



Check Point
SOFTWARE TECHNOLOGIES LTD



CHECK POINT
INFINITY

PROTECTING THE WHERE WITH CHECK POINT INFINITY

But, where is your where?

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY



CHECK POINT
INFINITY

Tom Kendrick | EMEA Customer Success Manager

CLOUD • MOBILE • THREAT PREVENTION

Why do we do this job? To protect our data, users and customers

- 05/2019 – **WhatsApp** buffer overflow in their own implementation of Secure Real Time Transport Protocol which was missing a packet length maximum size validation. As the RTCP function was called before the call was answered, it was possible to exploit the vulnerability, before the call was answered. See <https://research.checkpoint.com/>
- 02/2019 - **Metro Bank** is the first to disclose it has been subject to an SS7 attack. Attackers have exploited a telecom protocol vulnerability to intercept mobile text messages thus circumventing the protection of two-factor authentication (2FA). Though exploitation of SS7 vulnerability requires special capabilities, this is not an isolated case and researches report an increase in SS7 related attacks.
- 11/2018 - A new variant of the notorious TrickBot banking Trojan has been targeting the **Lloyds Bank** clients. The malicious emails impersonate the banks email address to lure users to open malicious attachments. The installed malware would then try to steal banking credentials and additional data form the infected computer.
- 10/2018 - **British Airways** has announced that last Septembers data breach had a greater impact than previously believed, as further 185,000 customers may have had their banking information stolen.
- 09/2018 - Security researchers have concluded that the data breach at British Airways was probably the work of MageCart, the hacking team behind the TicketMaster breach earlier this year, as it fits the groups modus operandi. Researchers reported that the attacker weaponized a genuine file on the companys website, adding to it a piece of code that extracts any data entered in the checkout page payment form, and sends it to a remote server located in Romania.

My inbox this week... (from a Customer)




Mon 13/05/2019 23:49

Andy

co.com>

Fw: Down payment

To: Kris

 This message was sent with High importance.

Kristi,

See below, can you have a check sent out today for the said amount?

From: Jean-Jacc a)

Sent: Monday, May 13, 2019 4:38 PM

To: Anc ia)

Subject: Down payment

I just spoke to Mark and he confirmed that all reviews concerning the acquisition is complete and at this moment the 30%(\$377,400) agreed initial payment is due. How soon can we have payment sent out?

Best regards,

Jean-Jacques

CEO,

9141

Ph: (

218

My inbox this week... (from a Customer)

RECEIVED	RECIPIENTS	SUBJECT	SENDER IP (SMTP)	SENDER IP (CLIENT)	SENDER EMAIL	SENDER NAME
Wed, 15 May 2019 20:55:54 GMT	KPieI	Re: Down payment	40.107.76.139	0.0.0.0	al @mar ...	Anc (Ma
Tue, 14 May 2019 17:53:48 GMT	KPieI	Re: Down payment	40.107.73.113	0.0.0.0	al @mar ...	Anc (Ma
Tue, 14 May 2019 00:08:12 GMT	KPieI	Re: Down payment	40.107.69.134	0.0.0.0	al @mar ...	Anc (Ma
Mon, 13 May 2019 23:49:10 GMT	KPieI	Re: Down payment	40.107.68.127	0.0.0.0	al @mar ...	Anc (Ma
Mon, 13 May 2019 23:28:33 GMT	ATRII	Fw:	40.107.72.97	0.0.0.0	al @mar ...	Anc (Ma
Mon, 13 May 2019 23:27:19 GMT	ATRII	Fw: Down payment	40.107.82.101	0.0.0.0	al @mar ...	Anc (Ma
Mon, 13 May 2019 23:25:58 GMT	ATRII	Server Test	40.107.76.138	0.0.0.0	al @mar ...	Anc (Ma

Create blacklist ruleCancel

My inbox this week... (from a Customer)

Hello,

We was target of CEO fraud attack from one domain very similar to ours.

Our domain: m[REDACTED]uctsco.com

Domain of attacker: m[REDACTED]uctco.com

I have checked and domain was registered two days ago and it has correct DNS record :

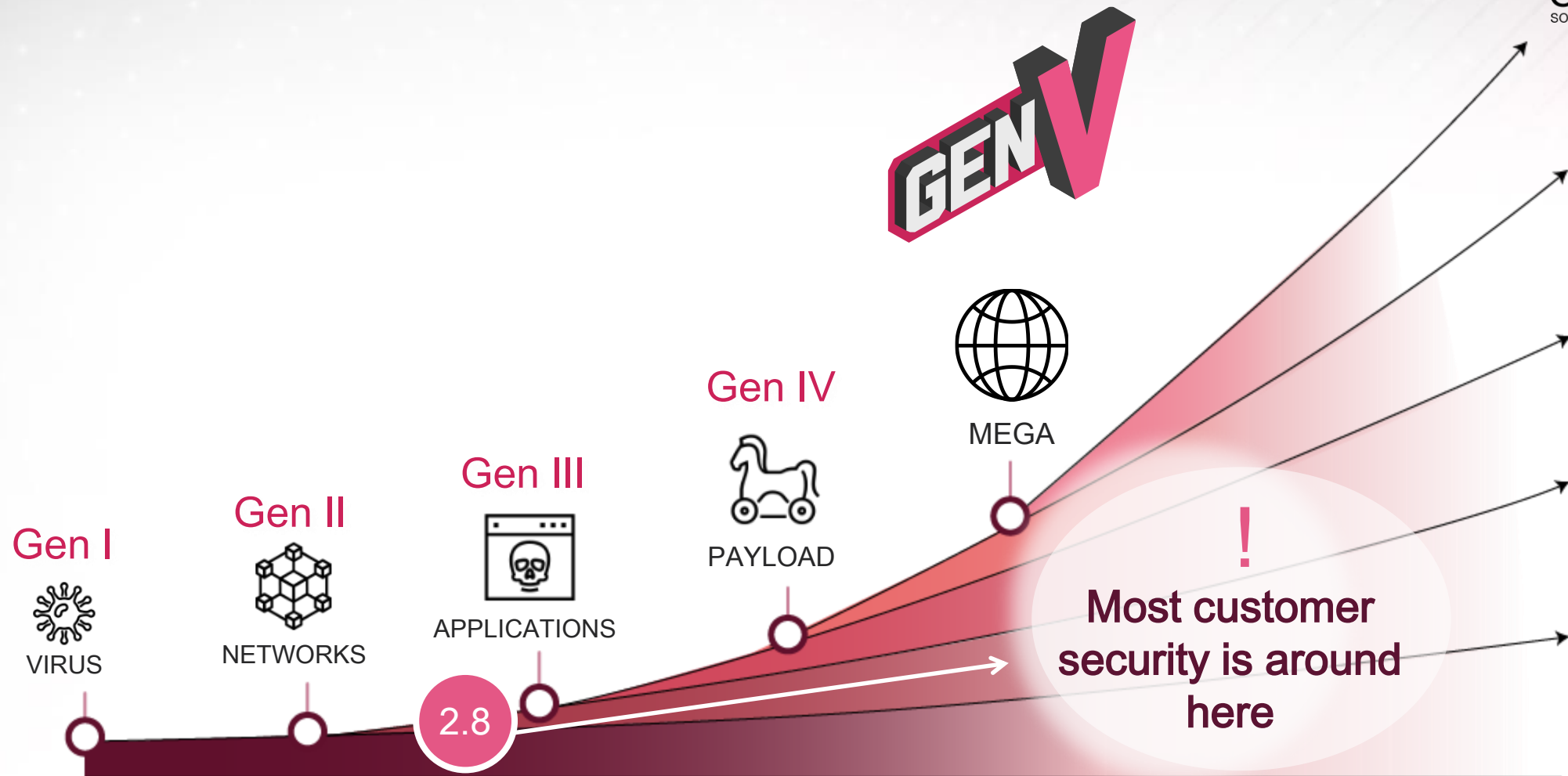
Name	Value
Registrar	GoDaddy.com, LLC
Name Server	NS33.DOMAINCONTROL.COM
Name Server	NS34.DOMAINCONTROL.COM

Name	Value
Domain Name	MA[REDACTED]CO.COM
Registry Domain ID	[REDACTED]_COM-VRSN
Registrar WHOIS Server	whois.godaddy.com

Where do we see customer's protections



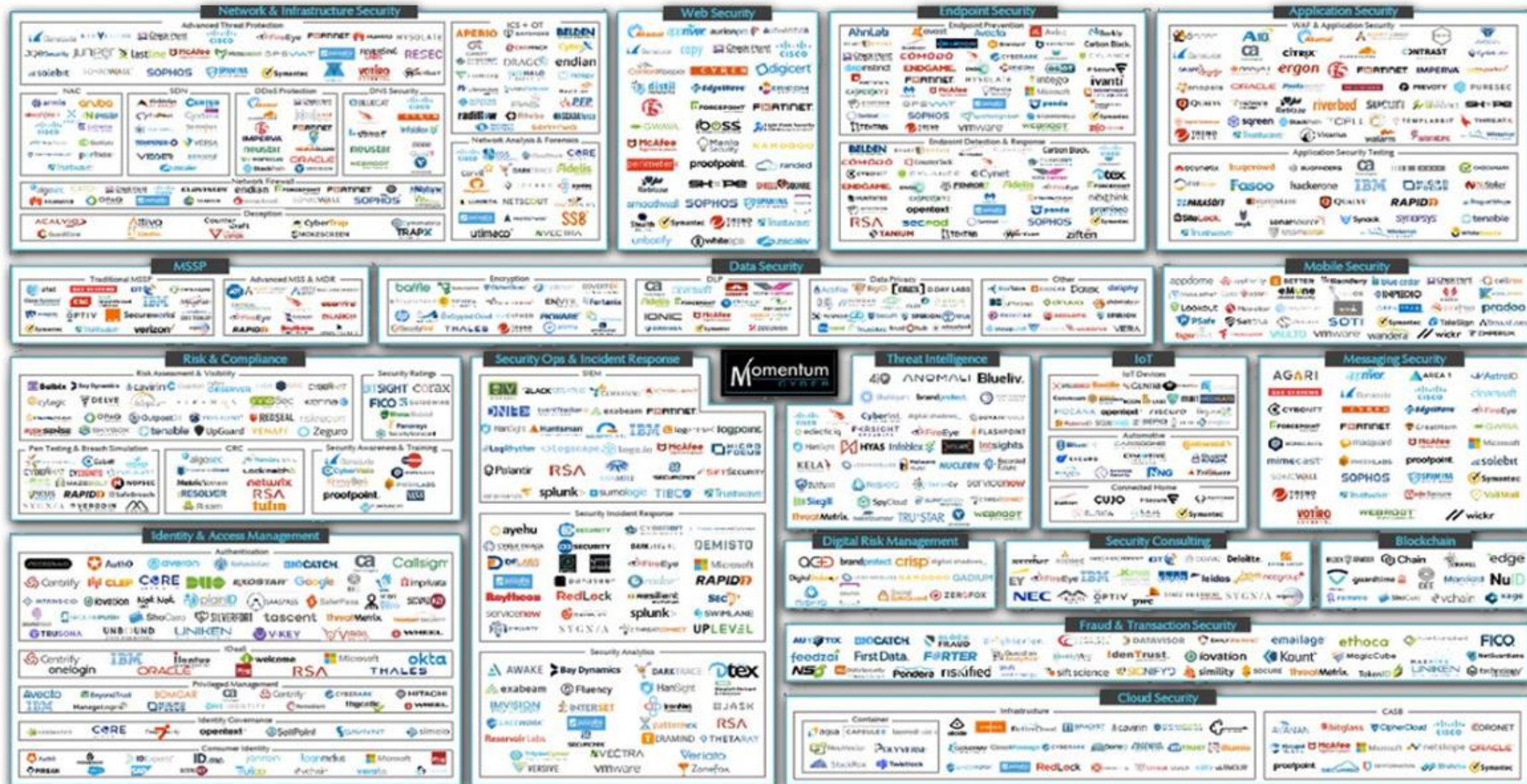
Check Point
SOFTWARE TECHNOLOGIES LTD



TOO MUCH COMPLEXITY



Check Point
SOFTWARE TECHNOLOGIES LTD



WELCOME TO THE FUTURE OF CYBER SECURITY

TOO MUCH COMPLEXITY

Too many different solutions

	2007	2018
Threat Actors	<50	>1,000
Threat Types	<50	>1,000,000
Alerts / Day (Average Per Firm)	<1,000	>1,000,000
Security Vendors	<100	>2,600
Security Spending	<\$3B	>\$90B

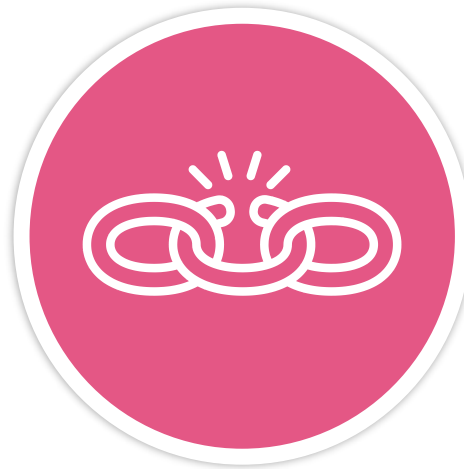
TOO MUCH COMPLEXITY



Check Point®
SOFTWARE TECHNOLOGIES LTD



Too many different
solutions



Solutions do not cooperate –
no shared intelligence or
architecture



No common management
makes common policy
impossible

COMPLEXITY - PREVENTING INFECTED FILES



Check Point
SOFTWARE TECHNOLOGIES LTD

9 ATTACK VECTORS

9 SECURITY TECHNOLOGIES

	Mobile Devices	Web Downloads	Corporate Email	Shared Folder	End Point Device	FTP	Messaging Apps.	SaaS Apps	Private Email
Anti Virus	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Sandbox	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
File Extraction	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Static Analysis	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
DLP	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
SSL Inspection	⚠	⚠	⚠	⚠	⚠		⚠	⚠	
Anti Ransomware	⚠				⚠				
Machine learning	⚠	⚠	⚠	⚠	⚠	⚠	⚠		

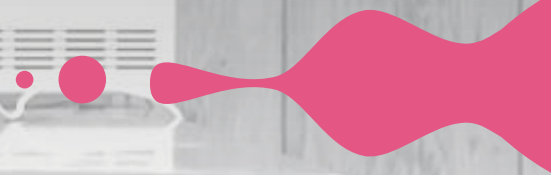
This is a
9 x 9
problem
Complexity
81
Technologies

WELCOME TO THE FUTURE OF CYBER SECURITY

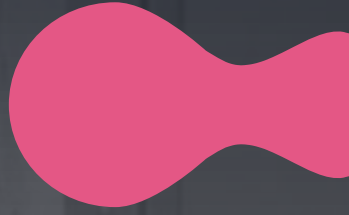
THE TRADITIONAL STRATEGY to SECURITY

Dual Vendor

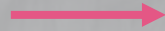
Best of Breed



THE TRADITIONAL APPROACH to SECURITY

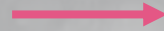


Virus



Anti-Virus

Malicious Websites



URL Filtering

Intrusion



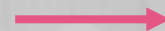
Intrusion Prevention

Botnet



Anti Bot

High Risk Applications



Application Control

Cloud



Cloud security

...and ends up with puzzle of security technologies



COMPLEXITY – BROADER VIEW



Check Point
SOFTWARE TECHNOLOGIES LTD

16 ATTACK VECTORS

26 SECURITY TECHNOLOGIES

	Business Email	Perimeter	End Point	Mobile	Web Browsing	Data Center	Cloud IaaS	Cloud SaaS	Messaging Apps	Branch Office	Web Server	IoT	USB Storage	Database	FTP/ File Share	Private Email	Vector 1	Vector 2	Vector 3
Firewall																			
Identity Access Management																			
Remote Access																			
DDOS																			
Site to Site IPSec																			
URLF																			
App Control																			
IPS																			
OWASP																			
Anti Virus																			
Anti Bot																			
File Emulation & Anti-Exploit																			
File Extraction																			
Anti Ransomware																			
DLP																			
Doc Security																			
Phishing																			
Account Take Over																			
Man in the Middle																			
Password Leak																			
Micro Segmentation																			
SSL & TLS Inspection																			
Compliance																			
Application Scan																			
Disk & Media Encryption																			
Forensics																			
Future 1																			
Future 2																			
Future 3																			

This is a
26 X 16 problem

Complexity
= **416!**

Complexity
Doubles
in **3** years!

(Adding 3 vectors
and technologies
per year)

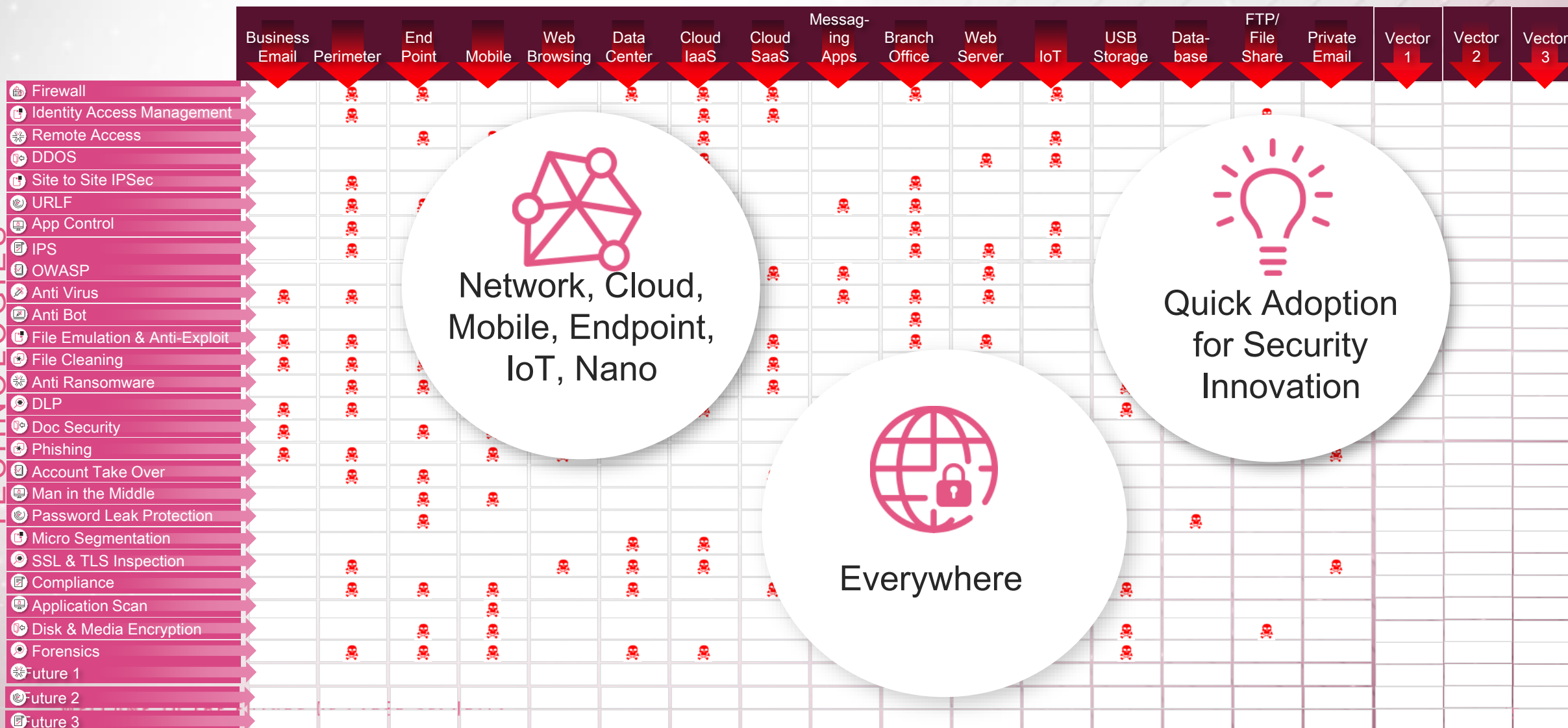
HOW DO WE PROACTIVELY ADDRESS WHAT'S COMING?



Check Point
SOFTWARE TECHNOLOGIES LTD

16 ATTACK VECTORS

26 SECURITY TECHNOLOGIES





Check Point
SOFTWARE TECHNOLOGIES LTD

ENTERPRISES ARE ONE STEP BEHIND THE ATTACKER

PATCHWORK OF POINT SOLUTIONS.

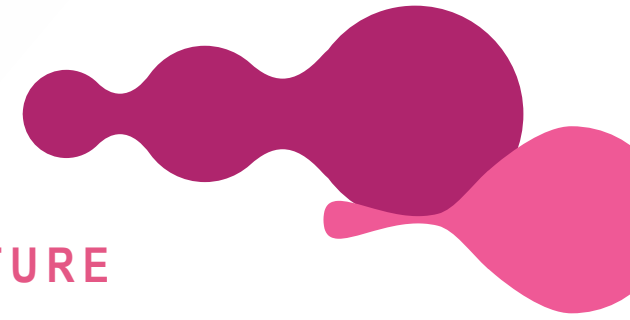
COMPLEX TO MANAGE

Looking for yesterday's signatures

Detection instead of **prevention!**



CHECK POINT
INFINITY



THE CYBER SECURITY ARCHITECTURE OF THE FUTURE



REAL TIME THREAT PREVENTION

Block the most
sophisticated attacks
before they infiltrate the
network



SHARED THREAT INTELLIGENCE

Unified threat
intelligence and open
interfaces block attacks
on all platforms



CONSOLIDATED MANAGEMENT

Single Management,
Modular Policy
Management &
integrated threat visibility

ACROSS ALL NETWORKS, ENDPOINT, CLOUDS AND MOBILE

INFINITY ARCHITECTURE

- So how can Infinity help me and my business?
 - Managing **security is complex** – and there's a **shortage of skilled staff**
 - Using Infinity, **we can secure the where of today, and the where of tomorrow**
 - As where expands, **you can expand using the same vendor** (we have a 25+ year history)
 - Infinity uses a common Threat Platform – **ThreatCloud** which is how
- What does Infinity look like in action? We will see shortly!



CHECK POINT
INFINITY

CHECK POINT THREAT CLOUD

- **Actionable Threat Intelligence** is what business needs –
 - ThreatCloud lets business owners and administrators allow their users to work with customers and third parties
 - **ThreatCloud lets users do business safely and securely**
 - Using AI and Machine learning, something learnt from one malware event, is shared, so other users, in a different business, maybe even on a different devices wont suffer from the same attack.




CHECK POINT
INFINITY

CHECK POINT THREAT CLOUD STATS

- Check Point has approx. 100 Cyber Security Researchers and about 100 more in R&D writing signatures.
- Threat Cloud:
 - Collects information from over 100,000 GW's and millions of endpoints worldwide
 - Handle requests regarding over 100 billion web pages and 1 billion files per day
 - Handles tens of millions of file emulation requests per day
 - Detects hundreds of millions of malicious events per day
 - Holds records for tens of millions of malicious files and websites
 - Updates over 1 million records per day from a wide variety of intelligence feeds coming from advanced in-house malware and threat research, AI algorithms and automated processes, partnerships and open sources.
- Total Threats Blocked per day on Gateways only: ~200M per day
- Threat Blocked per second: ~2-6k per second
- URLs processed daily: 1.5B domains per day.

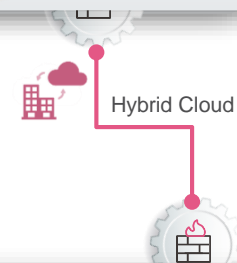
 **MOBILE**



 Shared Threat Intelligence
THREATCLOUD 



 **CLOUD**



NETWORK
Perimeter & Data centers



 **ENDPOINT**



R80
Consolidated
Security
Management

MOBILE



App Protection



Network Protection



Device Protection

Capsule
WorkSpace/Docs



Remote Access



Secure Business data



Protect docs everywhere



Shared Threat Intelligence

THREATCLOUD



CHECK POINT
INFINITY



ENDPOINT



Threat Prevention



Anti-Ransomware



Forensics

Access/Data Security



Access Control



Secure Media



Secure Documents



R30

**Consolidated
Security
Management**

CLOUD

Applications



Zero-Day Threat Protection



Sensitive Data Protection



End-to-end SaaS Security



Identity Protection



Infrastructure



Advanced Threat Prevention



Adaptive Security



Automation and Orchestration



Cross Environment Dynamic Policies



Hybrid Cloud



NETWORK

Headquarters



Access Control



Multi Layered Security



Advanced Threat Prevention



Data Protection



Branch



Access Control



Multi Layered Security



Advanced Threat Prevention



Wi-Fi, DSL, PoE Ready



DEMO TIME

- Lets see how Check Point can share intelligence from one detection, into Threat Cloud, and how everyone else will be protected



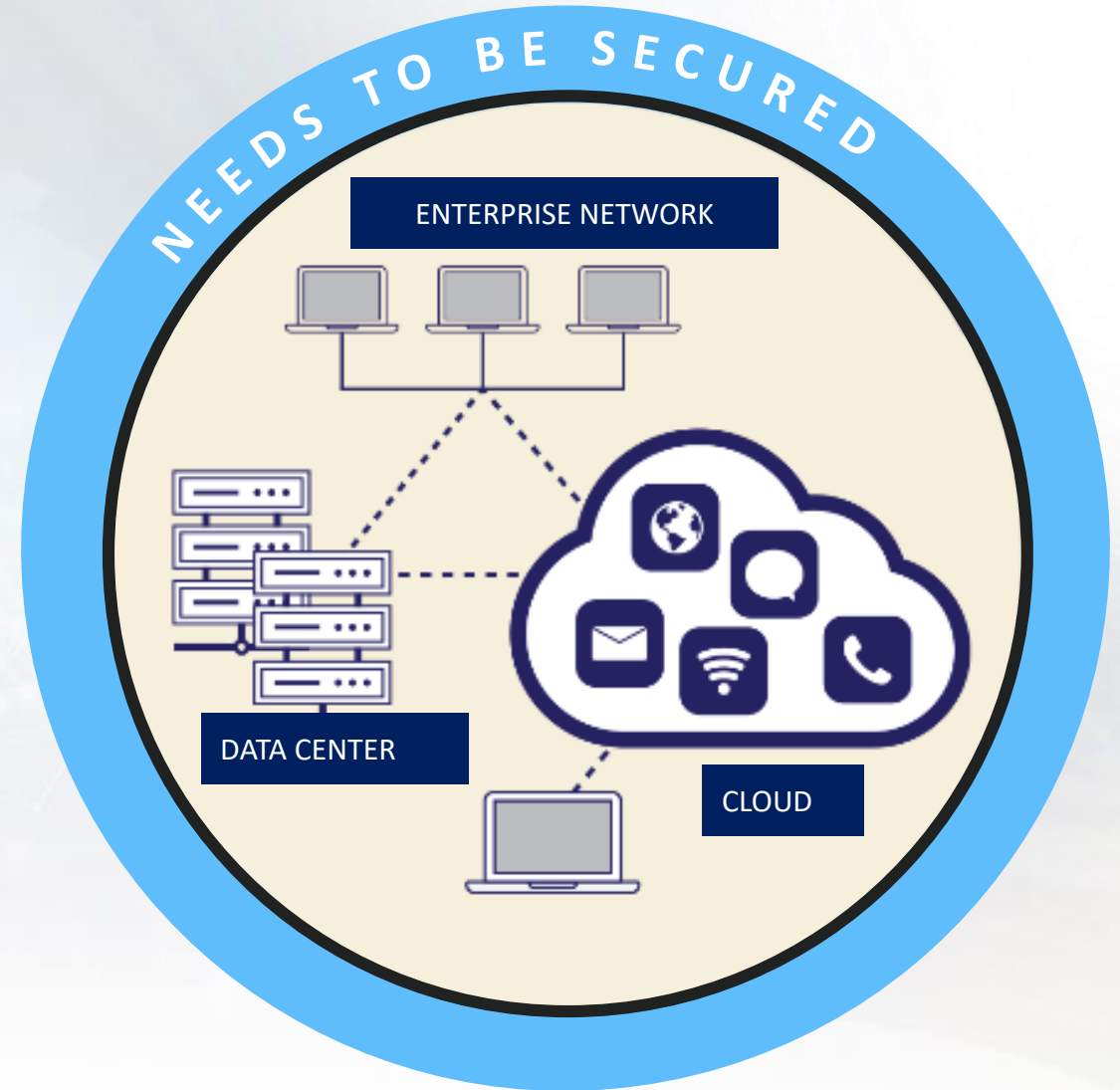
WHERE IS THE NEXT WHERE?



Drones are our CEO's latest hobby



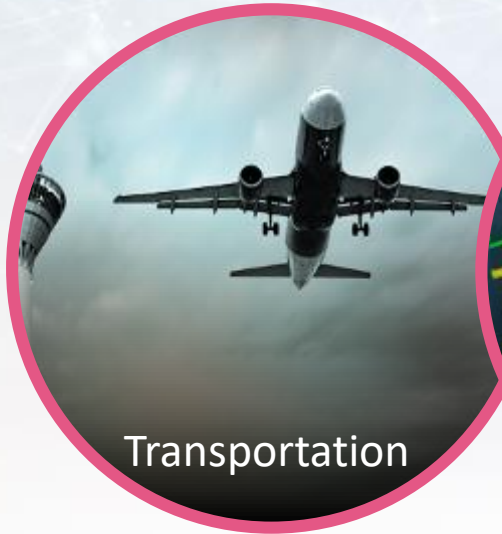
What's behind his gadget?



This is not only about drones...



...



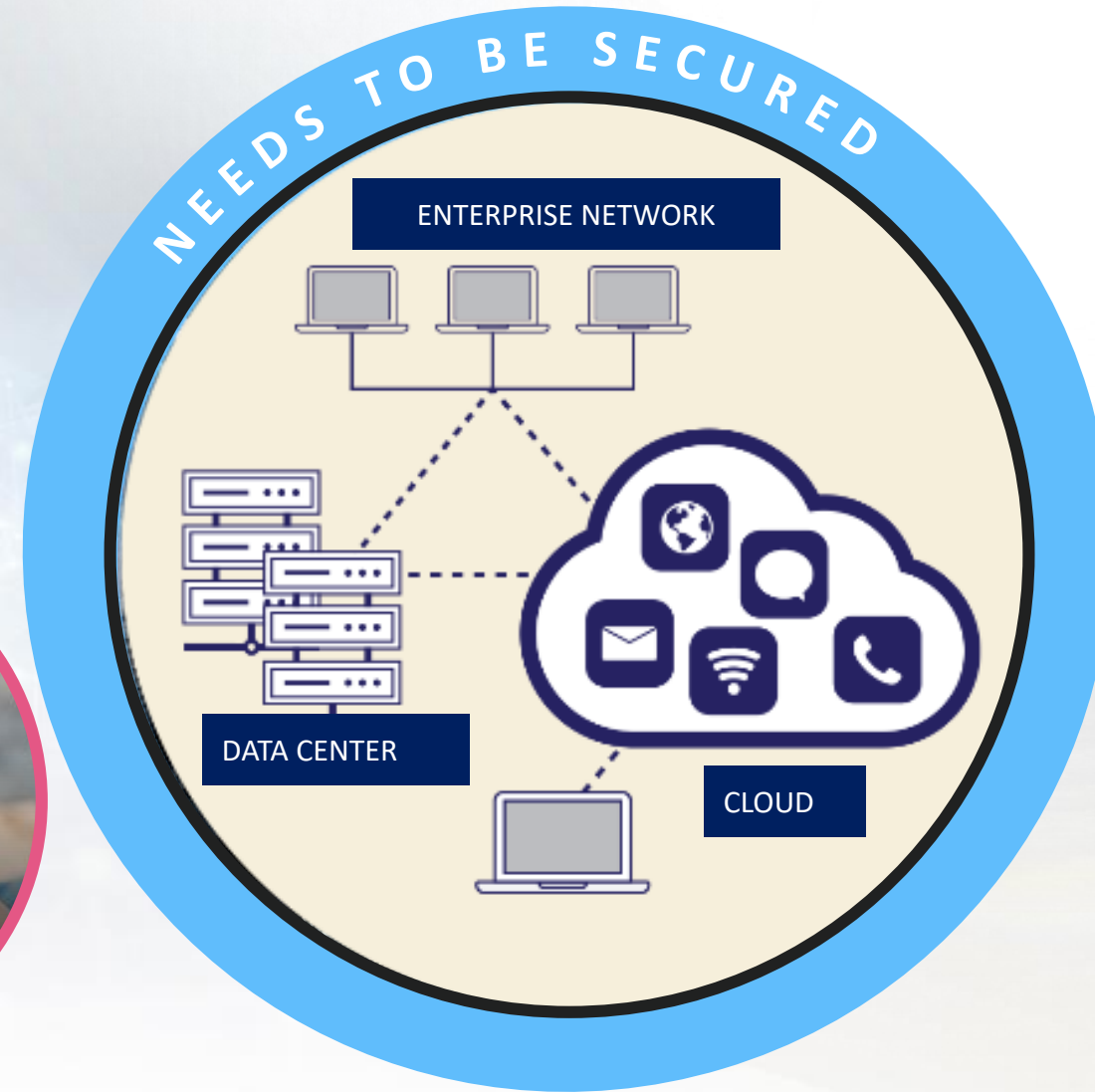
Transportation



Medical



Banking



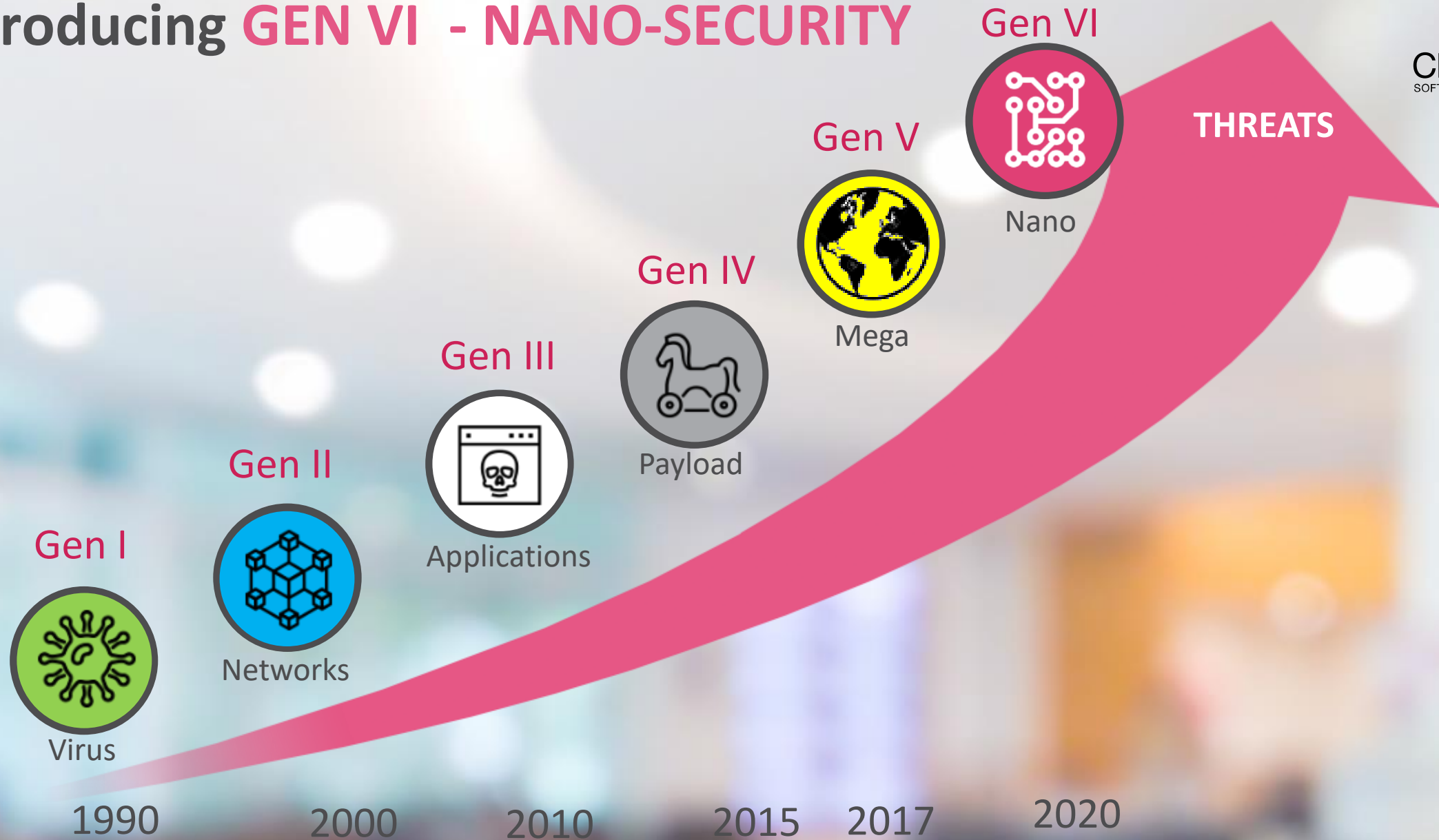
age of **THINGS**

Not just dealing with “computer networks”

Everything is interconnected,
everything is a target



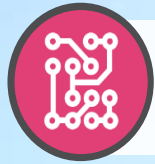
Introducing GEN VI - NANO-SECURITY



age of THINGS



Introducing GEN VI - NANO-SECURITY



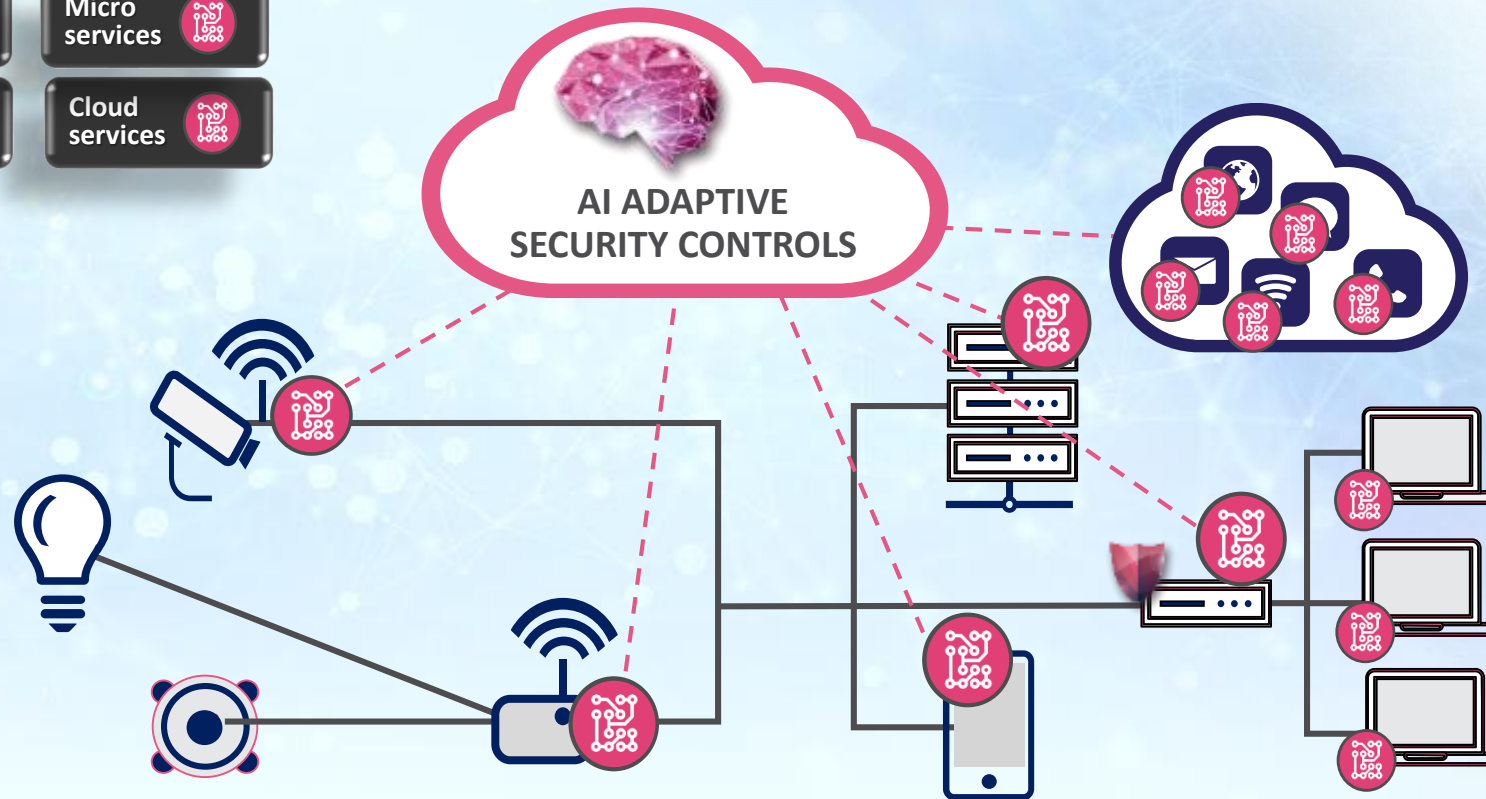
NANO AGENTS

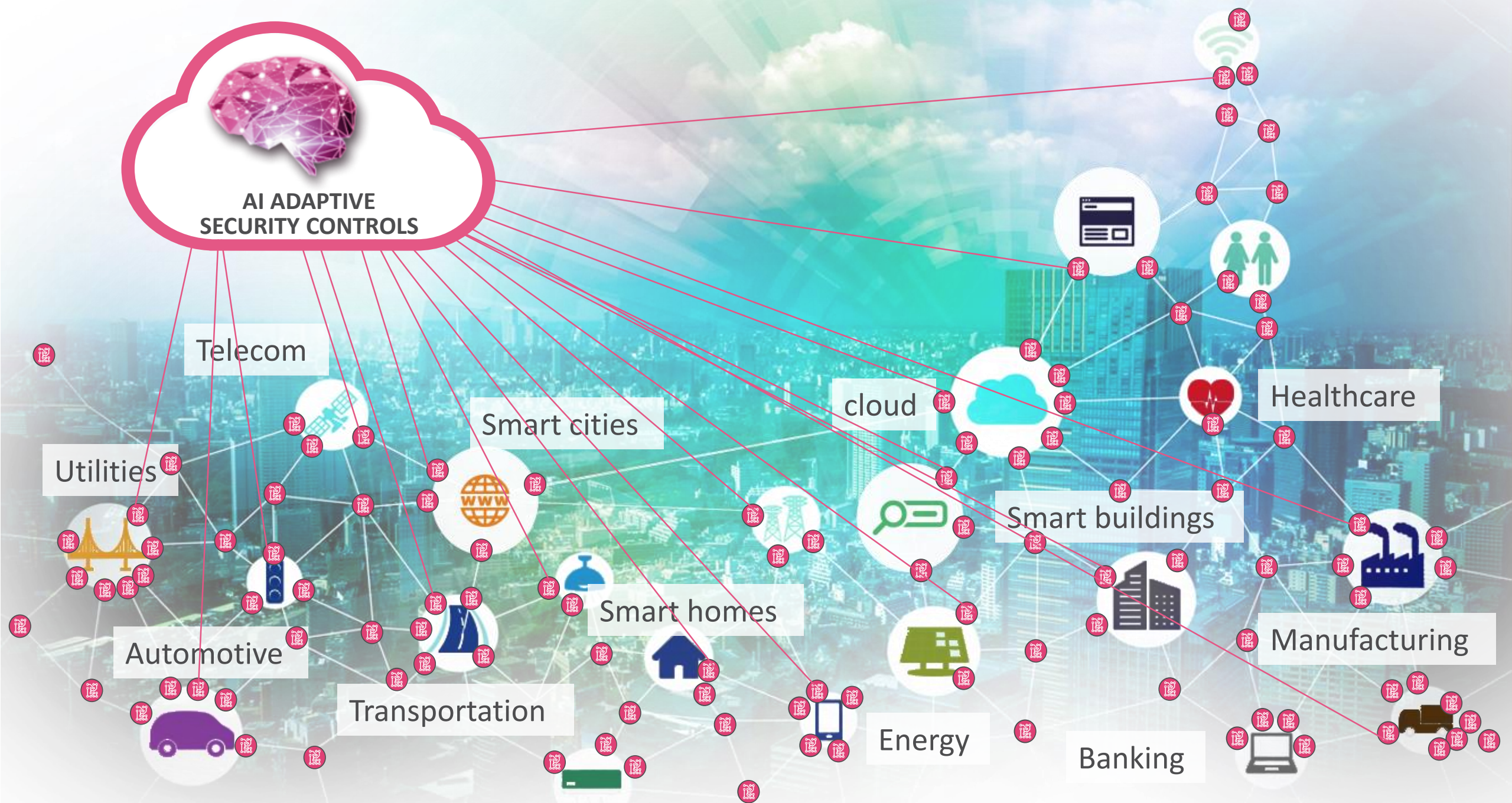
(OPEN SOURCE) SOFTWARE PLUG-IN
CONTROLLING EVERY SECURITY ATTRIBUTE



CENTRAL INTELLIGENCE AND CONTROL

PREDICTIVE SECURITY GUIDANCE BASED
ON SHARED AI





If you want to know more –
Come and talk to us!

