



YOU DESERVE THE BEST SECURITY

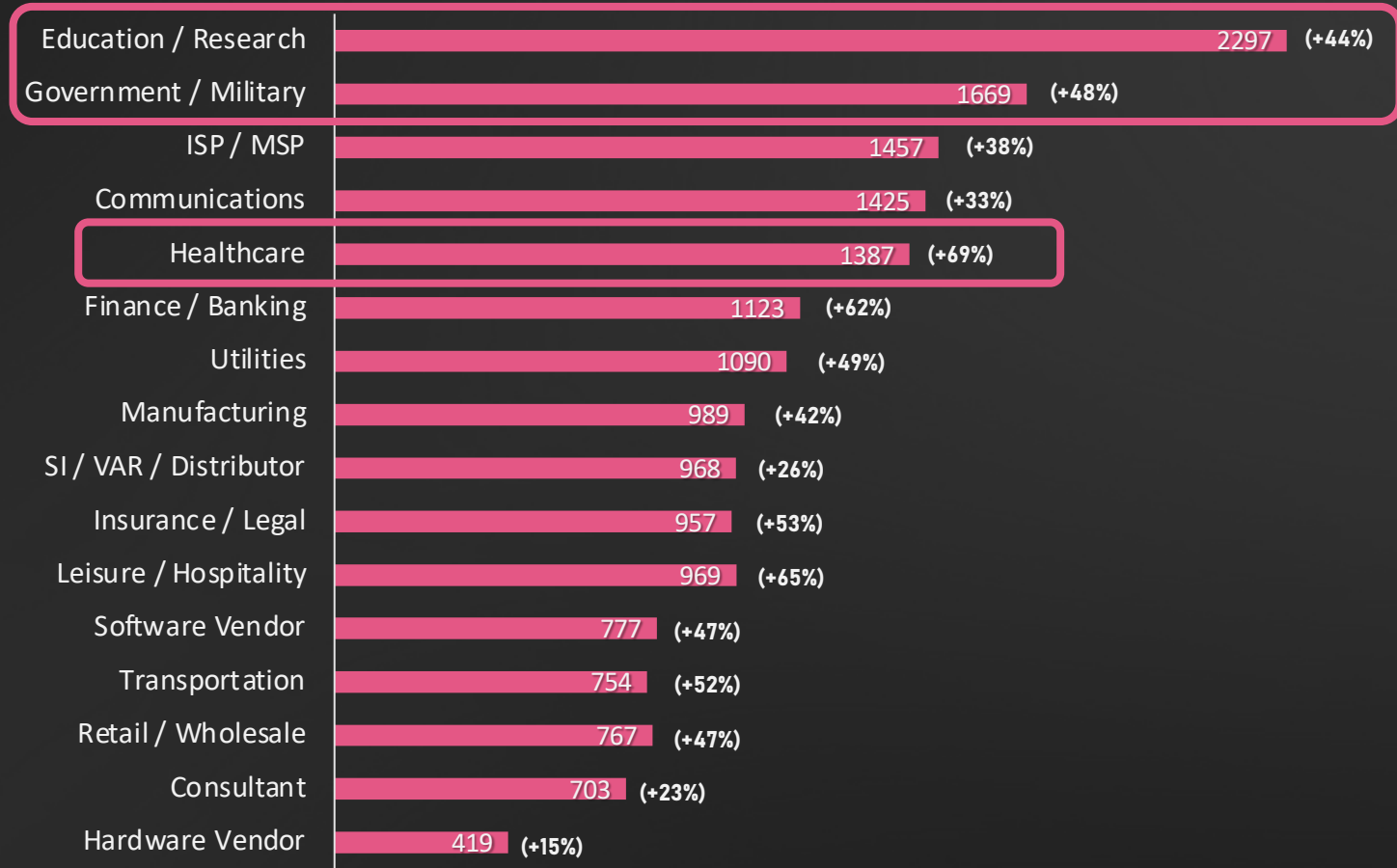
# SECURING YOUR DIGITAL ECOSYSTEM FROM RANSOMWARE

## STRATEGY NOT ACRONYMS

Deryck Mitchelson | Field Chief Information Security Officer, EMEA

October 2022

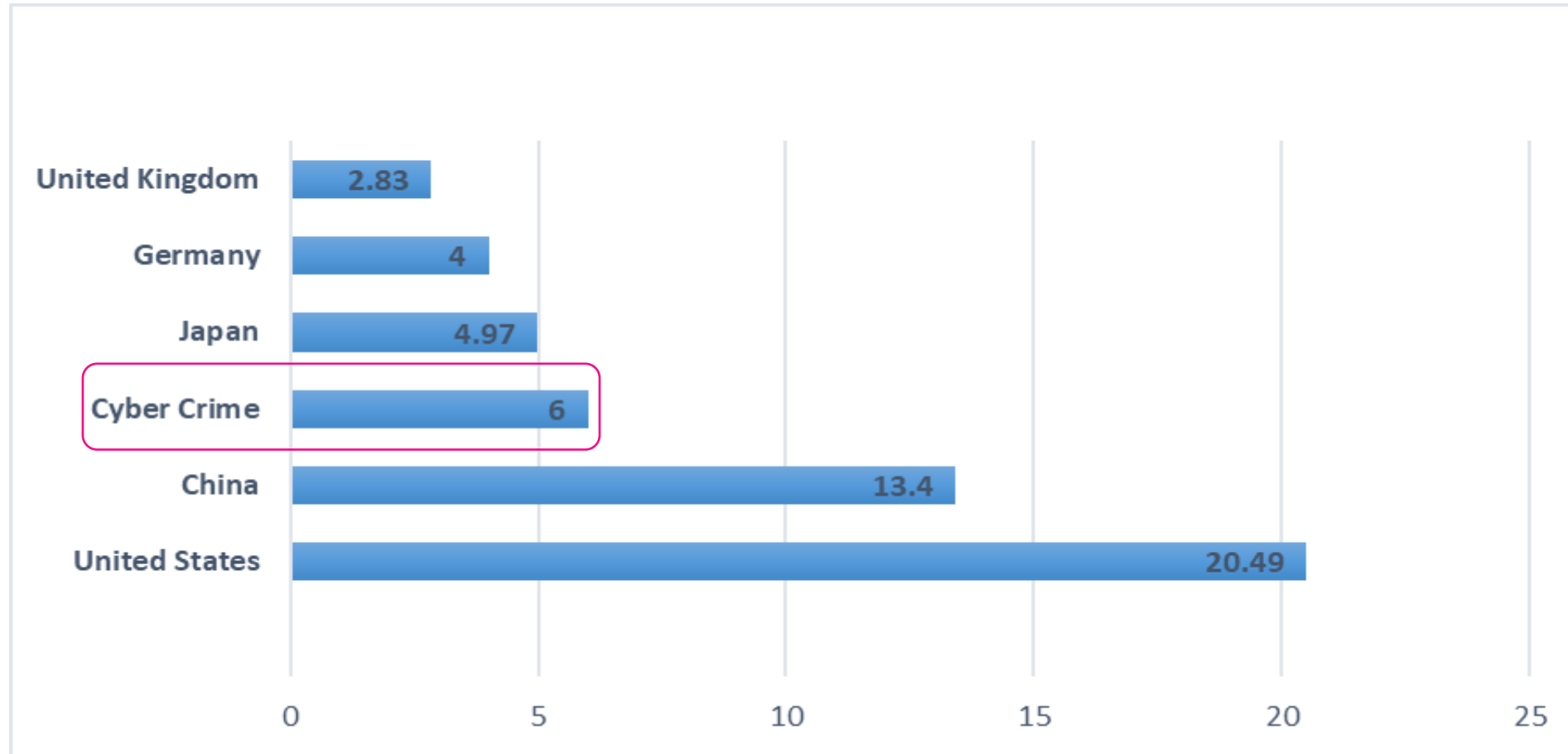
# Cyber Attacks by Industry



Average weekly attacks per organisation by industry H1 2022 compared to 2021

# Thriving Cyber Crime Economy Fueling Issues

Nominal GDP 2022 (Trillions)



# Too many acronyms – what does it all mean?



# Lessons from Pandemic

YOU DESERVE THE BEST SECURITY

# Biological Pandemic vs. Cyber Pandemic:

## Similarities and Parallelization, Lessons Learned

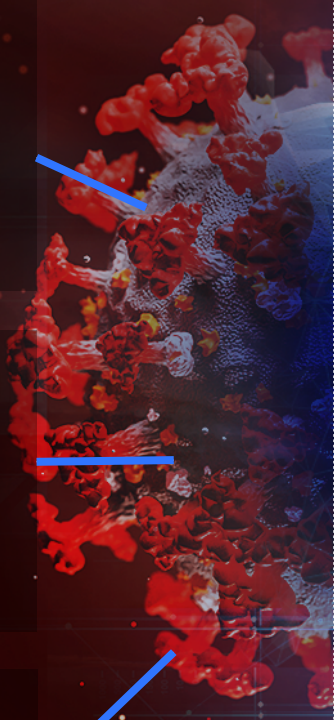
### BIOLOGICAL PANDEMIC



#### INFECTION RATE

Virus infection rate (RO) (source:WHO)  
The average number of people that one person with a virus infects

Flue: 1.3, SARS: 2-4, **Corona: 2.5**  
Ebola: 1.6-2, ZIKA: 2-6.6, Measels: 11-18



#### INFECTION PREVENTION

Best treatment: **Vaccination**  
Dealing with Infection Best Practices:

- 1) Quarantine, shelter in place
- 2) Isolation
- 3) Contact tracing



#### SAFETY BEST PRACTICES

common treatment (until vaccination):

- 1) Mask
- 2) Hygiene
- 3) Social distancing

### CYBER PANDEMIC



#### INFECTION RATE

Malware infection rate (RO) The average number of infections that one host with a malware causes

**Cyber attack** - >27 (source: WEF, NSTU),  
**Slammer**: doubled in size every 8.5 seconds,  
**Code red** - 2000 new hosts per minute



#### INFECTION PREVENTION

Best treatment: **Real Time Prevention**

Best Practices- **Continuous** process of:

- 1) **Quarantine**: sandboxing, micro segmentation
- 2) **Isolation**: Zero Trust, segregation
- 3) **Tracing**: Threat Intel., AI, SOC, Posture management



#### SAFETY BEST PRACTICES

- 1) **Awareness**: think before you click ...
- 2) **Cyber Hygiene**: Patches, Compliance...
- 3) **Asset distancing**- network Segmentation, Multi Factor authentication...

# For Academics – Calculating R0 for Cyber Attack

$$\frac{dS}{dt} = \mu N - \frac{rSI}{N} - (p_{SR} + \mu)S \dots \dots \dots (1)$$

$$\frac{dE}{dt} = \frac{rSI}{N} - (\alpha + p_{ER} + \mu)E \dots \dots \dots (2)$$

$$\frac{dI}{dt} = \alpha E - (\gamma + \mu)I \dots \dots \dots (3)$$

$$\frac{dR}{dt} = p_{SR}S + p_{ER}E + \gamma I \dots \dots \dots (4)$$

For steady states

$$\frac{dS}{dt} + \frac{dE}{dt} + \frac{dI}{dt} + \frac{dR}{dt} = 0 \dots \dots \dots (5)$$

Let us define also epidemic threshold,

$$R_0 = \frac{\alpha \mu r}{(\alpha + p_{ER} + \mu)(\gamma + \mu)(p_{SR} + \mu)} \dots \dots (6)$$

# Breaches are inevitable?

*“... massive institutional breaches don't need to happen as often as they do. Many occur not because of complex and sophisticated hacking, but because organisations have made basic and potentially avoidable mistakes in implementing their security schemes ...”*

– Lily Newman, *Wired.com*, 2018

CRN CRN

## Colonial Pipeline Hacked Via Inactive Account Without MFA

The Darkside ransomware gang broke into Colonial Pipeline through an inactive account that didn't use multifactor authentication,...

5 Jun 2021





***Are you prepared?***

# Cyber Hygiene Should be an Immediate Priority

- Identify key services, products and assets ✓ ?
- Develop and exercise incident response plan ✓ ?
- Establish cyber awareness and education programme ✓ ?
- Secure backups and regular restoration regime ✓ ?
- Enforce least privilege and full auditing ✓ ?
- Prioritise patch and change management, vulnerability scanning ✓ ?
- Map cyber risks to business priorities and impact ✓ ?
- End-to-end network security and monitoring ✓ ?
- Multi-factor authentication enforcement ✓ ?

# High Profile Breaches. Where they fully prepared?



Hacker group published 20GB of confidential data and 71,000 employee credentials

**Feb '22**



Hacker group published 190GB of confidential data including source code for bootloader of newer devices.

**Mar '22**



Phishing email allowed hacker group to deliver ransomware payload

**April '22**



Hacker leaks 128GB of leaked files from Amazon streaming service Twitch

**October '21**



Hacker group published 9GB of source code for 250 projects stolen from Microsoft including Bing, Cortana

**March '22**

# Highest Impact Security Threats to Digital Transformation

- Ransomware
- Supply Chain
- Cloud Adoption

YOU DESERVE THE BEST SECURITY

# First Ransomware Attack

AIDS Trojan in 1989

20,000 infected floppy disks

mailed to attendees at WHO conference

Launched a questionnaire on AIDS research

Symmetric cryptography used which wasn't difficult to reverse

One organization lost 10 years of research

Dear Customer:

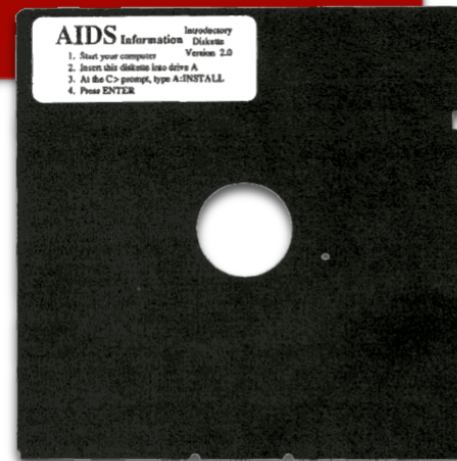
It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue



# Ransomware – Evolving Motivations

## Financial

(private to public, cooperation and supply chain)

## Data theft and Espionage

(Lazarus)

## Cyber Terror and political influence

(Pay2Key)

## Cyber weapon trading

(Ransomware as a service)

# Ransomware Prolific

Ransomware attacks increased by up to 93% in 2021

- 1200 organisations per week under attack
- Average ransom payment increased by 171%
- Double Extortion: encrypting and exfiltration of files
- More than 40% ransomware families incorporated data exfiltration to the attack process
- Increased threat landscape from SaaS, Cloud, Remote Working

Average cost of a data breach risen from USD 3.86m to USD 4.24m

Phishing attacks were related to 36% of ransomware. Is your email secure from zero-day malware and next generation phishing?

Pandemic and Geo-Conflict has led to a surge in ransomware attacks

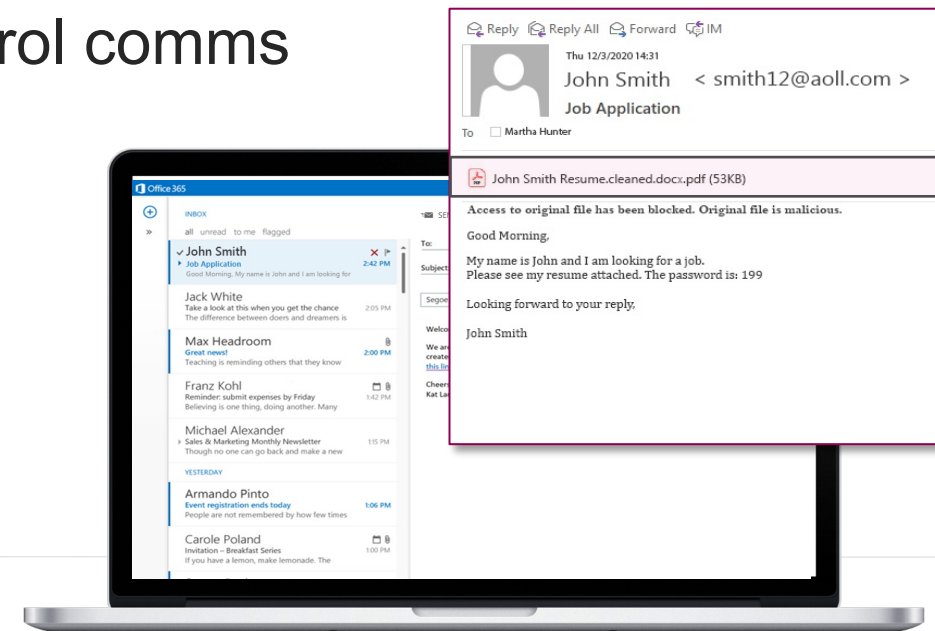
RaaS business models significantly lowering the technical barrier to entry

Rapid weaponisation of vulnerabilities such as Log4j and Zero-days

DarkSide brought in more than \$90m from ransomware in 2021

# Assume you will be compromised. Prevent the next Ransomware Attack

- **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 Command & Control comms
- Implement **Network Segmentation**
- Deploy **Multi Factor Authentication** everywhere
- **Patch vulnerabilities** and **secure remote access**
- Exercise and implement **Incident response** to call in the case of emergency





# Ransomware Prevention – CIS Control Selection

Category	CIS Safeguard #	CIS Safeguard Title
<b>Identify</b>		
Know Your Environment	1.1	Establish and Maintain Enterprise Asset Inventory
	2.1	Establish and Maintain Software Asset Inventory
	2.2	Ensure Authorised Software is Currently Supported
	3.1	Establish and Maintain a Data Management Process
	5.1	Establish and Maintain an Inventory of Accounts
<b>Protect</b>		
Secure Configurations	4.1	Establish and Maintain a Secure Configuration Process Enterprise Assets
	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
	4.4	Implement and Manage a Firewall on Servers
	4.7	Manage Default Accounts
Account and Access Mgt	5.2	Use Unique Passwords
	5.3	Disable Dormant Accounts
	5.4	Restrict Admin Privs to Dedicated Admin Accounts
	6.1	Establish Access Granting Process
	6.2	Establish Access Revoking Process
	6.3	Require MFA for Externally Exposed Applications
	6.4	Require MFA for Remote Network Access
	6.5	Require MFA for Admin Access
Vulnerability Mgt Planning	7.1	Establish and Manage a Vulnerability Mgt Process
	7.2	Establish and Manage a Remediation Process
	7.3	Perform Automated OS Patch Management
	7.4	Perform Automated Application Patch Mgt
	12.1	Ensure Network Infrastructure is Up-to-Date
Malware Defense	10.1	Deploy and Maintain Anti-Malware Software
	10.2	Configure Automatic Anti-Malware Signature Updates
	10.3	Disable Autorun and Autoplay for Removable Media
Security Awareness & Skills Training	14.1	Establish and Maintain a Security Awareness Program
	14.2	Train Workforce Members to Recognise Social Engineering Attacks
	14.6	Train Workforce Members on Recognising and Reporting Security Incidents

# Ransomware Prevention – CIS Control Selection

Detect		
Network Monitoring and Defense	13.1	Centralise Security Event Alerting
	13.2	Deploy a Host-Based Intrusion Detection Solution
	13.3	Deploy a Network Intrusion Solution
	13.7	Deploy a Host-Based Intrusion Prevention Solution
	13.8	Deploy a Network Intrusion Prevention Solution
Respond		
Data Recovery & Incident Response	17.1	Designate Personnel to Manage Incident Handling
	17.2	Establish and Maintain Contact Information for Reporting Security incidents
	17.3	Establish and Maintain an Enterprise Process for Reporting Incident
	8.1	Establish and Maintain an Audit Log Management Process
	8.2	Collect Audit Logs
	8.3	Ensure Adequate Log Storage
Recovery		
Data Recovery & Incident Response	11.1	Establish and Maintain a Data Recovery Process
	11.2	Perform Automated (Immutable) Backups
	11.3	Protect Recovery Data
	11.4	Establish and Maintain an Isolated Instance of Recovery Data

# Endpoint Protection That PREVENTS Ransomware

## Single Agent, Unified Management

### Access Control

- Host Firewall
- Compliance
- Web-browsing protection

### Threat Intelligence

### Sandboxing

- Threat Emulation
- Threat Extraction

### Web Protection

- Zero-day Phishing site protection
- Corporate Password Reuse Protection
- URL Filtering
- Malicious site protection

### Virtual Private Network

- Remote access

### Prevention

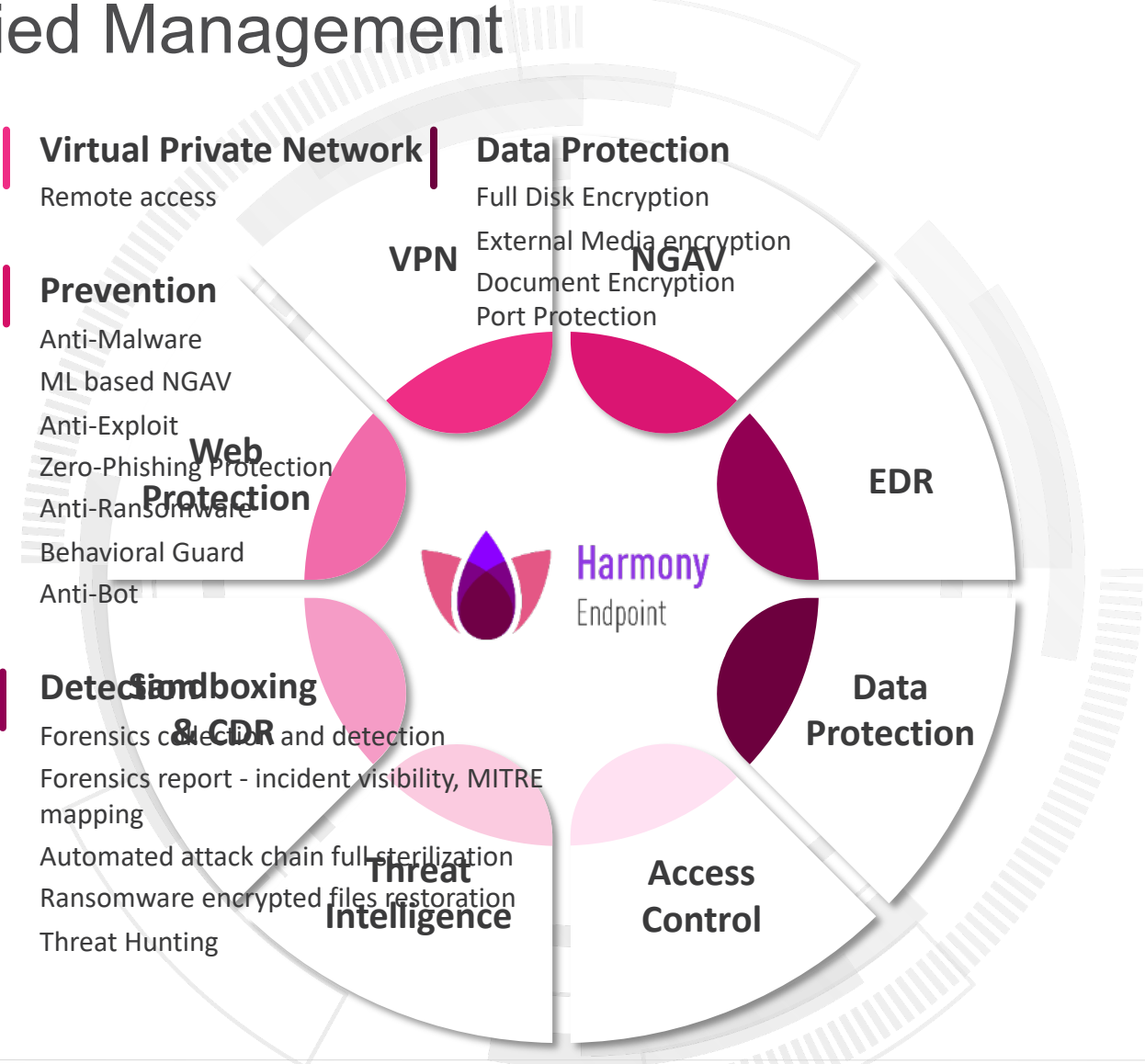
- Anti-Malware
- ML based NGAV
- Anti-Exploit
- Zero-Phishing Protection
- Anti-Ransomware
- Behavioral Guard
- Anti-Bot

### Detection & CDR

- Forensics collection and detection
- Forensics report - incident visibility, MITRE mapping
- Automated attack chain full sterilization
- Ransomware encrypted files restoration
- Threat Hunting

### Data Protection

- Full Disk Encryption
- External Media encryption
- Document Encryption
- Port Protection





Harmony  
Endpoint

Anti-Ransomware



# Supply Chain Threat – Seismic Rise

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


Enterprise supply chains are becoming more complex with supply chain attacks becoming more targeted. Shift to cloud native development and DevOps processes has made securing

82% of CIOs believe their software supply chains are vulnerable

85% of CIOs have been specifically instructed by board to take action to improve security of software development and build environments

Venafi CIO pipeline Survey 2022

# Supply Chain Threat - Manage your Vulnerabilities


 Bleeping Computer

## Fortinet says critical auth bypass bug is exploited in attacks

"Fortinet is aware of an instance where this vulnerability was ... Per a Shodan search, more than 140,000 FortiGate firewalls can be reached...

1 week ago




 CPO Magazine

## New Microsoft Exchange Zero-Day Vulnerabilities Exploited by State-Sponsored Hackers

According to Shodan crawls, approximately 250,000 on-premises Microsoft Exchange servers exposed to the internet are at risk.

2 weeks ago




 SecurityWeek

## Sophos Firewall Zero-Day Exploited in Attacks on South Asian ...

"Sophos has observed this vulnerability being used to target a small ... A researcher from Japan pointed out that a Shodan search shows more...

3 weeks ago

 Tech Business News

## Cisco urges customers to patch vulnerabilities discovered in ...

...

According to Clements, Shodan, a search engine for internet-connected devices, found over 12,000 web management interfaces exposed to the...

8 Aug 2022



# Strategy for Mitigating Supply Chain Risks

- Audit your supply chain
- Prioritise patch management
- Assess security posture of all suppliers
- Follow DevSecOps best practices
- Enable Multi Factor Authentication
- Review supplier access and elevated privileges
- Implement least privilege access and network segmentation
- Identify and audit fourth parties
- Increase security awareness
- Assume you will be breached and exercise incident response

# Digital Transformation Threat (Cloud Acceleration)

## Cloud Services attacks doubled in 2021

- **COVID-19 driven** shift to home and hybrid working
- **2021** Wave of attacks leveraging flaws in the leading cloud services
- Acceleration from on premise to cloud - **Hybrid and Multi-Cloud**
- Identity and Access Management (IAM) flaws caused by **provider flaws or trust policy logic**
- Unsecured **APIs** and mis-configurations prevalent

## Example - OMIGOD Flaw (Microsoft Azure)

- **65%** of all customers vulnerable
- **Easily exploited** – Single request needed

Mis-configured clouds and account compromise are leading cause of cyber breaches

89% of enterprises have multi-cloud strategy

Public cloud breaches overtook private cloud in 2021 with 27% experienced a breach

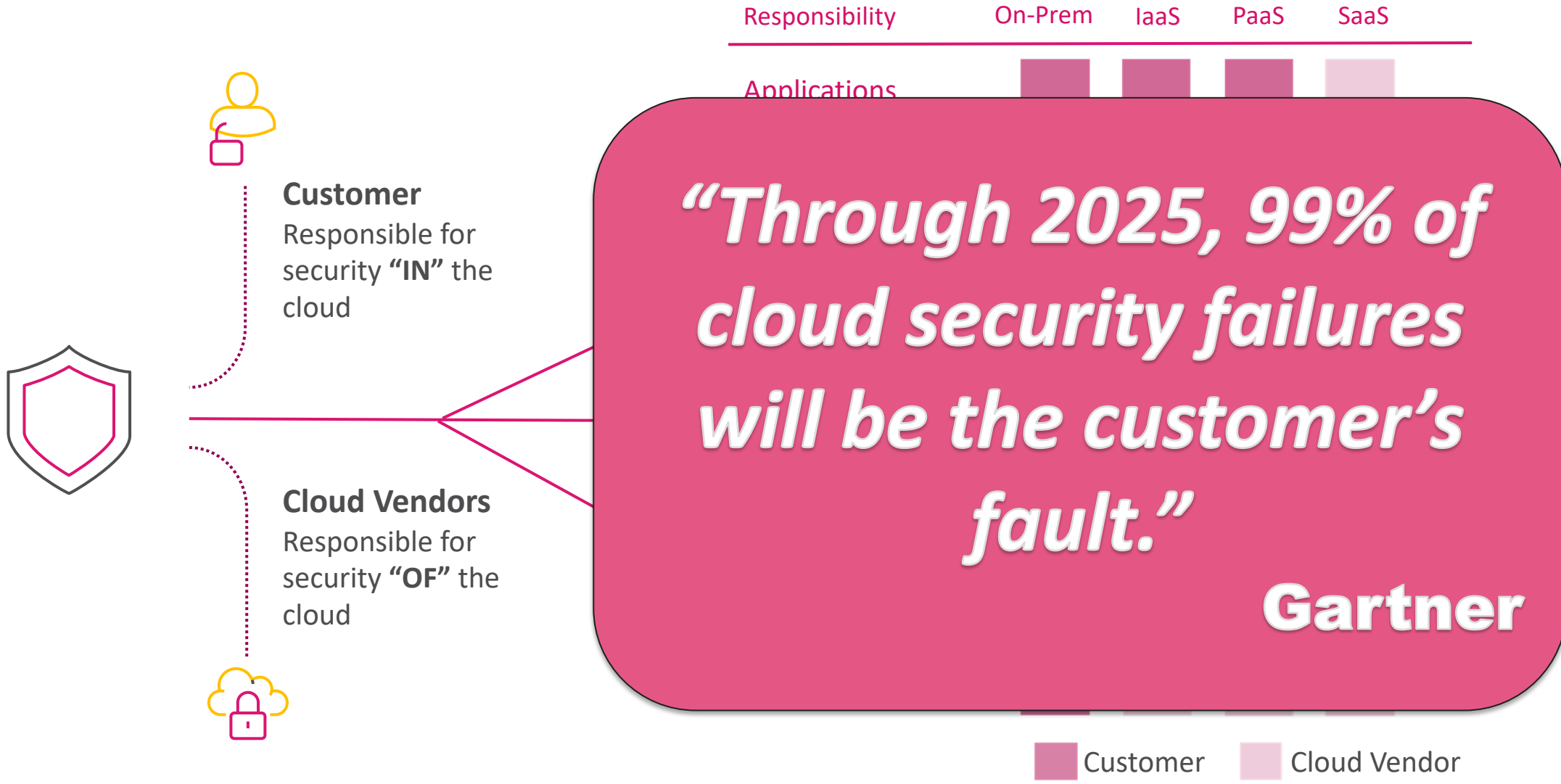


# Top Security Challenges in the Public Cloud

- 1 Increased Attack Surface
- 2 Lack of Visibility and Tracking
- 3 Misconfigurations
- 4 Managing multi-Clouds
- 5 Securing DevOps
- 6 Compliance and Regulations



# Cloud Security is a Shared Responsibility

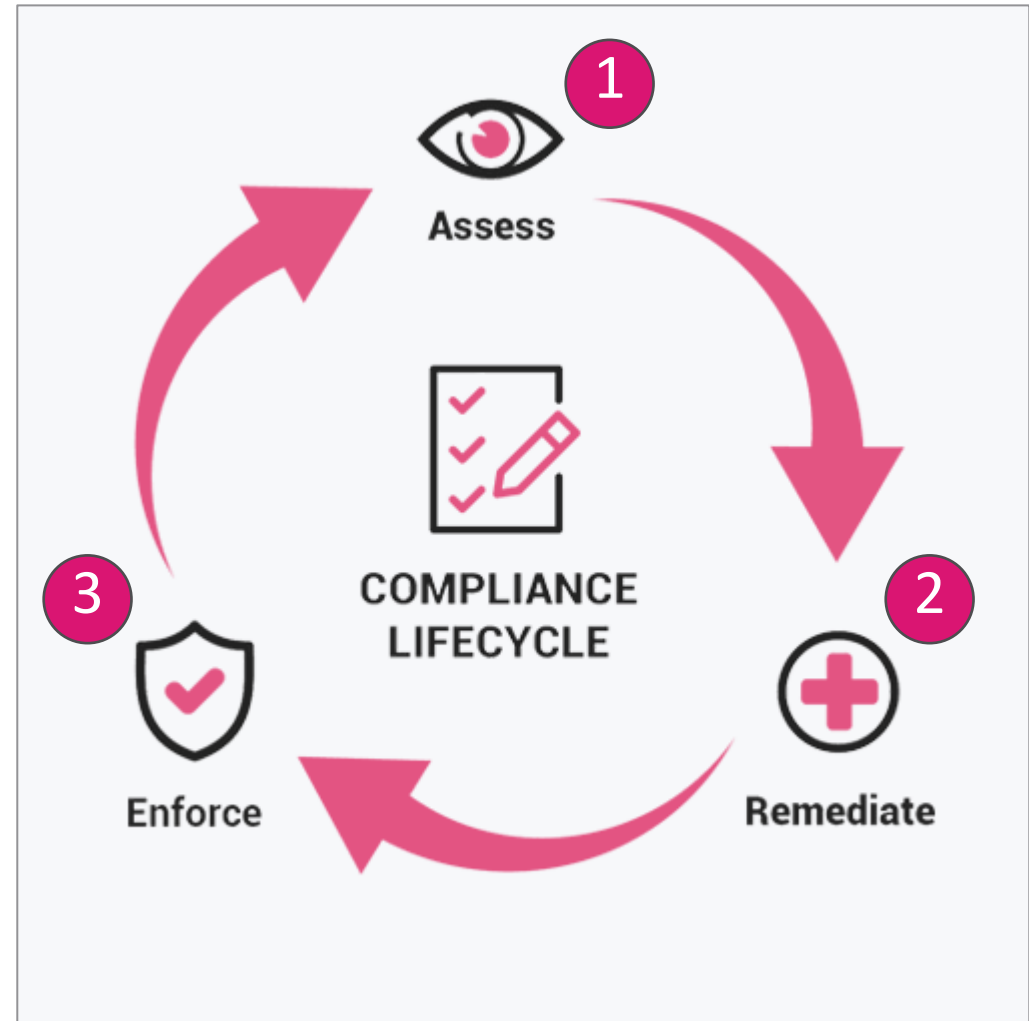


# 6 Pillars of Robust Cloud Security

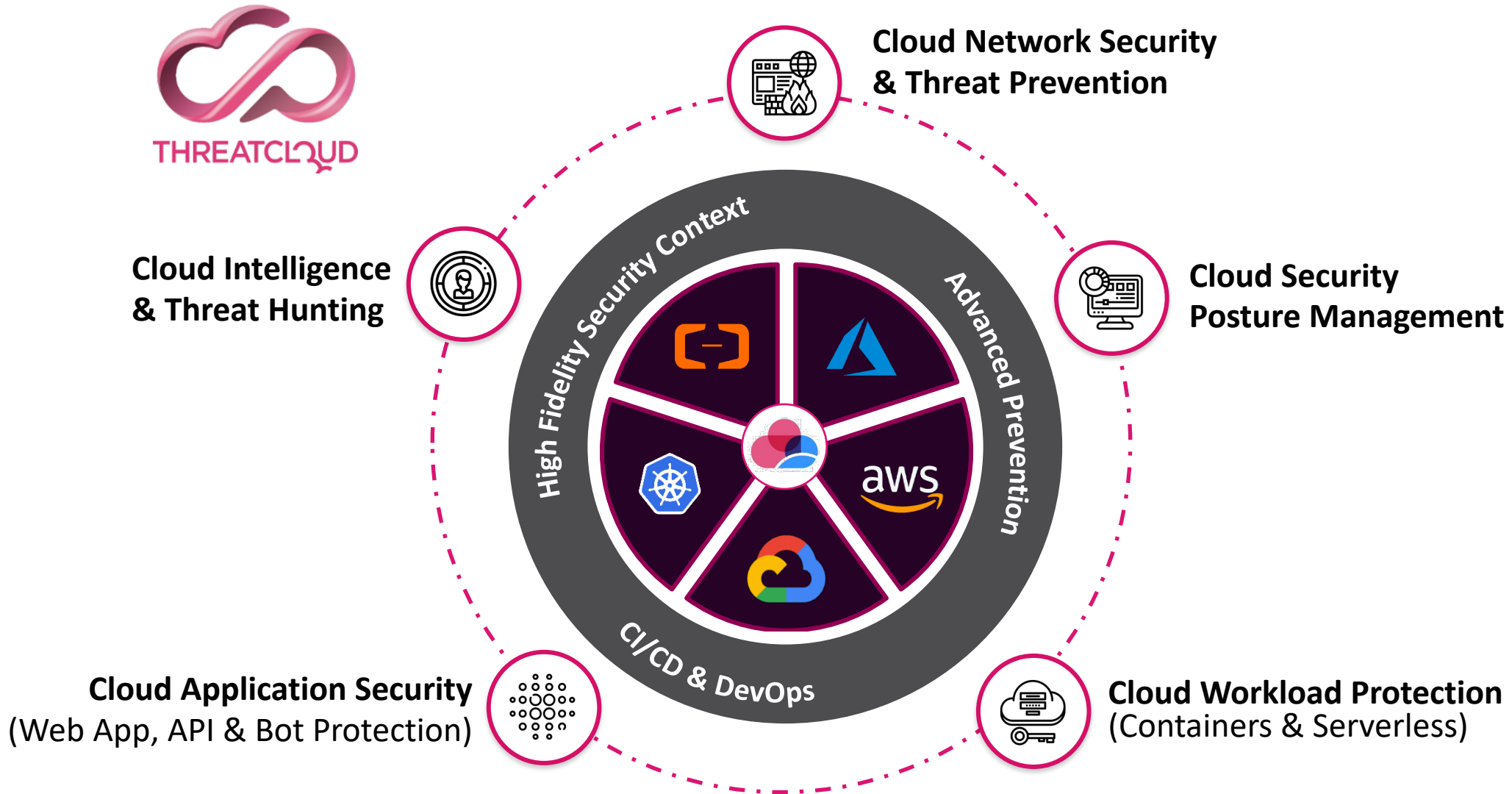
- Granular policy-based Identity and Access Management and authentication controls
- Zero-trust cloud network security controls across logically isolation networks and micro-segments
- Enforcement of virtual server protection policies and processes such as change management and software updated
- Safeguarding all applications through layering next-generation web application firewall
- Platform agnostic enforcing policies across all environments
- Threat intelligence that detects and remediates known and unknown threats in real-time



# Implement Continuous Compliance and Auto Remediation for Public Clouds



# Mitigating Native Cloud Security Gaps – Preventing Your Breach



# Developing Your Security Strategy

YOU DESERVE THE BEST SECURITY

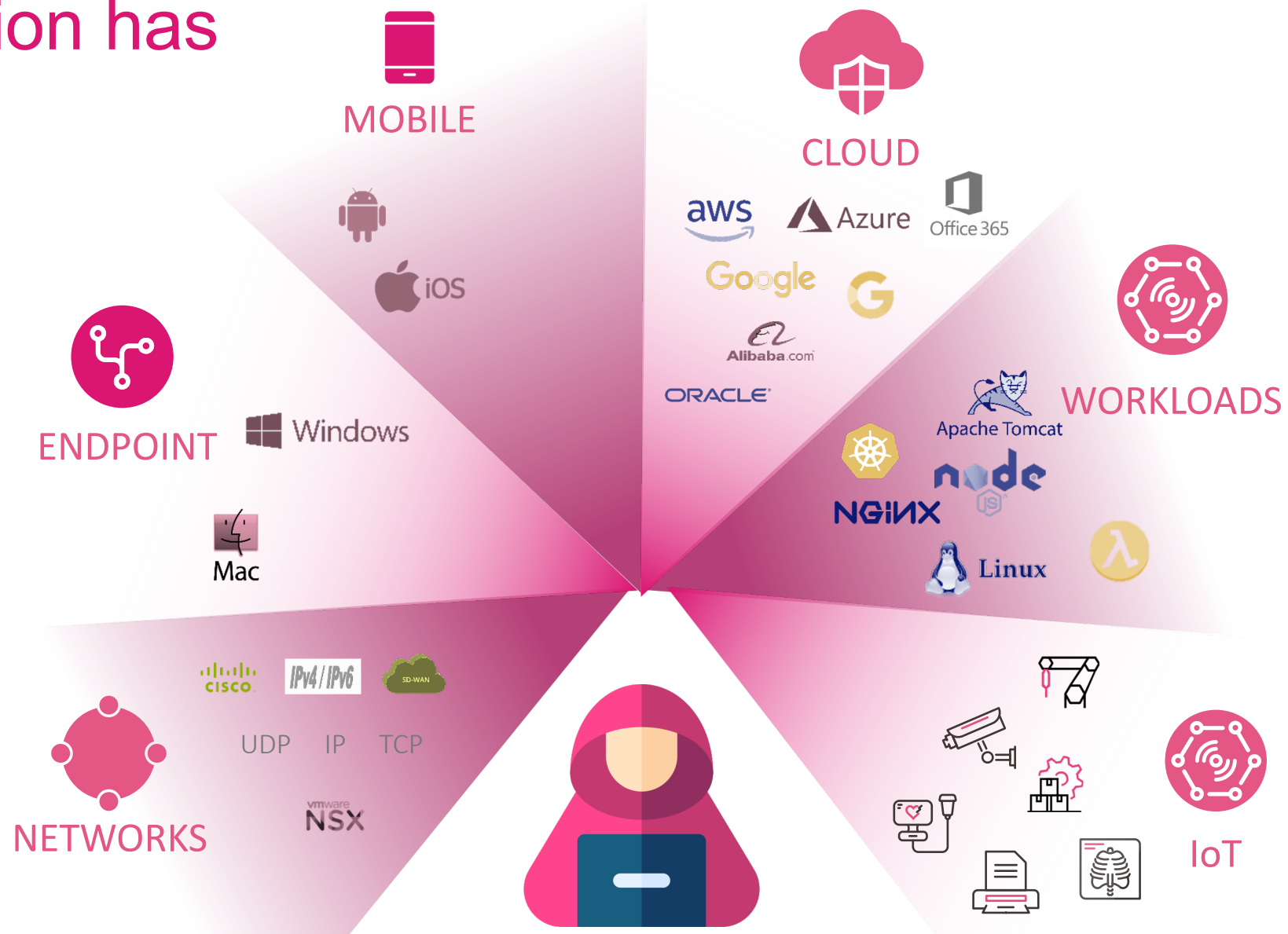
# Do you have a formal cyber security strategy?



Survey: 1,243 UK Business, 696 micro, 264 small, 149 medium, 134 large, 82 finance and insurance, 424 charities

# Digital Transformation has No Perimeters

## A threat actor will find your weakest link





# YOUR COMPLETE SECURITY STRATEGY

**CloudGuard** | SECURE THE CLOUD

<p><b>CloudGuard</b> Posture Management Posture Management &amp; Visibility</p>	<p><b>CloudGuard</b> Intelligence Network Traffic Analysis</p>
<p><b>CloudGuard</b> Workload Runtime Workload Protection</p>	<p><b>CloudGuard</b> Network Cloud Access Control &amp; Prevention</p>
<p><b>CloudGuard</b> AppSec Web and API Protection</p>	

Multi & Hybrid Cloud

SD-WAN

**Quantum** | SECURE THE NETWORK

<p><b>Quantum</b> Security Gateway Enterprise Firewall</p>	<p><b>Quantum</b> Maestro Hyperscale</p>	<p><b>Quantum</b> Lightspeed Hyper-Fast Firewall</p>	<p><b>Quantum</b> R31 Secure-OS</p>
<p><b>Quantum</b> SMB SMB-suite</p>	<p><b>Quantum</b> Rugged ICS Security</p>	<p><b>Quantum</b> IoT Protect IoT Security</p>	<p><b>Quantum</b> Smart-1 Cloud Security Management</p>

<ul style="list-style-type: none"> <li>Access Control</li> <li>Advanced Threat Prevention</li> <li>Data Protection</li> </ul>	<ul style="list-style-type: none"> <li>Wide Range of Firewalls</li> <li>Up to 3 Tbps Throughput</li> <li>1,10,25,40,100 GbE ports</li> <li>Wi-Fi, DSL, 3G/4G/ LTE</li> </ul>	<ul style="list-style-type: none"> <li>Unified Policy</li> <li>Autonomous Security</li> <li>Event Management</li> <li>Compliance</li> </ul>
---	--	---

**Horizon**

UNIFIED MANAGEMENT & SECURITY OPERATIONS

**Horizon**  
MDR  
Managed Prevention & Response

**Horizon**  
XDR  
Extended Prevention & Response

**Horizon**  
Events  
Unified Events

**INFINITY**  
PORTAL  
Management & Unified Visibility

**THREATCLOUD**  
Threat Intelligence

**Harmony** | SECURE USERS & ACCESS

REMOTE ACCESS

**Harmony**  
Connect (SASE)

- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Branch FWaaS

EMAIL & COLLABORATION

**Harmony**  
Email & Collaboration

- Account Takeover Protection
- Data Loss Prevention
- Threat Prevention
- Zero Phishing

ENDPOINT & MOBILE

<p><b>Harmony</b> Endpoint</p> <ul style="list-style-type: none"> <li>Threat Prevention</li> <li>Anti-Ransomware</li> <li>Forensics</li> <li>Secure Media</li> <li>Access Control</li> </ul>	<p><b>Harmony</b> Browse</p> <ul style="list-style-type: none"> <li>Zero Day Browser Protection</li> <li>Threat Prevention</li> <li>Zero Phishing</li> </ul>	<p><b>Harmony</b> Mobile</p> <ul style="list-style-type: none"> <li>App Protection</li> <li>Network Protection</li> <li>Device Protection</li> </ul>
--	--	--

# SUMMARY

- Every business and sector under attack
- Layering security provides best defence
- End-to-End Security – No Weaknesses



**THANK YOU**

 deryckm@checkpoint.com

 [www.linkedin.com/in/deryckmitchelson/](http://www.linkedin.com/in/deryckmitchelson/)

YOU DESERVE THE BEST SECURITY