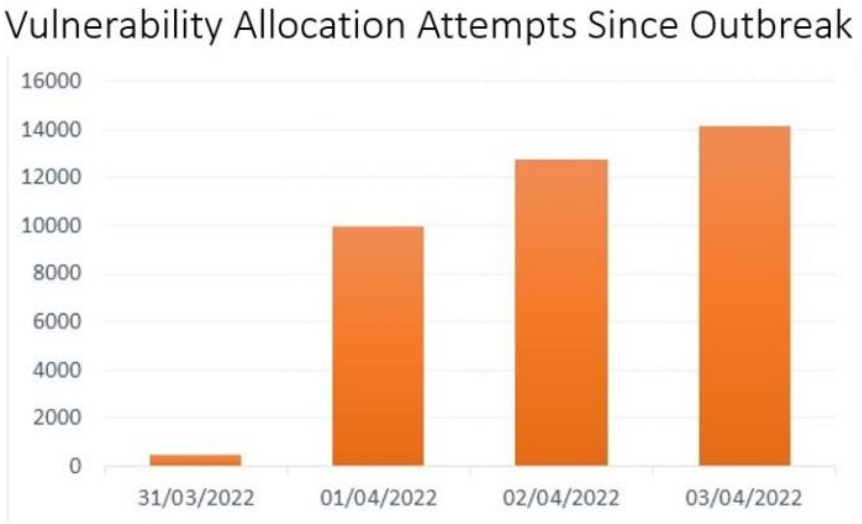


EXCLUSIVE
By
cp<r>
CHECK POINT RESEARCH

Spring4Shell exploitation attempts hit 16% of organizations worldwide

- CPR spots ~37K attempts to allocate the Spring4Shell vulnerability In the first weekend
- 16% of the organizations worldwide impacted by exploitation attempts
- 28% of the organization were impacted in Software vendor sector
- The most impacted region seen is Europe, with an impact of 20%

Check Point customers remain protected, vulnerability does not affect our Infinity portfolio



Check Point Prevents Theft of Crypto Wallets on OpenSea, the World's Largest NFT Marketplace

Investigation led to the discovery of critical security vulnerabilities on OpenSea's platform

- CPR's findings has prevented the thefts of crypto wallets of users
- CPR proved it was possible to steal crypto wallets of users
- CPR collaborated with the OpenSea teams which implemented a fix

EXCLUSIVE
By
cp<r>
CHECK POINT RESEARCH

Check Point Research Reveals Leaks of Conti Ransomware Group

- **Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'**
  - CPR showed organizational structure of Conti, highlighting key groups and people – *some unaware of the nature of their company*
  - Conti group has several physical offices, operates much like a regular tech company
  - Conti's HR team offers monthly bonuses, fines, employee of the month and performance reviews

EXCLUSIVE
By
cp<r>
CHECK POINT RESEARCH

CISA, FBI and NSA 1H 2022 Warnings

- CISA, FBI and NSA warn of nation-state threat actors leveraging custom-made malware dubbed PIPEDREAM to attack ICS/SCADA devices.

- The FBI has issued a warning addressed to the Food and Agriculture (FA) organizations on the greater risks of ransomware attacks during the harvest and planting periods.

- CISA, the FBI and the US Treasury Department alert on the North Korean APT group Lazarus targeting companies in the blockchain and cryptocurrency sectors, using social engineering on employees.

- The FBI warns of Business Email Compromise (BEC) scams which have surpassed $43 billion globally since 2016.

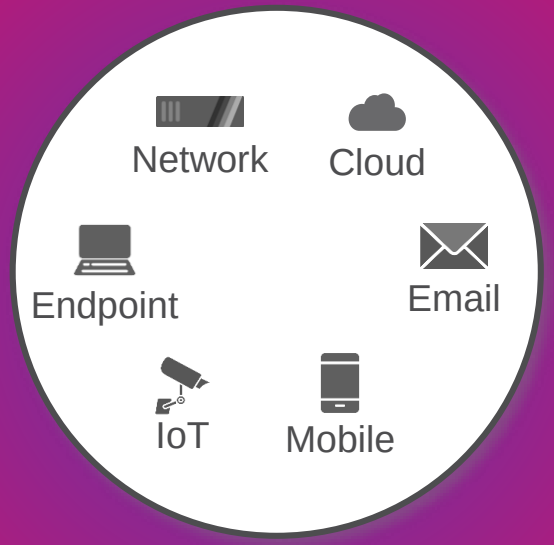
- CISA and other international cyber authorities have released a joint advisory warning of possible threats aimed at managed service provides (MSP) and their clients.

- **Alert (AA22-137A) - Weak Security Controls and Practices Routinely Exploited for Initial Access**

It’s Time to Rethink Your Security Strategy

PROACTIVE

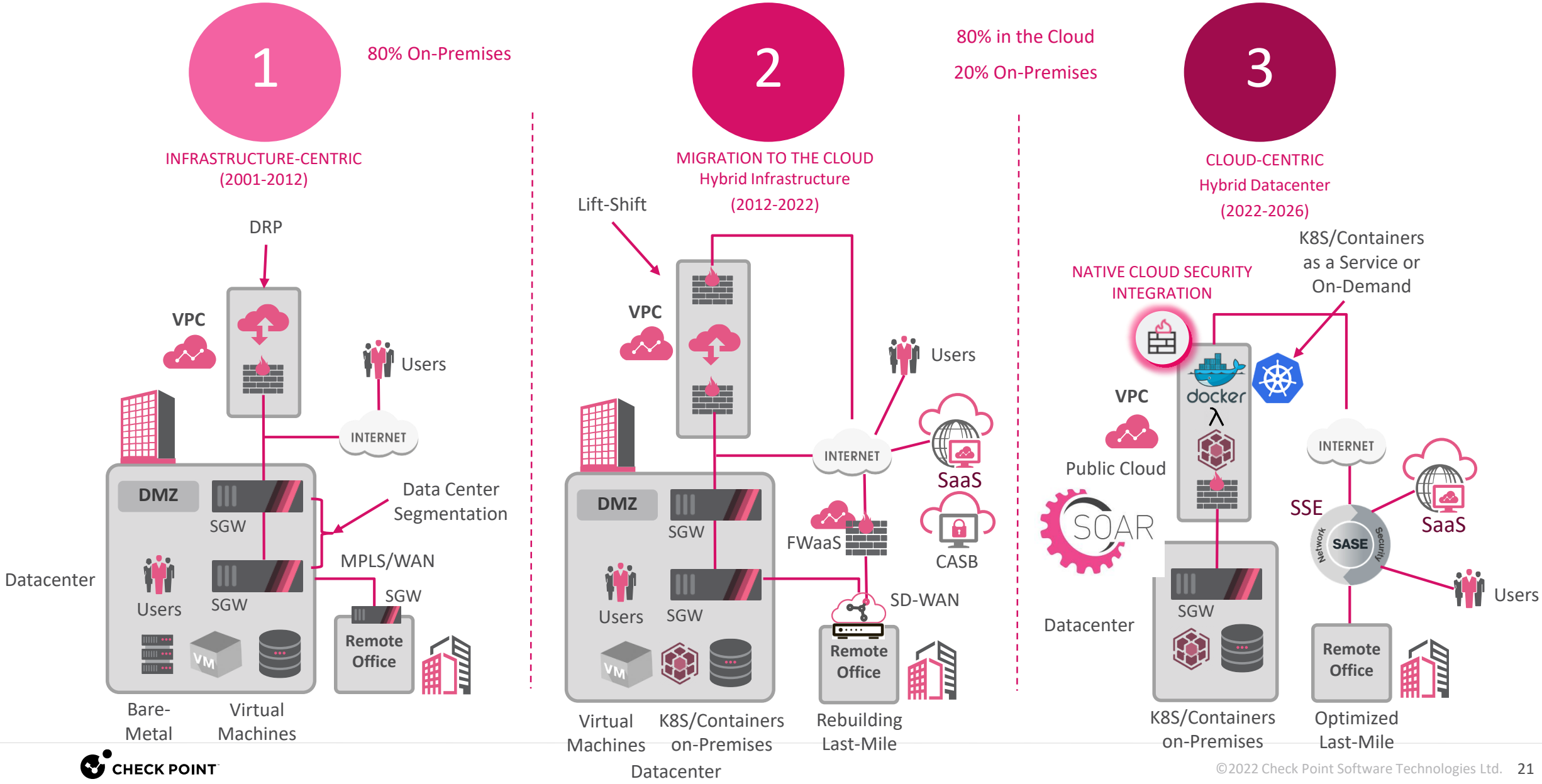
Prevention First!
Block attacks faster
than anyone else



ON DETECTION

Precise Detection
Automatic Remediation
Simple Investigation

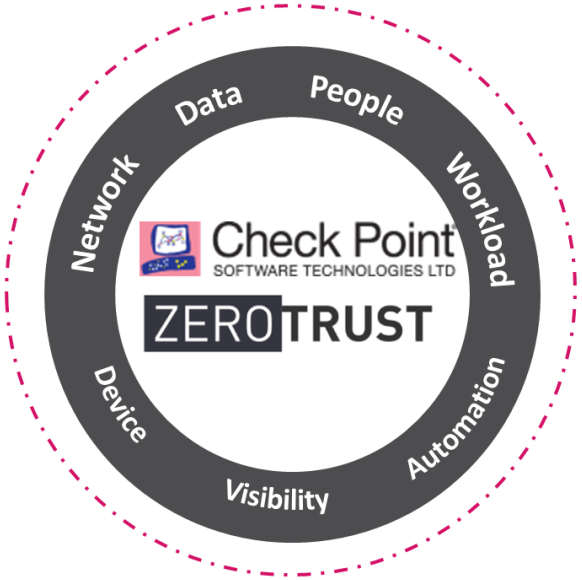
Digital Transformation Journey



Zero Trust is more than 20 years old…

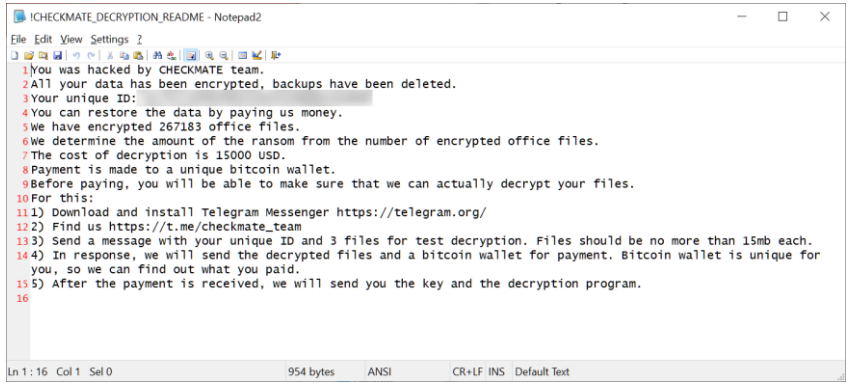
- Still evolving towards not trusting anyone
  - Digital Transformation Journey we have just started to embark on

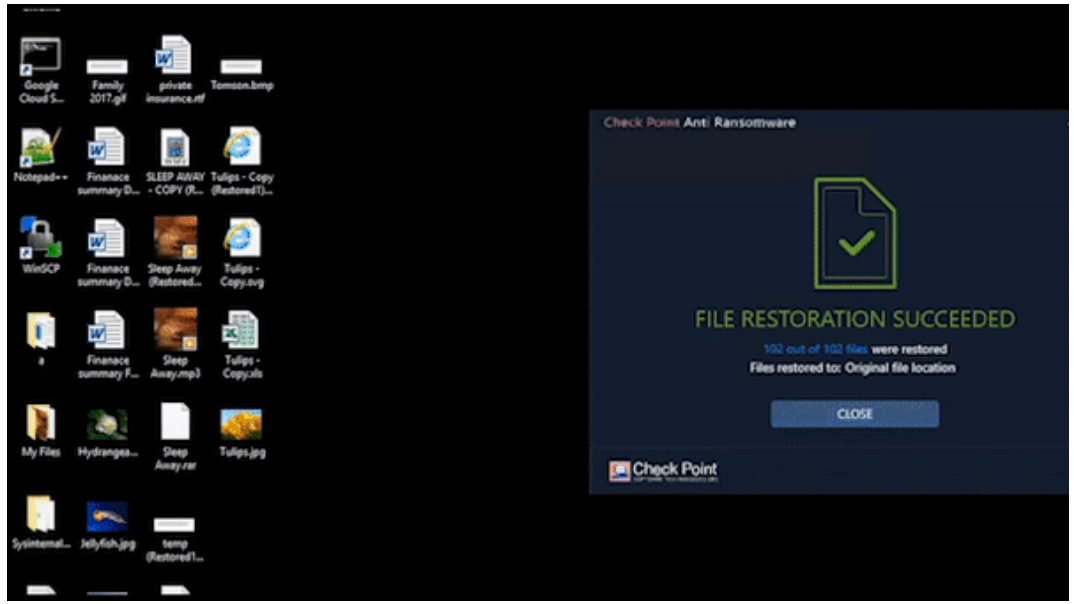
- Simple things still not prevented
  - Trusting SMS for authentication and MFA
  - Email and Phishing still the biggest issue



Ransomware Doesn’t Always Start with Ransomware

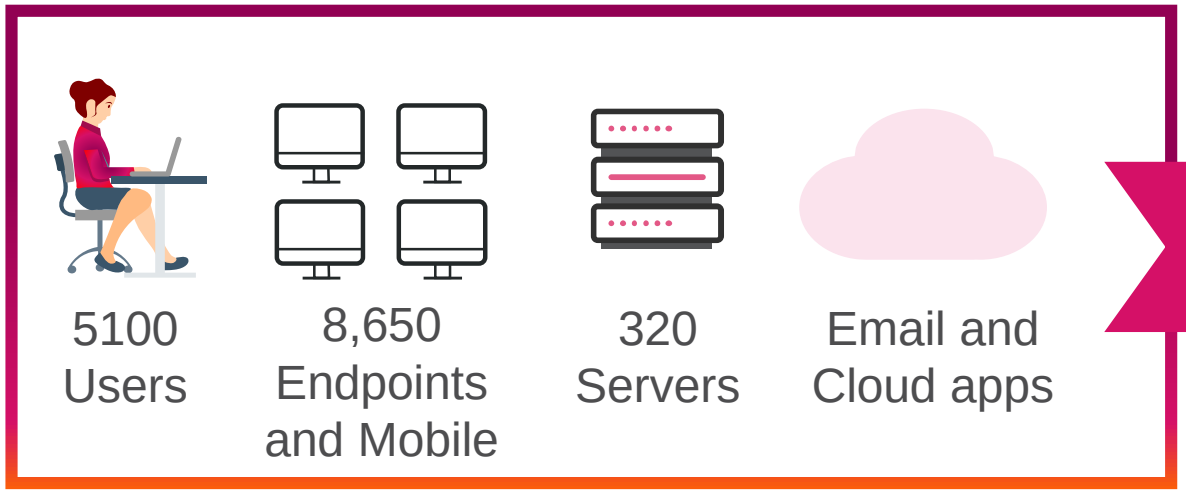
- Beware of other malicious codes (Trickbot or Dridex) that infiltrate organizations and set the stage for a subsequent ransomware attack
- July 2022 Updates
  - AstraLocker shuts down
  - RedAlert and omega launch
  - Checkmate Ransomware attacks SMB





One Week at an Enterprise

Number of Alerts Is Overwhelming



230M Events

7,784 security alerts

3 Security Analysts 5X9

1 SUCCESSFUL INFILTRATION

Sensitive Data Encrypted

What we can do about it

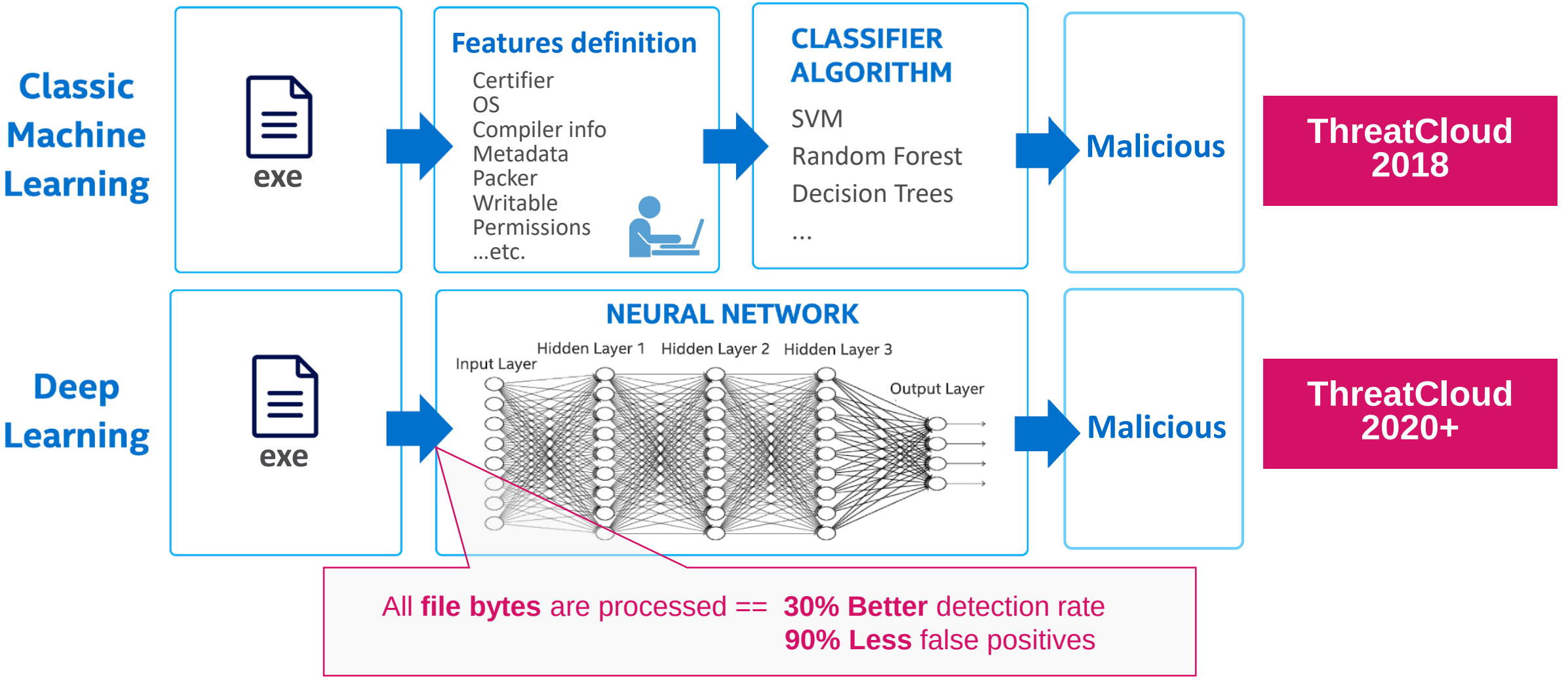
1. **Secure your Users and Access**
   Endpoint is your security edge

2. **Secure your Cloud**
   The entire SDLC – Code to Runtime

3. **Secure your Network**
   The network is everywhere

Start the Best Prevention with Cutting Edge Technologies

Classic Machine Learning vs. Deep Learning



Check Point Threat Cloud - AI-driven Prevention

60+
AI & Traditional Engines

- Visual Similarity Deep Learning
- Vectorization Classifier
- Metadata Analyzer
- In-Memory Emulation Machine Learning
- Machine-generated Signatures
- Machine-generated Intelligence
- Static Analysis Machine Learning
- Code Flow Analyzer Machine earning
- Malware Classifiers
- Code Flow Analyzer
- On-Device Behavior Analysis
- Smart Backup and Restoration
- Anomaly Detection
- Zero Phishing
- Macro Analyzer
- Similarity Models

2021 Check Point ThreatCloud Statistics

Inspected

- **1 Trillion** website visits and links
- **210 Billion** file downloads and attachments

Prevented

- **6.8 Billion** malicious website connections
- **185 Million** malware downloads
- **778 Million** vulnerability exploit attempts

Check Point catches what everyone else missed

3 Examples of malware variants detected by ThreatCloud before VirusTotal

TRICKBOT

12 days
before VirusTotal

ZLOADER

15 days
before VirusTotal

HANCITOR

17 days
before VirusTotal

THREATCLOUD

HAVE THE BEST AND 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

Check Point Managed Detection and Response

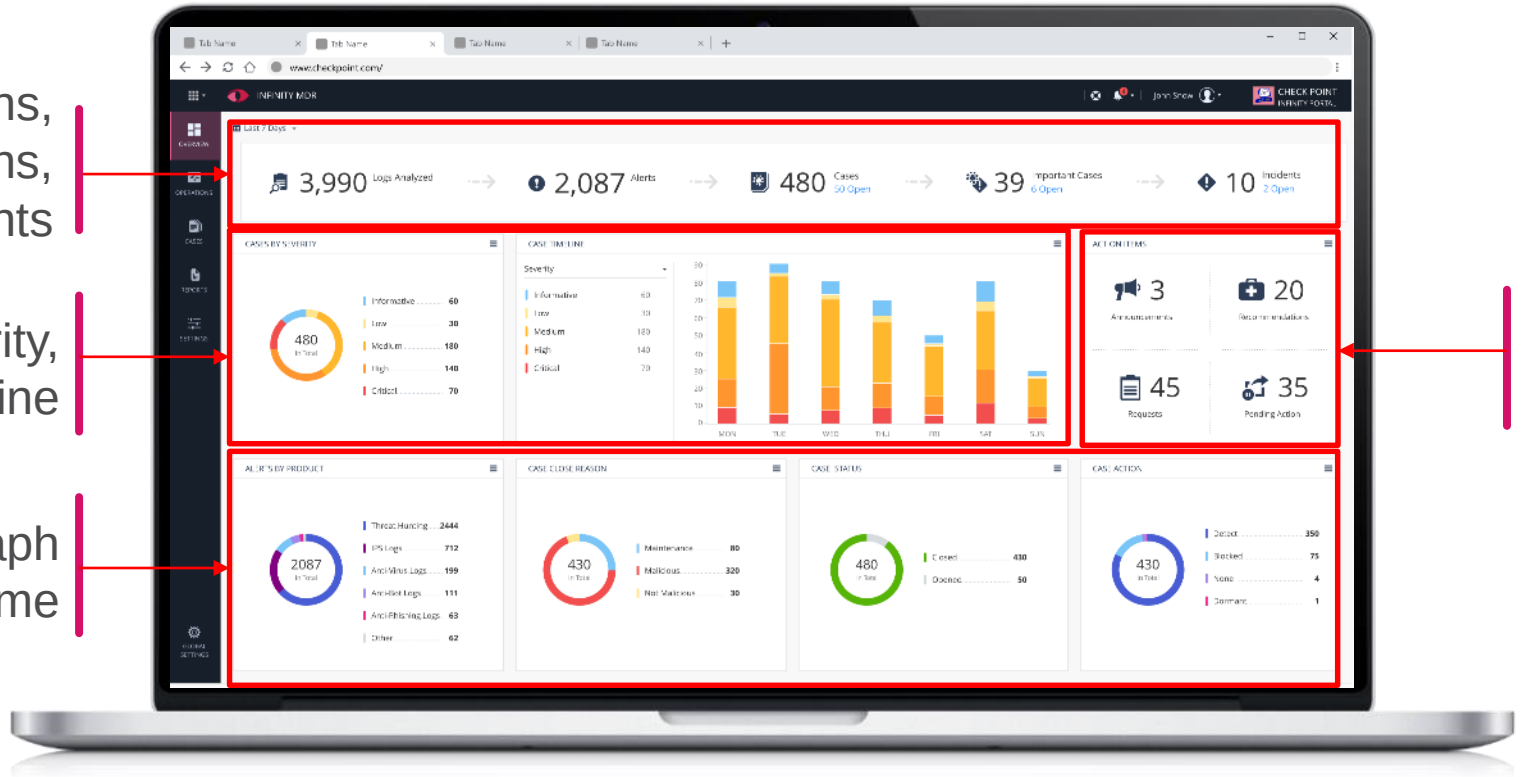
Intuitive Web Portal Providing You a Detailed View of All Incidents, Threat Analysis, and Security Recommendations

Customer Level Overview

Quick overview of actions, recommendations, Important cases, incidents

Cases by severity, and case timeline

Core status graph view based on time



Action items summary

Protect your organization from GenV Attacks

- **Deploy Anti-Ransomware** solution on all your end-point devices
- **Prevent malicious attachments** from reaching your corporate emails
- **Prevent users from downloading malware & Zero-Days** from the internet and private emails
- **Inspect traffic**, files and updates used by your internet facing applications
- **Block infected machines** from communicating with C&C
- Exercise and implement **Incident response** to call in the case of emergency

Cybercriminals Find New Opportunities in 2022:
Deepfakes, Cryptocurrency and Mobile Wallets

- Fake news 2.0 and the return of misinformation campaigns
- Supply chain cyber-attacks continue to grow, and governments will address the challenge
- The cyber ‘war & pandemic’ intensifies
- Data breaches are larger scale and more costly
- Mobile malware attacks increase as more people use mobile wallets and payment platforms
- Cryptocurrency becomes a focal point for cyberattacks globally
- Attackers leverage vulnerabilities in microservices to launch large scale attacks
- Attackers weaponize deepfake technology

Thank You & Questions

YOU DESERVE THE BEST SECURITY