How to Respond to the 2020 Threat Landscape

Jonathan Care

Gartner®

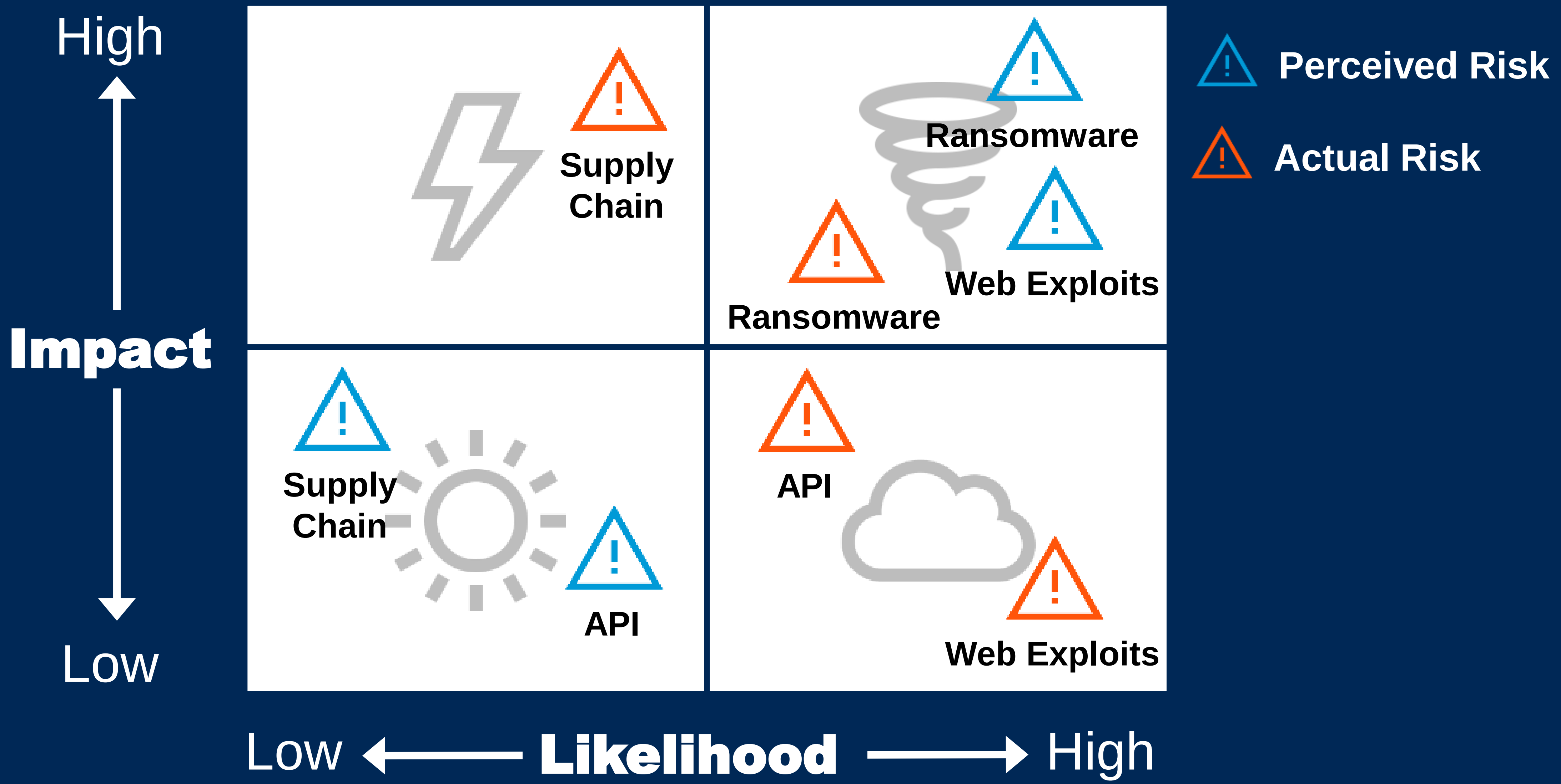
Threat Hype Overshadows Actual Risk

Threat Post: "$5.3M Ransomware Demand: Massachusetts City Says No Thanks"

WPVI-TV: "Wawa Announces Massive Data Breach, 'Potentially All' Locations Affected, CEO says"

Security Magazine: "Digital Shadows Report: Dark Web's Reaction to COVID-19"

Allianz: "Cyber Risk ranked #1 Global risk in 2019"



Perceived Risk

Actual Risk

High

Impact

Low

Supply Chain

Ransomware

Web Exploits

Ransomware

Supply Chain

API

API

Web Exploits

Low

Likelihood

High

Short-Term Threat Forecast

Short-Term Threat Forecast

1

Ransomware and Phishing Top the List

2

Supply Chain Is a Weak Link

3

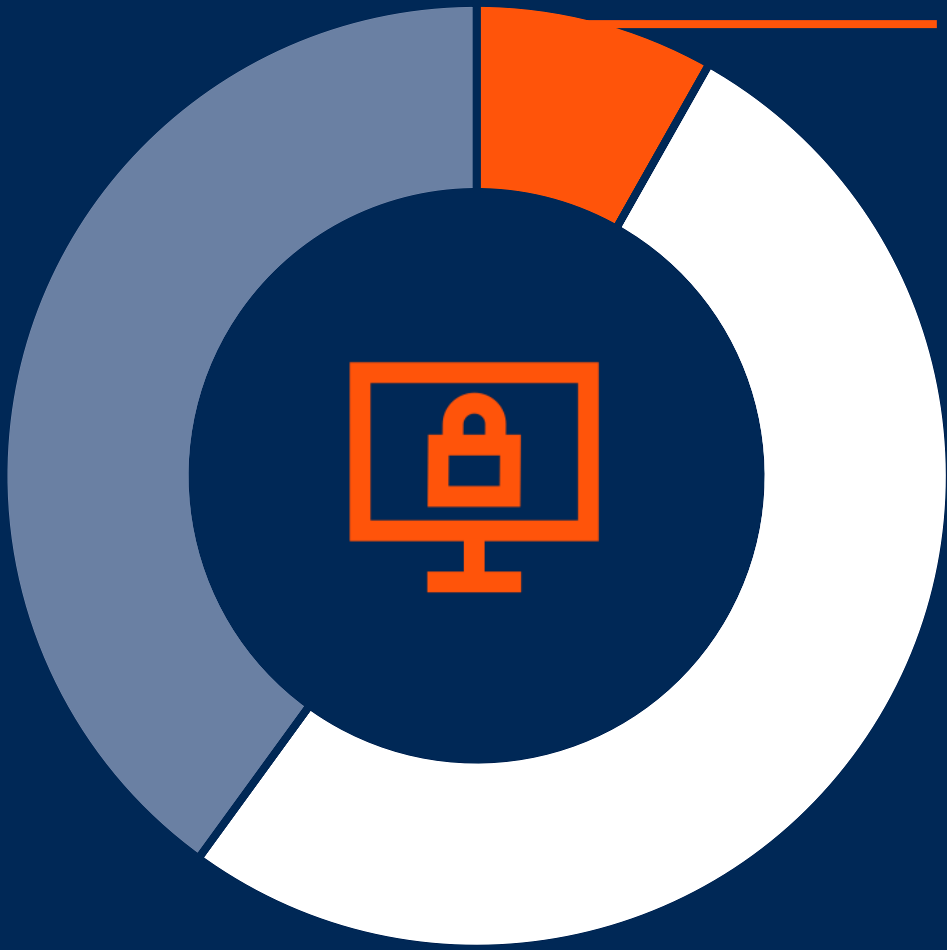
Threats Diversify

Gartner

66%

of companies agree ransomware is a serious danger

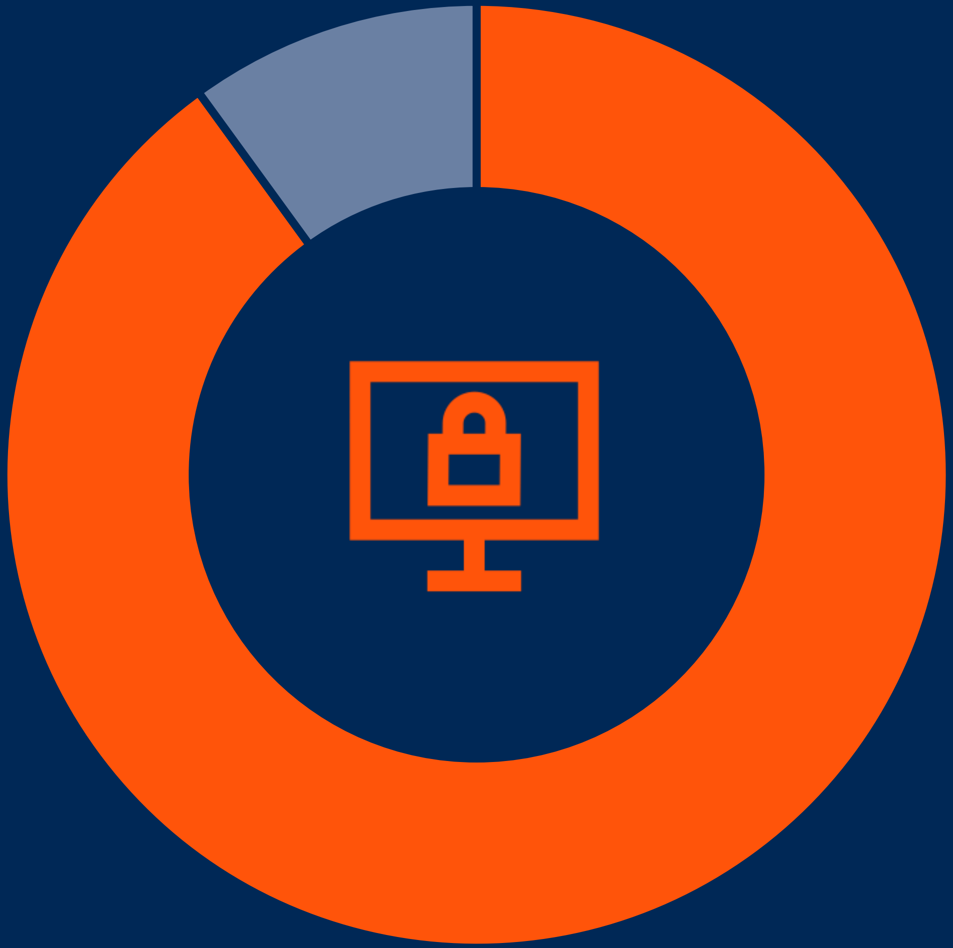
Source: “The Rise of Ransomware,” Ponemon Institute



13%

are prepared for
a ransomware attack

Source: “The Rise of Ransomware,” Ponemon Institute

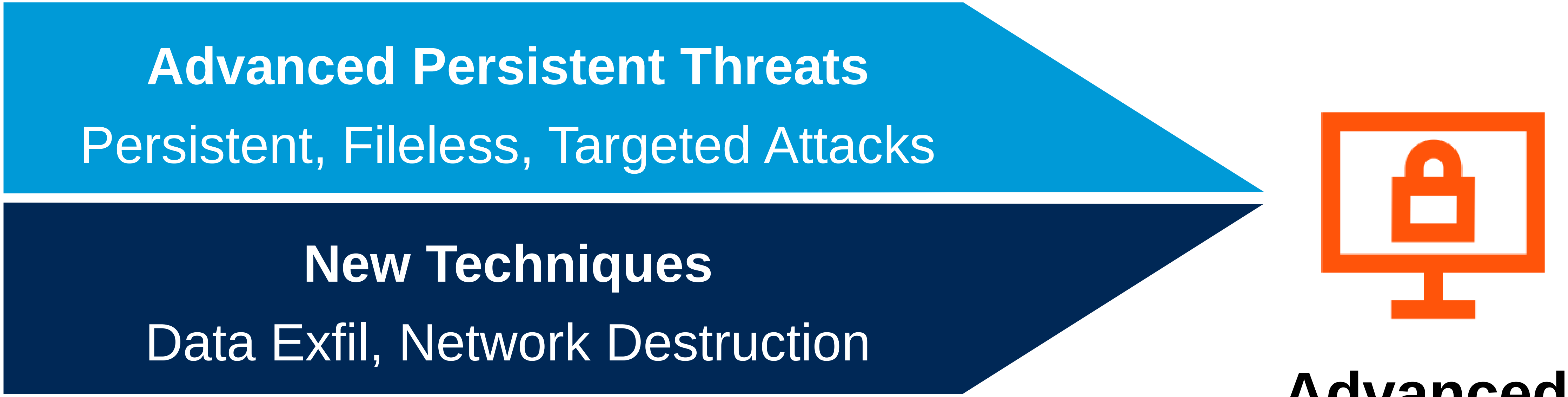


90%

of ransomware attacks are preventable!

Source: Gartner (2019)

Ransomware — On the Rise in 2019



Advanced Persistent Threats

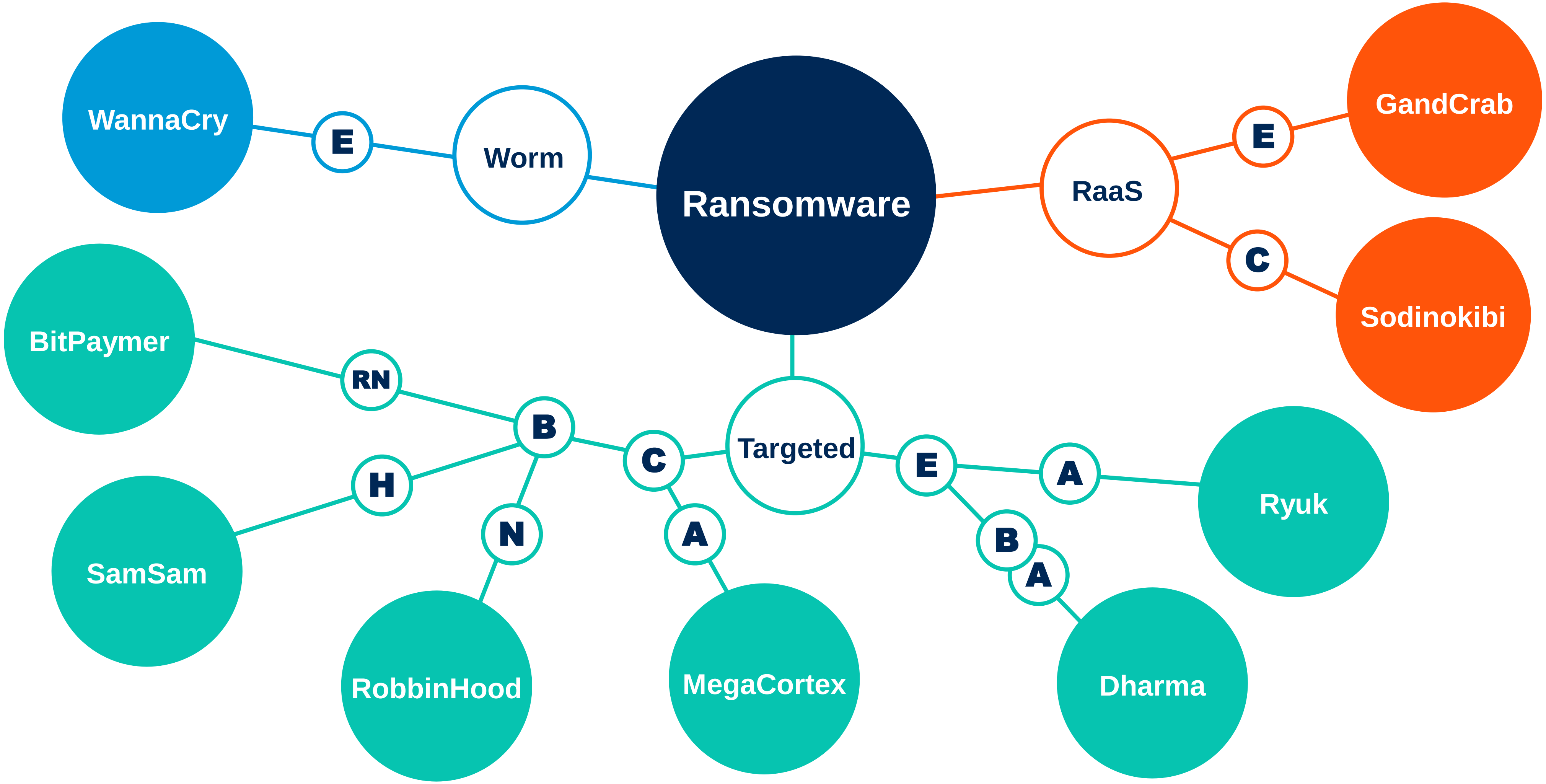
Persistent, Fileless, Targeted Attacks

New Techniques

Data Exfil, Network Destruction

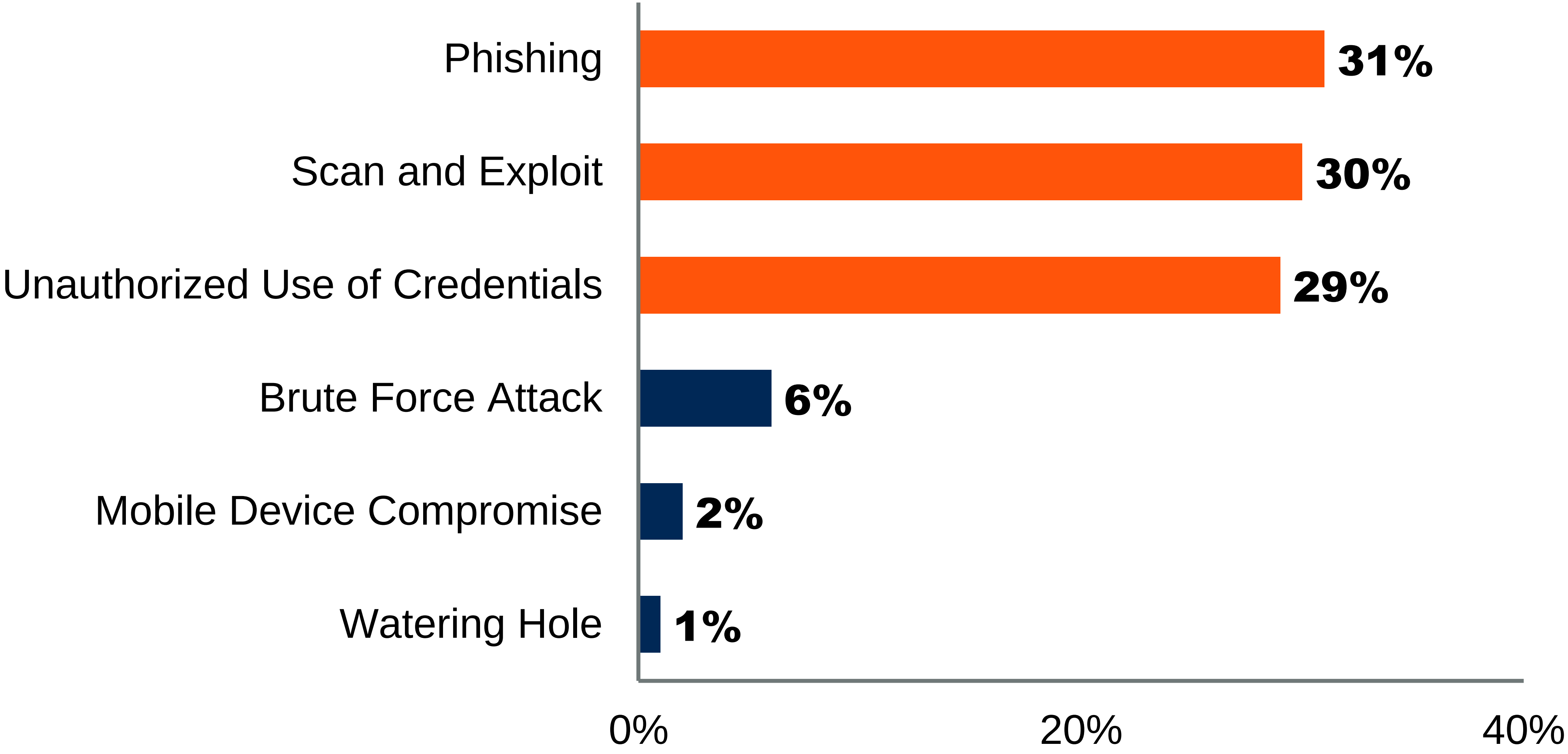
Advanced Ransomware

There Is No Single Type of Ransomware



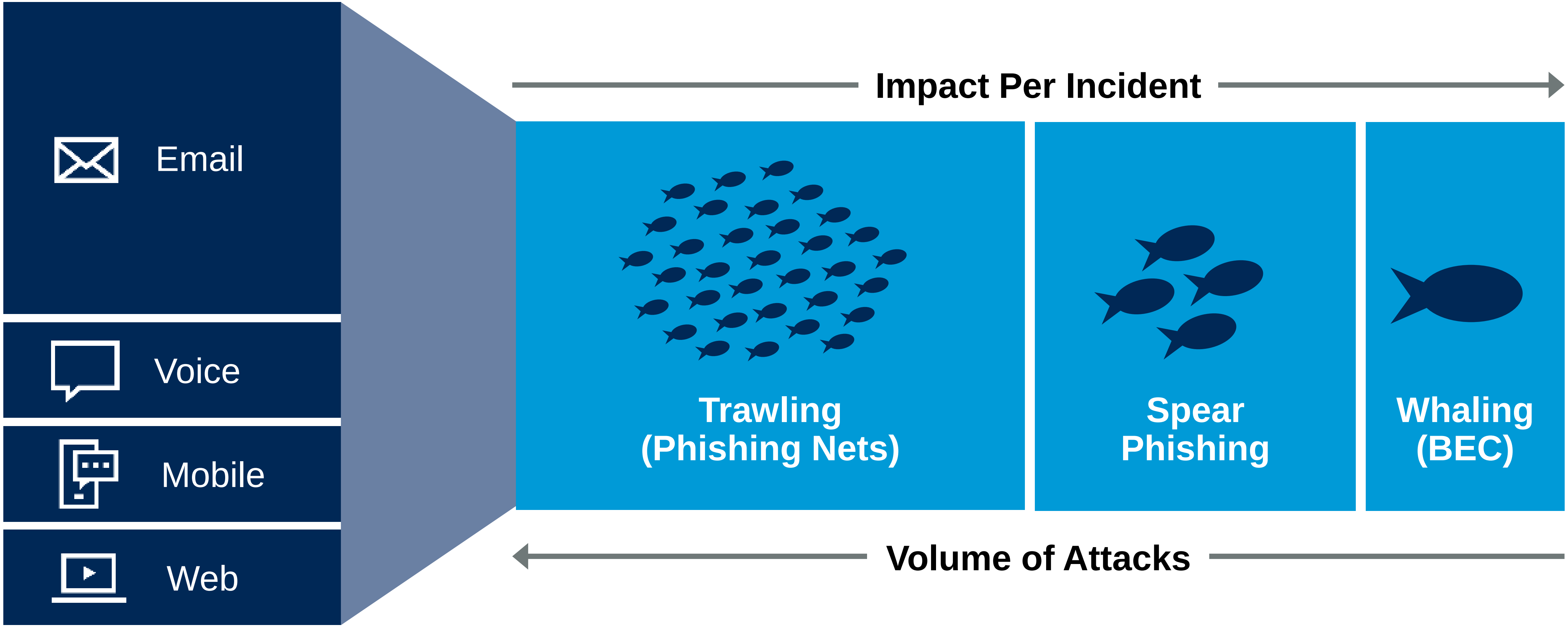
Source: "Sophos 2020 Threat Report," Sophos
Note: Graphic reflects a sample of malware variants and not a complete list. The attributes visualized are
Privilege Escalation (E – Exploit, C – Credentials); Rename (B – Before, A – After); Key Blob (RN — Ransom Note, H – Header, N – New)

Top Initial Access Vectors



Source: IBM Security’s X-Force Threat Intelligence Index 2020

Phishing Is Complex!



Email

Voice

Mobile

Web

Impact Per Incident

Trawling (Phishing Nets)

Spear Phishing

Whaling (BEC)

Volume of Attacks

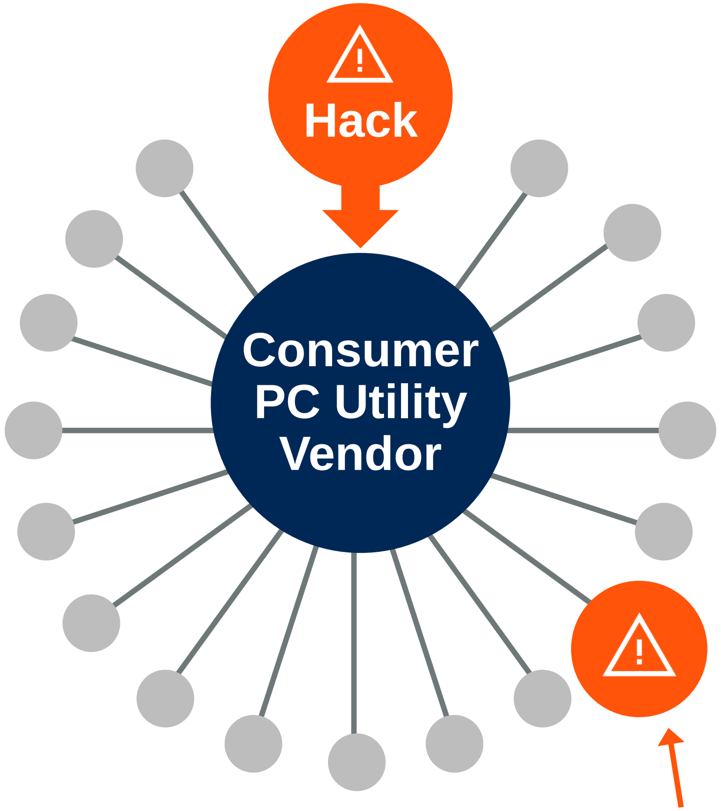
Through 2023, at least 99% of cloud security failures will be the customer's fault.

Account Takeover and Credential Stuffing

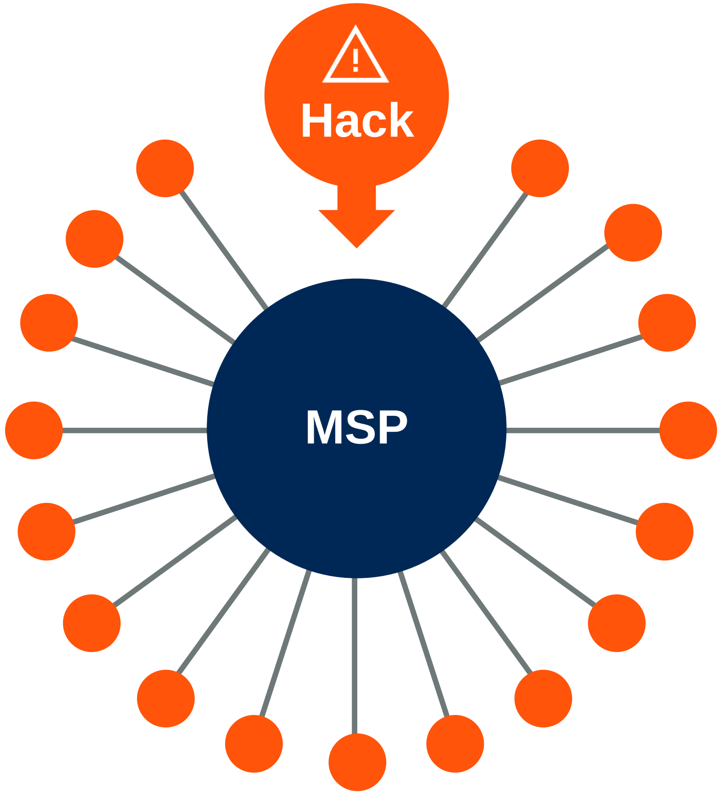
Cloud

Nontraditional Threats

Hardware/Software Supply Chain Security

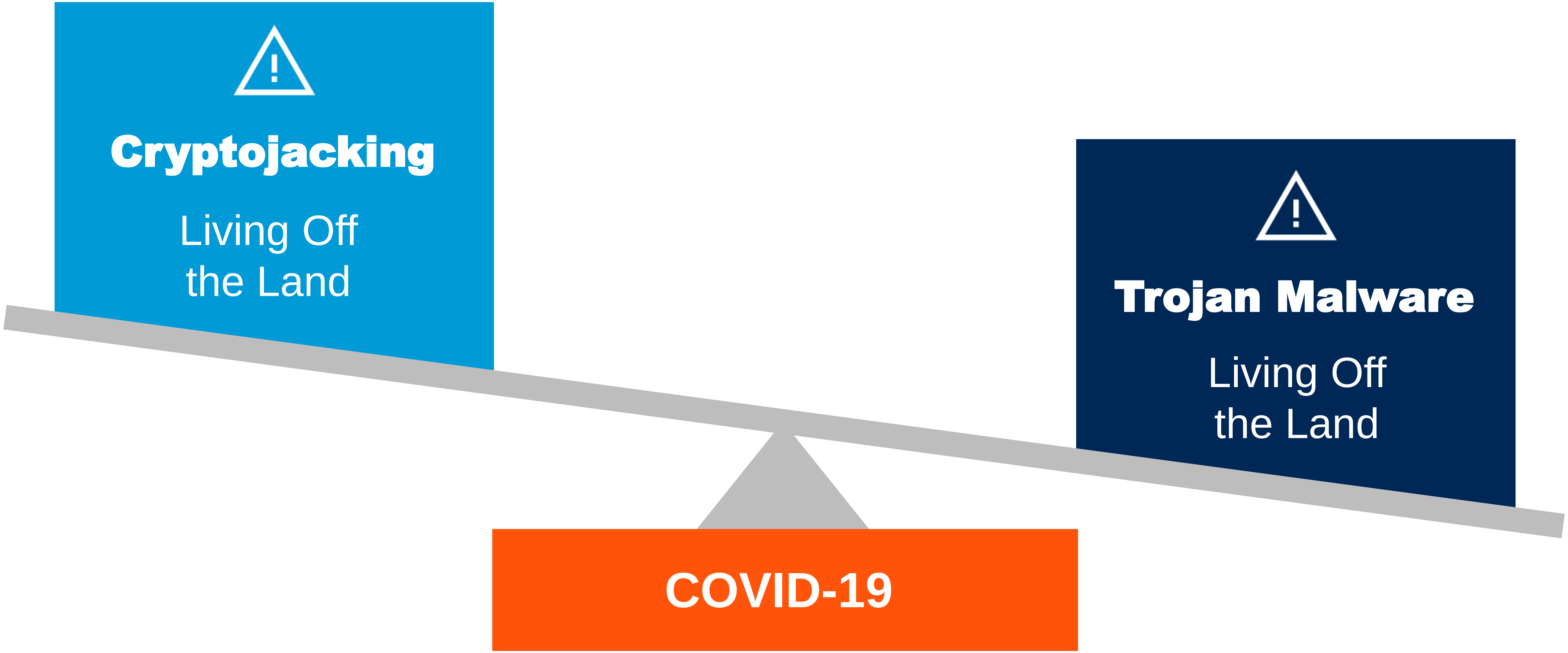


Data Stolen From Target Organization



Hundreds of Customers Impacted

Other Threats in 2020



⚠

Cryptojacking

Living Off
the Land

⚠

Trojan Malware

Living Off
the Land

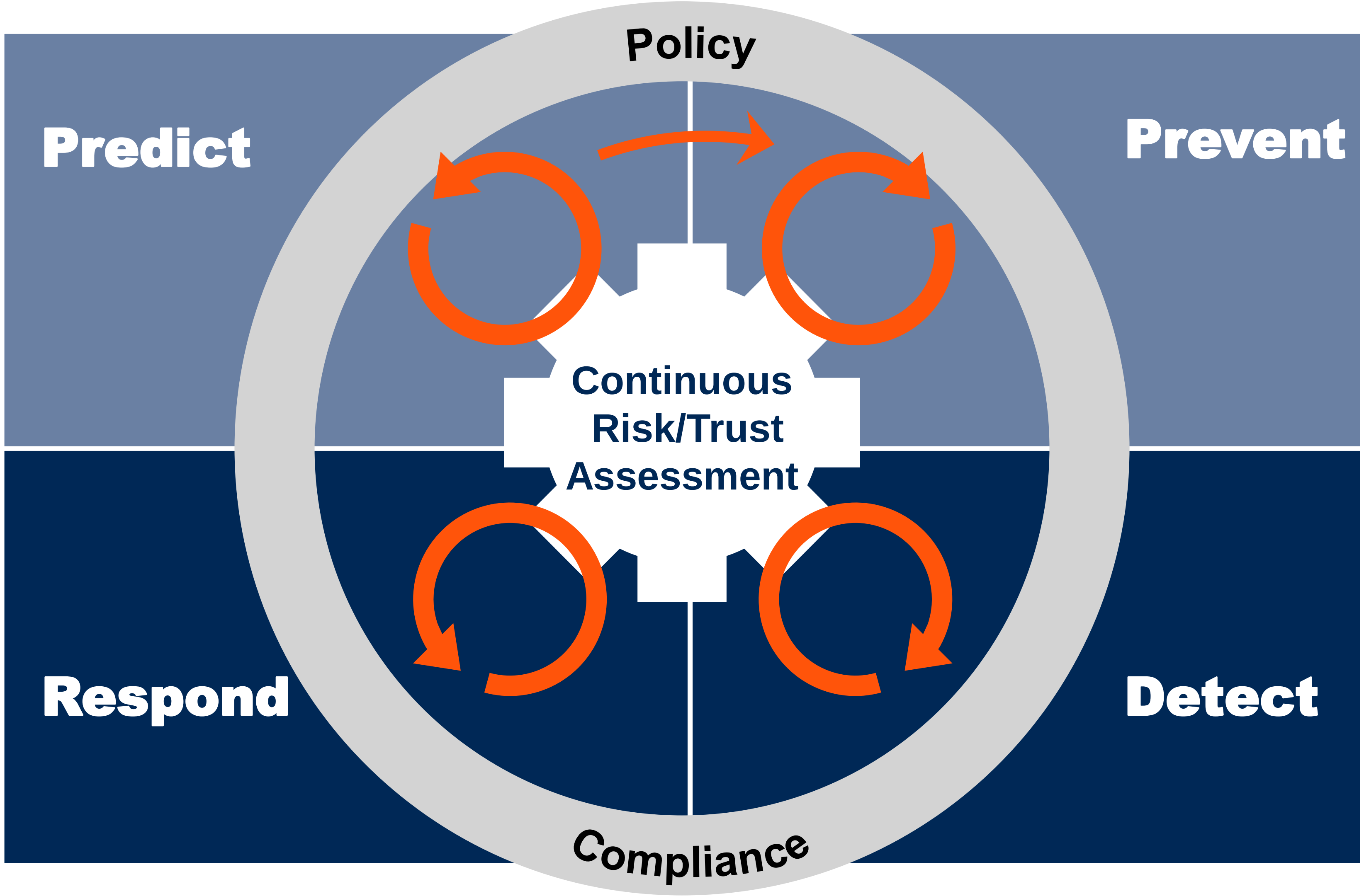
COVID-19

Summary: Short-Term Threats

- ✓ Ransomware and phishing top the list.
- ✓ Supply chain is a weak link in security threat models.
- ✓ Cloud threats are mostly due to misconfigurations.
- ✓ Take action now to retire obsolete technologies.

How to Prepare for Short-Term Threats Today

Continuous Adaptive Risk and Trust Assessment (CARTA)



See the complete diagram in the appendix

CARTA — Ransomware Protection

Predict

- Risk-Based Vulnerability Management
- Attack Surface Management
- Continuous Automated Attack Platforms
- Threat Modeling (MITRE ATT&CK, P.A.S.T.A., etc.)
- Supply Chain Risk Assessment

Prevent

- Endpoint Protection Platform
- Network Access Control
- Network Segmentation/Microsegmentation
- Network Firewall/IDPS
- Secure Web Gateway (+ Browser Isolation)

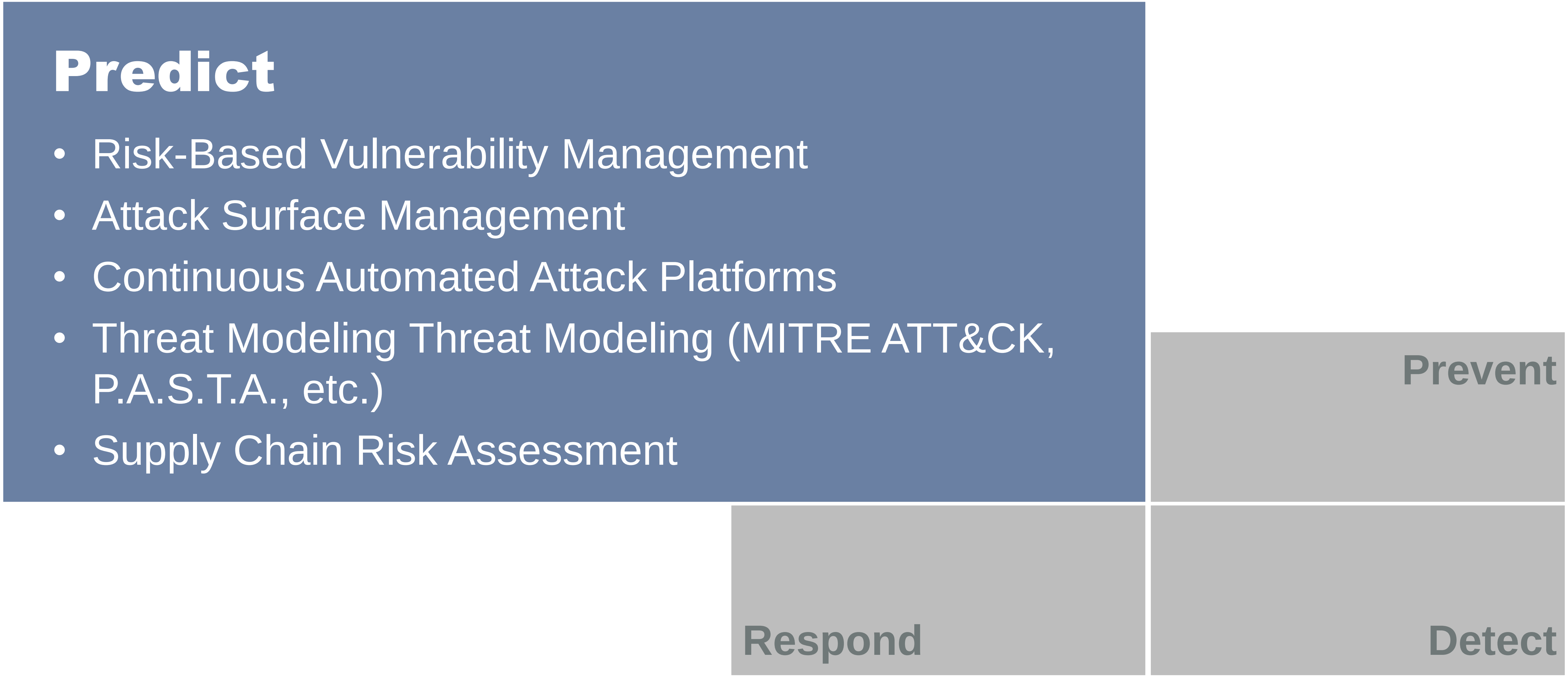
Respond

- Automated Response Actions (SOAR)
- Execute Business Continuity and DR Plans
  - However Be Aware of APT
- Digital Risk Protection Services
- (U.S.) Report Infection at Internet Crime Complaint Center (IC3)

Detect

- Extended Detection and Response (XDR)
- User Activity Monitoring
- Security Information and Event Management (SIEM)
- Network Detection and Response (NDR)

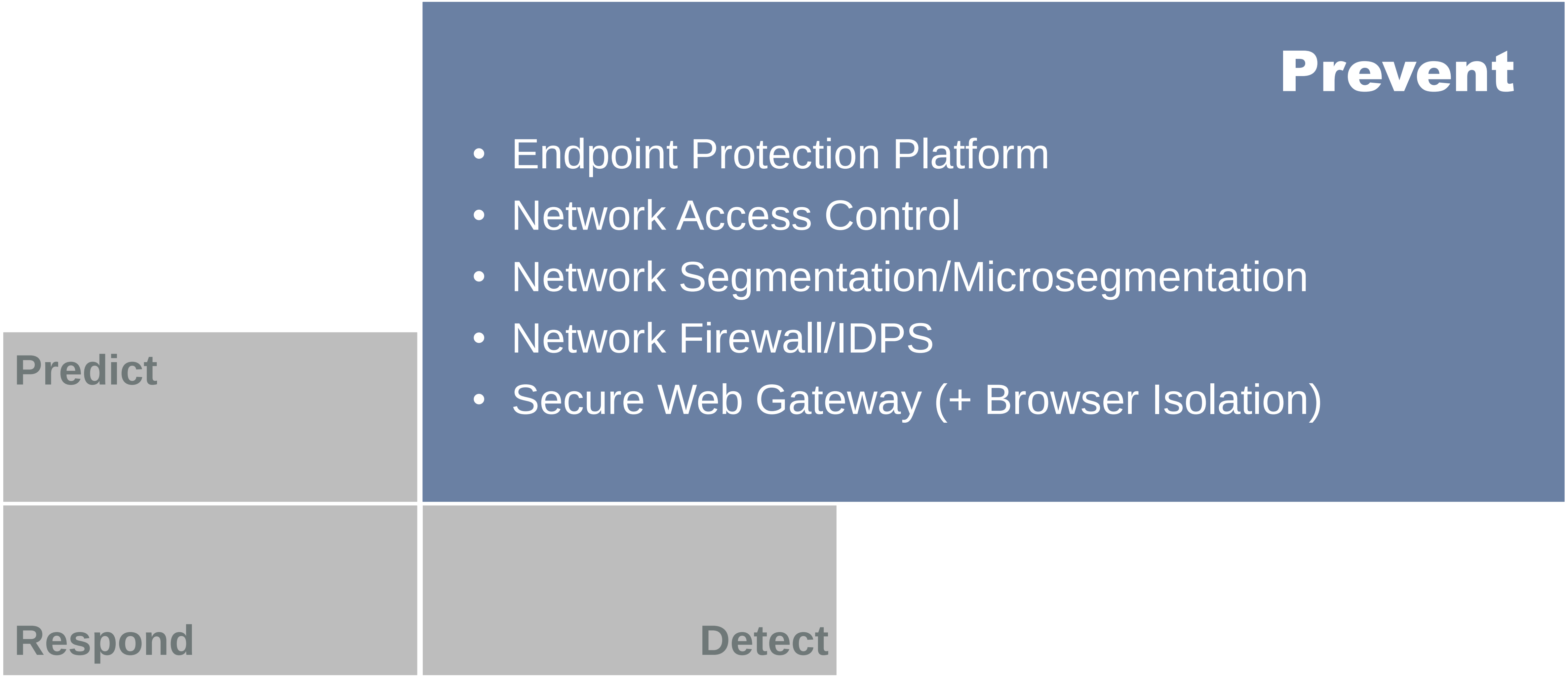
CARTA — Ransomware Protection



Predict

- Risk-Based Vulnerability Management
- Attack Surface Management
- Continuous Automated Attack Platforms
- Threat Modeling Threat Modeling (MITRE ATT&CK, P.A.S.T.A., etc.)
- Supply Chain Risk Assessment

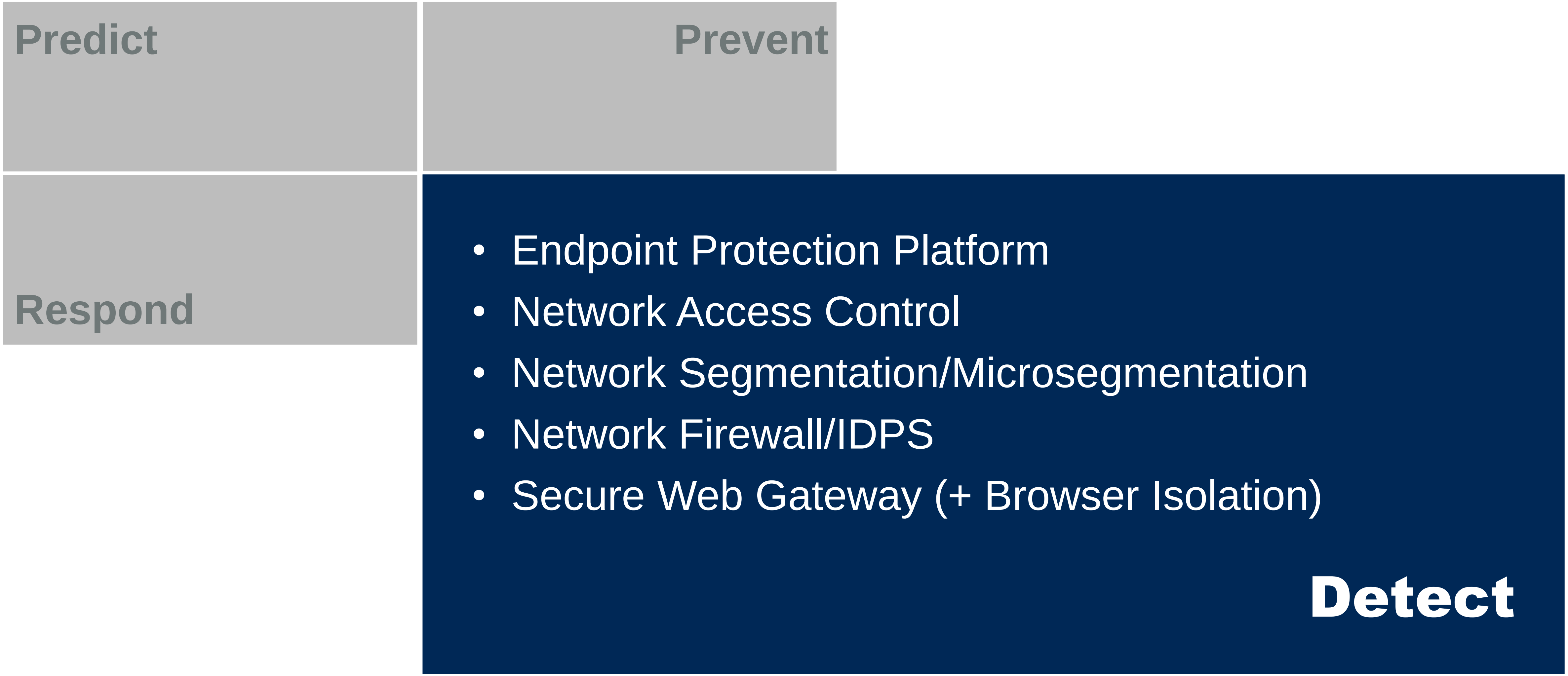
CARTA — Ransomware Protection



Prevent

- Endpoint Protection Platform
- Network Access Control
- Network Segmentation/Microsegmentation
- Network Firewall/IDPS
- Secure Web Gateway (+ Browser Isolation)

CARTA — Ransomware Protection



Predict

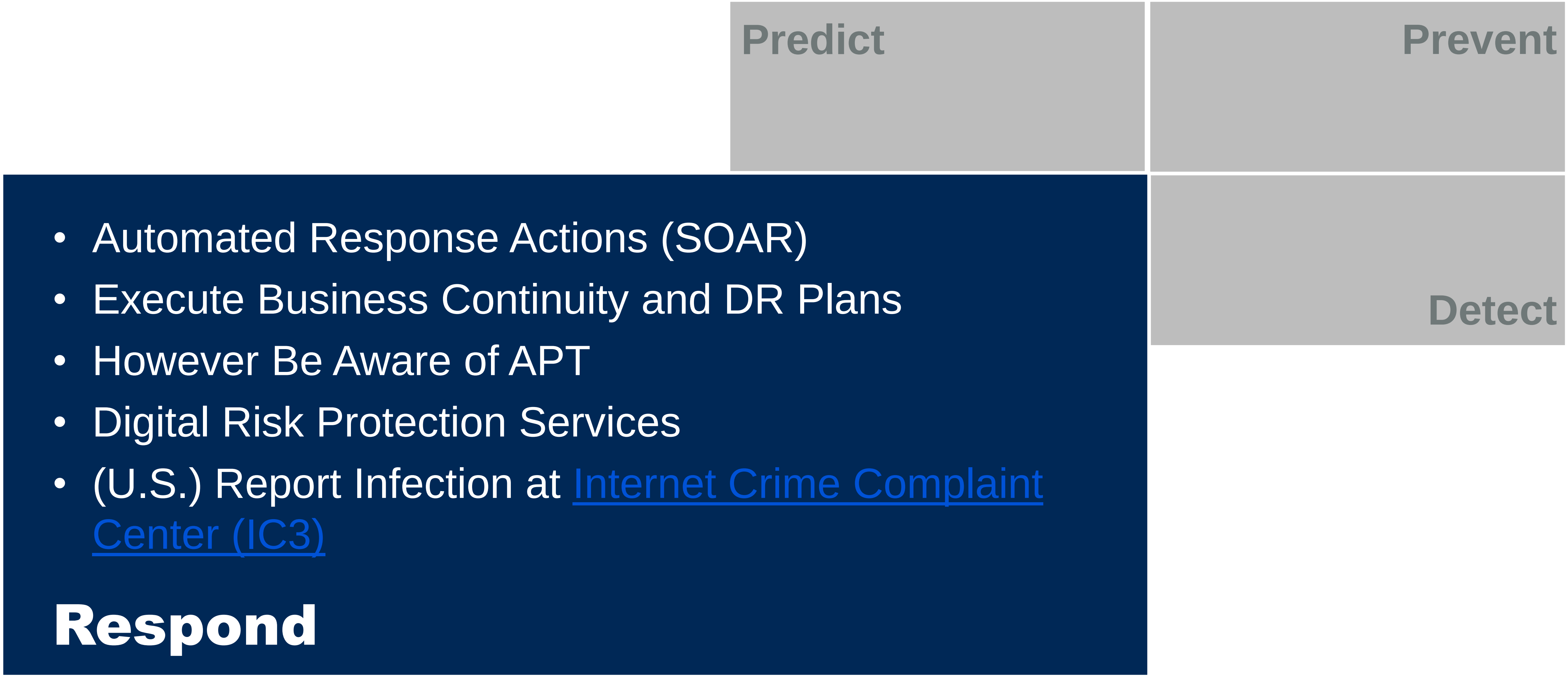
Prevent

Respond

- Endpoint Protection Platform
- Network Access Control
- Network Segmentation/Microsegmentation
- Network Firewall/IDPS
- Secure Web Gateway (+ Browser Isolation)

Detect

CARTA — Ransomware Protection



Predict

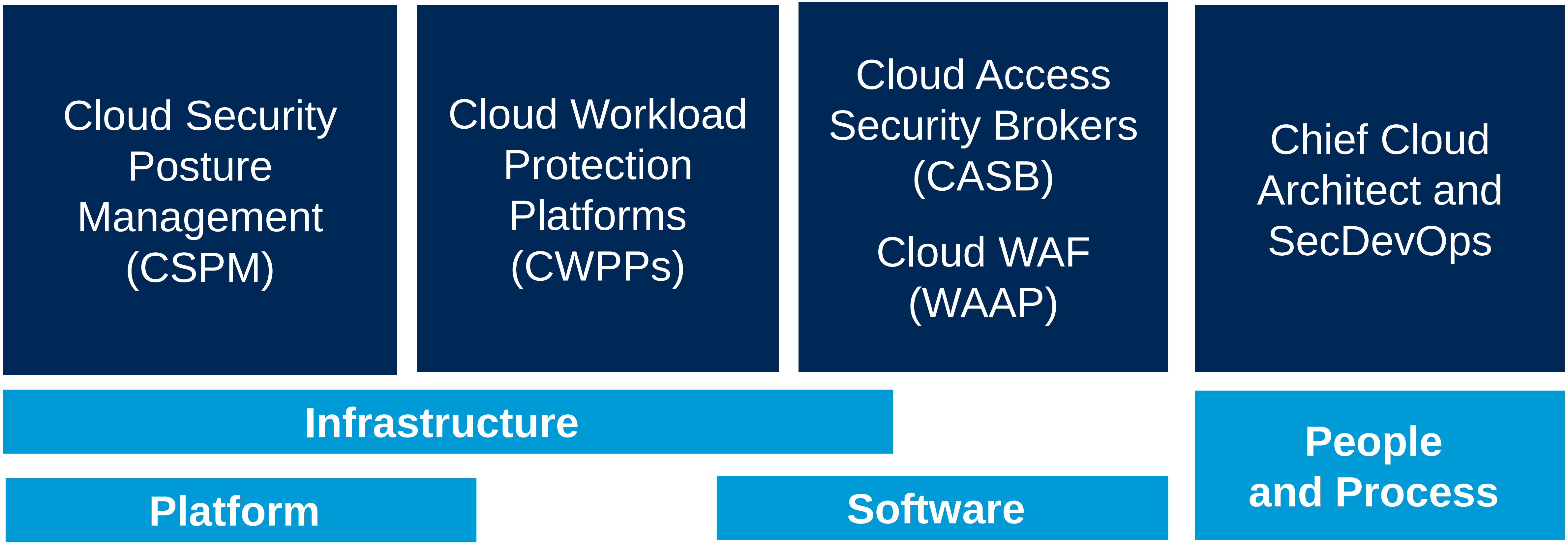
Prevent

Detect

- Automated Response Actions (SOAR)
- Execute Business Continuity and DR Plans
- However Be Aware of APT
- Digital Risk Protection Services
- (U.S.) Report Infection at [Internet Crime Complaint Center (IC3)]

Respond

Cloud Security — Four Primary Areas of Investment



Cloud Security Posture Management (CSPM)

Cloud Workload Protection Platforms (CWPPs)

Cloud Access Security Brokers (CASB)

Cloud WAF (WAAP)

Chief Cloud Architect and SecDevOps

Infrastructure

Platform

Software

People and Process

What Are Ways to Optimize Costs When Preparing?

- ✓ Basic security hygiene is key — Don’t go hunting for new, shiny objects unless it truly improves security posture.
- ✓ Tune and turn on prevention — Many companies put preventative tools in detection mode because they were burned by false positives.
- ✓ Reduce shelfware now or as contracts come up for renewal.
- ✓ Focus on people and process before the tool. People are still the weakest link, but long term, can become a powerful force!

Threats Evolve
We Must Too

Action Plan for Security and Risk Leaders

Monday Morning:

- *Pull out* your threat models (or start creating them).
- *Identify* threats which benefit from a CARTA mindset to build a more robust and resilient strategy.

Next 90 Days:

- *Use* your predictions to assess your preventative posture to prevent the highest risk threats.
- *Assess* your detect and respond capabilities including the quality, quantity, and speed of your threat landscape feedback loops.
- *Kill* vulnerable legacy technologies like Flash, Silverlight, and … Java.

Next 12 Months:

- *Evaluate* and *update* threats continuously and improve security risk profile using the CARTA mindset.

Recommended Gartner Research

- **How to Respond to the 2020 Threat Landscape**
  John Watts (G00719273)
- **Defend Against and Respond to Ransomware Attacks**
  Brad LaPorte and Paul Webber (G00463878)
- **How to Make Cloud More Secure Than Your Own Data Center**
  Neil MacDonald and Tom Croll (G00430108)
- **Facing New Vulnerabilities — Cyber-Physical Systems**
  Katell Thielemann (G00719408)
- **Protecting Against Business Email Compromise Phishing**
  Mark Harris, Ravisha Chugh and Ant Allan (G00716389)

For information, please contact your Gartner representative.