Check Point Infinity SOC Webinar
14. & 19. Januar 2021

Check Point SOFTWARE TECHNOLOGIES LTD | CHECK POINT INFINITY SOC

INFINITY SOC

ACHIEVING SOC CERTAINTY

Stéphane Badan | Security Engineer

OUR STORY BEGINS
WITH A EUROPEN BANK

5,000
Employees

€1.1B
Revenues

2 SECURITY OPERATION MANAGERS
SOC WORKING HOURS: 8:00- 17:00

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

AND YET, ONE DAY……

23
FEBRUARY
2020

- Ryuk ransomware outbreak
- 500 critical systems are down
- 3 branches are completely paralyzed

EMERGENCY CALL

INCIDENT RESPONSE TEAM
CHECK POINT

Check Point SOFTWARE TECHNOLOGIES

 3

HOW DID THIS HAPPEN?

THE ANATOMY OF THE ATTACK

INCIDENT RESPONSE TEAM
CHECK POINT

Spear-phishing email leads to **Trickbot Trojan** Infection

Trickbot lateral movement infects 500 hosts

Threat actor uses **Trickbot** to deploy **Ryuk ransomware**

Oct 2019 | Nov 2019 | Dec 2019 | Jan 2020 | Feb 2020

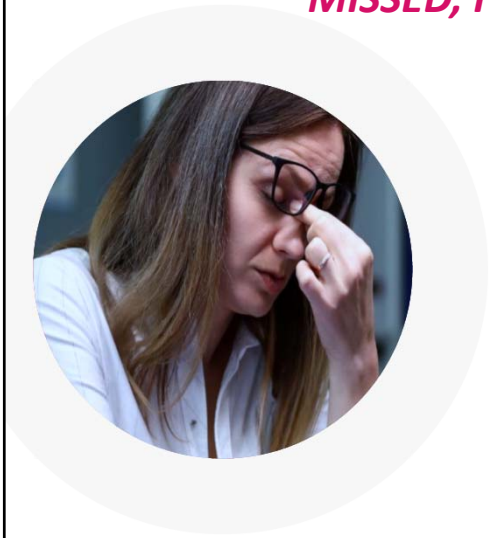
Check Point SOFTWARE TECHNOLOGIES

 4

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

"THINKING ABOUT WHAT WE'VE PROBABLY MISSED, HAS KEPT US UP AT NIGHT"



"Too many false positives leading to time-consuming investigation"

"Thousands of new alerts everyday create a never-ending backlog"

"Piecing together information from multiple monitoring tools is a nightmare"

Check Point SOFTWARE TECHNOLOGIES

 6

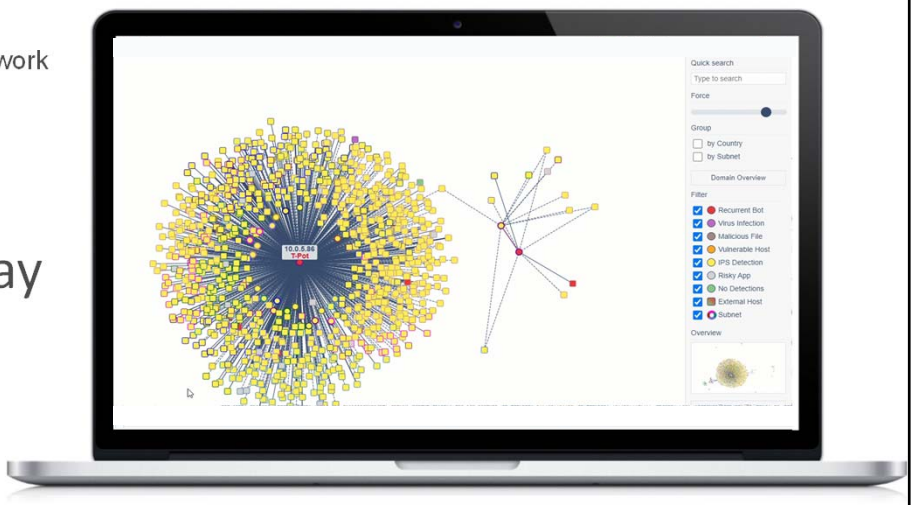
AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

SOC DAILY ROUTINE:
FINDING A NEEDLE IN A HAYSTACK

Typical medium sized network
2,000 Users

10 Million
logs every day



Check Point SOFTWARE TECHNOLOGIES

 7

YOU DESERVE
CERTAINTY

Check Point SOFTWARE TECHNOLOGIES

 8

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

CHECK POINT
INFINITY SOC

ACHIEVING SOC CERTAINTY

99.9 % PRECISION

Expose and shutdown only real attacks, inside and outside the organization.

RAPID INVESTIGATION

With the industry's most powerful threat intelligence.

ZERO FRICTION

No deployment, integration and privacy pains.

Check Point SOFTWARE TECHNOLOGIES

 9

CHECK POINT
INFINITY SOC

ACHIEVING SOC CERTAINTY

99.9 % PRECISION

Expose and shutdown only real attacks, inside and outside the organization.

RAPID INVESTIGATION

With the industry's most powerful threat intelligence

ZERO FRICTION

No deployment, integration and privacy pains

Check Point SOFTWARE TECHNOLOGIES

 10

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

PRECISION
FROM MILLIONS OF LOGS TO ONLY REAL ALERTS

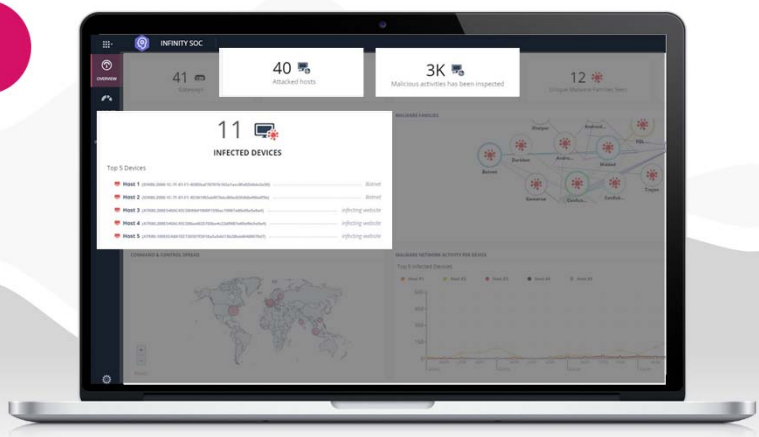
IN AN AVERAGE WEEK:

59,000,000
logs across endpoint, network, cloud, mobile and IoT

3,000
Malicious activities

40
Targeted assets

11
Infected assets



Check Point SOFTWARE TECHNOLOGIES

 11

PRIORITIZATION
RESPOND INTELLIGENTLY BASED ON SEVERITY AND PROBABILITY

AUTOMATED TRIAGE

99% TRICKBOT MALWARE
99% — Host #1 — 6:58, 6/20/2020
Host 1 might be infected with Trickbot (High probability)

99% ADWARE
99% — Host #2 — 6:58, 6/20/2020
Host 2 might be infected with Adware (High probability)

30% EXTERNAL THREAT
30% — Lookalike URL — 13:42, 6/8/2020
Lookalike URL impersonating your website (Low probability)

10% MOBILE THREAT
10% — Mobile Device — 6:57, 6/8/2020
Mobile Device might be infected with Trojan Horse (Low probability)

Check Point SOFTWARE TECHNOLOGIES

 12

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

RESPONSE
MINIMIZE ATTACK IMPACT WITH A SINGLE-CLICK REMEDIATION

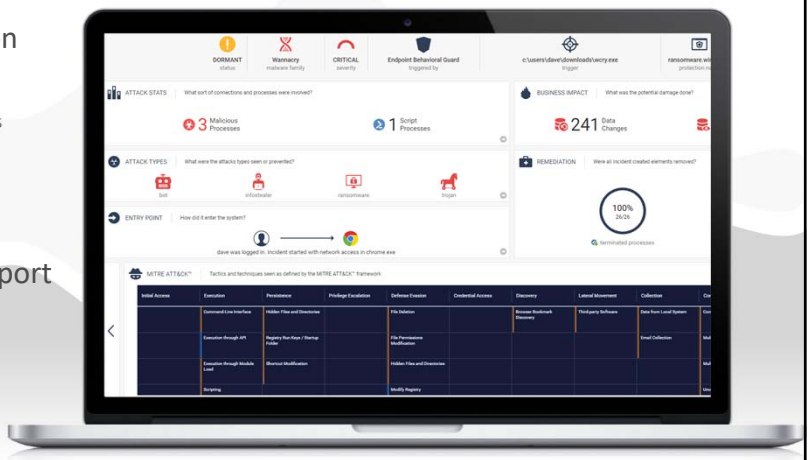
1 Install lightweight client on infected host

Identify and kill all malicious processes

Block C&C communications

Delete all installed malicious files

2 Get a detailed Forensic report with actionable insights

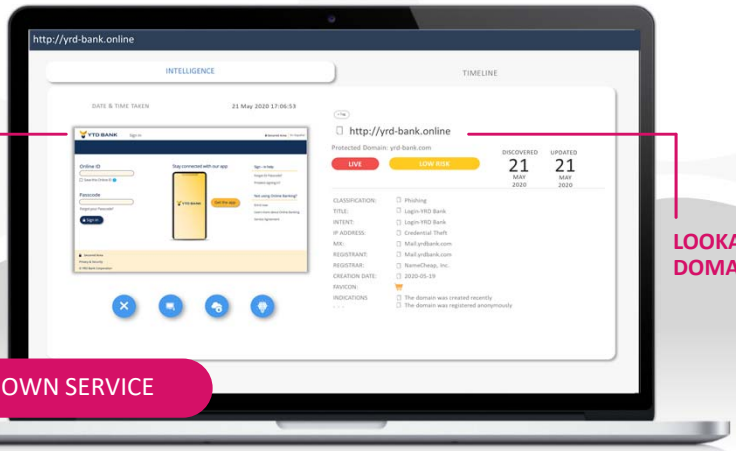


Check Point SOFTWARE TECHNOLOGIES

 13

EXTERNAL THREAT
PREVENT PHISHING CAMPAIGNS AGAINST YOUR CUSTOMERS AND EMPLOYEES

DETECTS 3X MORE THREATS THAN THE COMPETITION
WITH VISIBILITY INTO
REAL-TIME INTERNET TRAFFIC



IMPERSONATION
TO YOUR CORPORATE
WEBSITE/EMAIL DOMAIN

LOOKALIKE DOMAIN

TAKEDOWN SERVICE

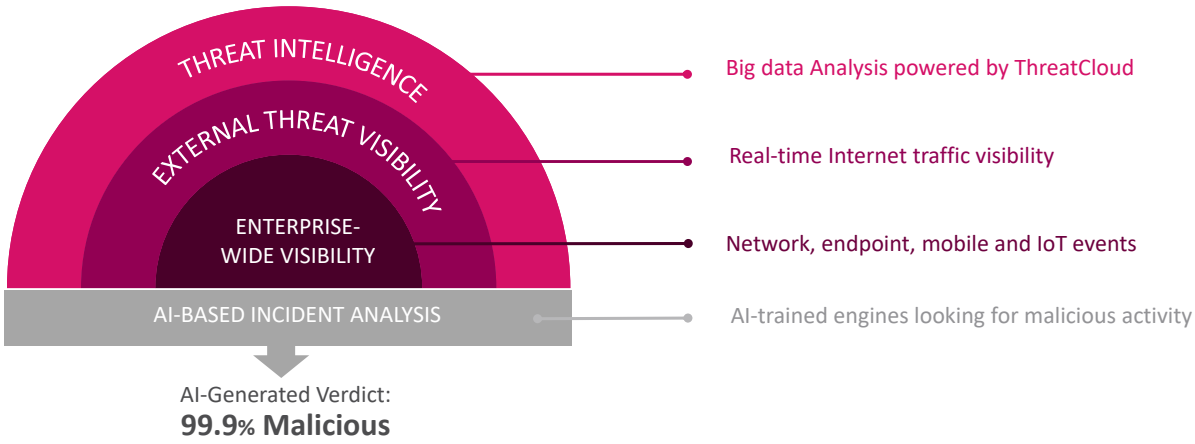
Check Point SOFTWARE TECHNOLOGIES

 14

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

TRUE XDR:
EXPOSE THE STEALTHIEST ATTACKS WITH 99.9% PRECISIONS



Check Point SOFTWARE TECHNOLOGIES

 15

CHECK POINT
INFINITY SOC
ACHIEVING SOC CERTAINTY

99.9 % PRECISION

Expose and shutdown only real attacks, inside and outside the organization.

RAPID INVESTIGATION

With the industry's most powerful threat intelligence.

ZERO FRICTION

No deployment, integration and privacy pains.

Check Point SOFTWARE TECHNOLOGIES

 16

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

cp<r>
CHECK POINT RESEARCH

DEVELOPED BY THE CHECK POINT RESEARCH TEAM

USED DAILY TO EXPOSE AND INVESTIGATE THE WORLD'S MOST DANGEROUS AND SOPHISTICATED CYBER-ATTACKS

Check Point SOFTWARE TECHNOLOGIES

 17

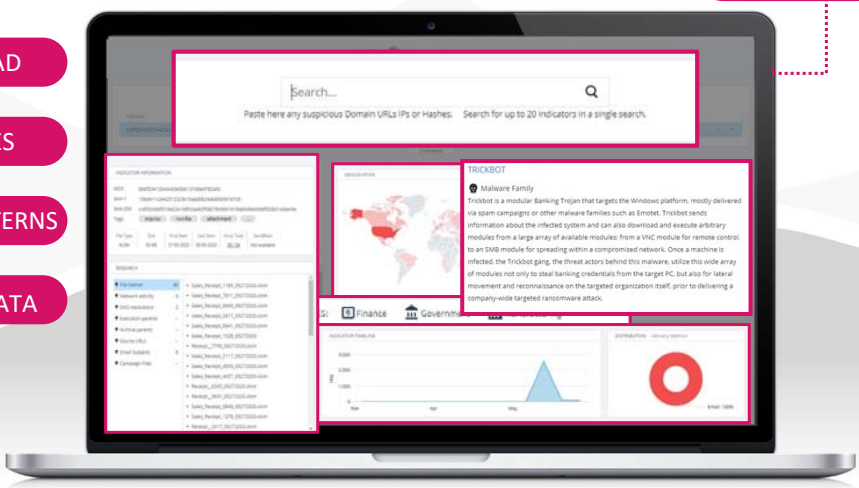
'GOOGLE SEARCH' ANY IOC FROM A CENTRALIZED PORTAL

GET EXCLUSIVE AND HIGHLY PROCESSED INTELLIGENCE

THREATCLOUD

- GEOGRAPHICAL SPREAD
- TARGETED INDUSTRIES
- ATTACK TIMELINE & PATTERNS
- EXCLUSIVE RESEARCH DATA

AND MORE...



Check Point SOFTWARE TECHNOLOGIES

 18

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

OBTAIN EXCLUSIVE INTELLIGENCE
TO DEEPEN INVESTIGATIONS

INDICATOR

COMM

NETW

CA

THE INDUSTRY'S FIRST
SOCIAL MEDI

CRK
@ch3tanK
Dissecting the 10k Lines of the new TrickBot Dropper – Yoroi Blog

Dissecting the 10k Lines of the new TrickBot Dropper

Introduction

AND MANY MORE…

Check Point
SOFTWARE TECHNOLOGIES

 19

QUICKLY DETERMINE WHETHER A SUSPICIOUS FILE IS MALICIOUS
WITH SANDBLAST'S THREAT EMULATION SERVICE

- Malware family
- Geos targeted
- MITRE ATT&CK techniques
- Emulation videos
- Dropped files
- C2 URLs
- And More!

CHECK POINT NSS RECOMMENDED

INDUSTRY'S BEST CATCH RATE
2019 NSS LABS BPS

Threat Details Report

Urgent PO Septemer.pdf.exe

MALWARE FAMILY

Trickbot

Similarity Analysis

MITRE ATT&CK

Check Point
SOFTWARE TECHNOLOGIES

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

FUELED BY THE WORLD'S MOST POWERFUL THREAT INTELLIGENCE

Check Point
SOFTWARE TECHNOLOGIES LTD

EXTRENAL FEEDS

AI ENRICHMENT

cp<r>
CHECK POINT RESEARCH

THREATCLOUD

PREDICTIVE INTELLIGENCE

100's OF MILLIONS OF:

DEVICES | CLOUDS | GATEWAYS

The Power of ThreatCloud	2,000 Zero-Day Files Detected Daily	150,000 Connected Networks	13 Million Files Emulated Daily	3 Billion Websites & Files Handled Daily

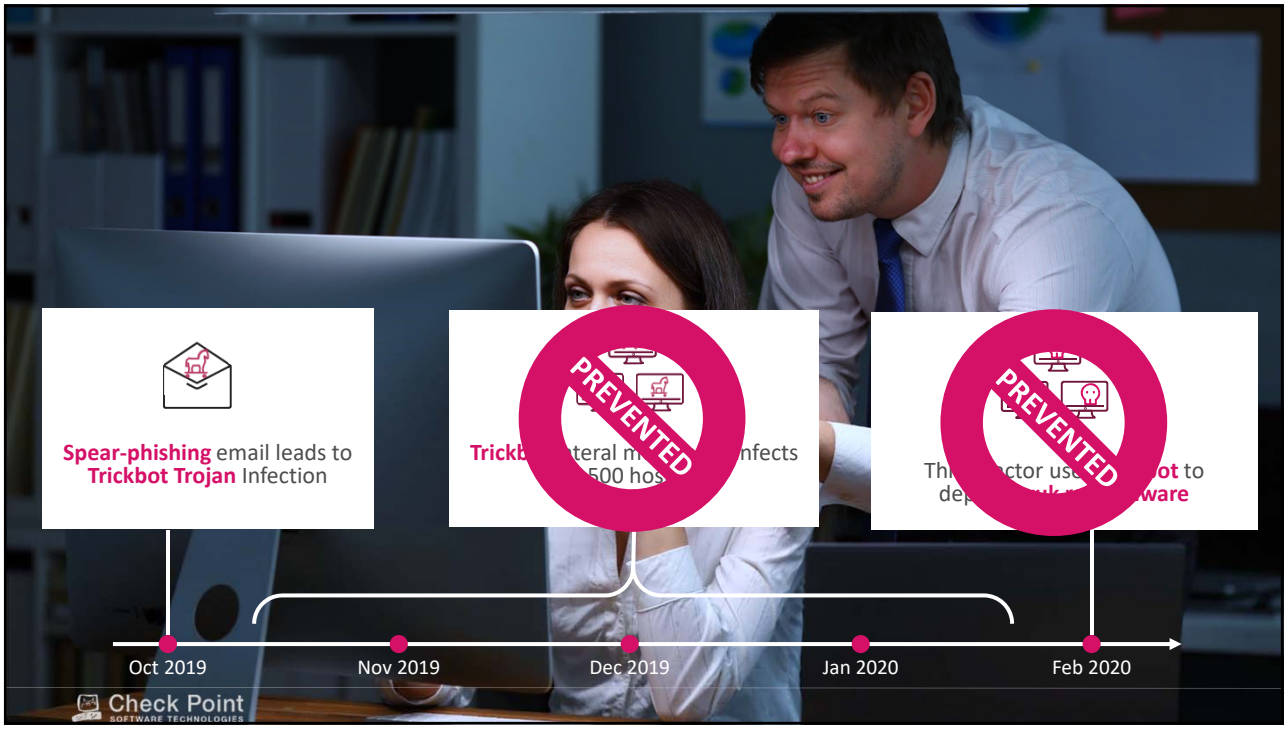
DEMO

Check Point
SOFTWARE TECHNOLOGIES

 22

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

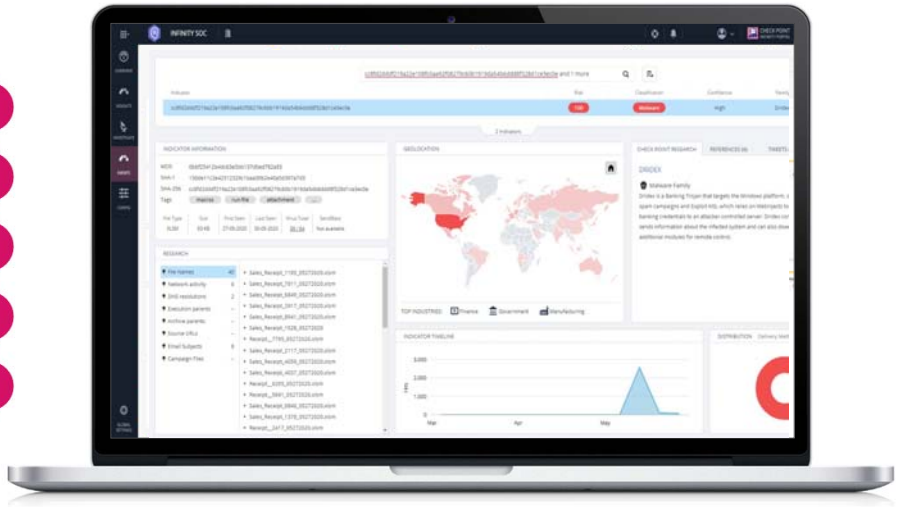


AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

REDUCE TCO AND AVOID COMPLEXITIES
WITH A SINGLE, CENTRALLY MANAGED SOC PLATFORM

- INETRNAL TREATS
- EXTERNAL THREATS
- REMEDIATION
- INVESTIGATION
- MANAGMENT



Check Point SOFTWARE TECHNOLOGIES

 25

GET STARTED IN LESS THAN 3 MINUTES
A NON-INTRUSIVE IMPLEMENTATION
NO NEED TO DEPLOY ADDITIONAL ENDPOINT AGENTS

01 Sign up to Infinity Portal

02 Select your gateways (for existing customers)

03 Connect to ThreatCloud

04 Get Started

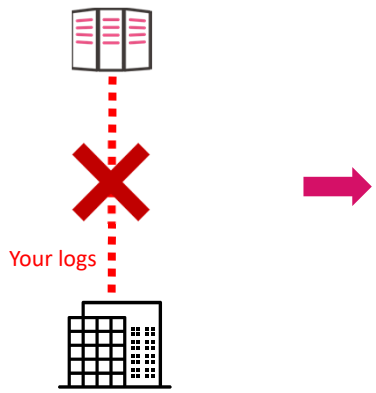
Check Point SOFTWARE TECHNOLOGIES

 26

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

AVOID PRIVACY ISSUES AND HIGH COSTS
YOUR LOGS ARE NOT EXPORTED OR STORED



Protect privacy and maintain compliance

Avoid costly log storage

Check Point SOFTWARE TECHNOLOGIES

 27

CHECK POINT
INFINITY SOC
ACHIEVING SOC CERTAINTY

99.9 % PRECISION

Expose and shutdown only real attacks, inside and outside the organization.

RAPID INVESTIGATION

With the industry's most powerful threat intelligence

ZERO FRICTION

No deployment, integration and privacy pains

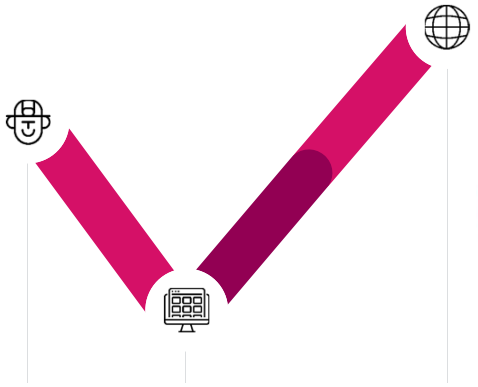
Check Point SOFTWARE TECHNOLOGIES

 28

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

READY FOR THE NEXT STEP?



CHECK POINT
INFINITY SOC

Get a **1:1 DEMO** with a Security Expert

Start a free **INFINITY SOC** trial

Learn more at: www.checkpoint.com/products/Infinity-SOC

Check Point SOFTWARE TECHNOLOGIES

Q&A

Check Point SOFTWARE TECHNOLOGIES

AVANTEC
Competence. Security. Trust.

Check Point Infinity SOC Webinar
14. & 19. Januar 2021

INFINITY SOC

ACHIEVING SOC CERTAINTY

THANK YOU

Check Point
SOFTWARE TECHNOLOGIES

 31

AVANTEC
Competence. Security. Trust.