

How to Respond to the 2020 Threat Landscape

Jonathan Care

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

Gartner®

A high-action photograph of a kayaker in a red kayak navigating through turbulent white-water rapids. The kayaker is wearing a white helmet and a dark wetsuit with a purple life vest. They are holding a black paddle and looking intently at the water ahead. The water is splashing and churning around the kayak. The overall scene conveys a sense of danger and intense physical effort.

Threat Hype Overshadows Actual Risk

Gartner

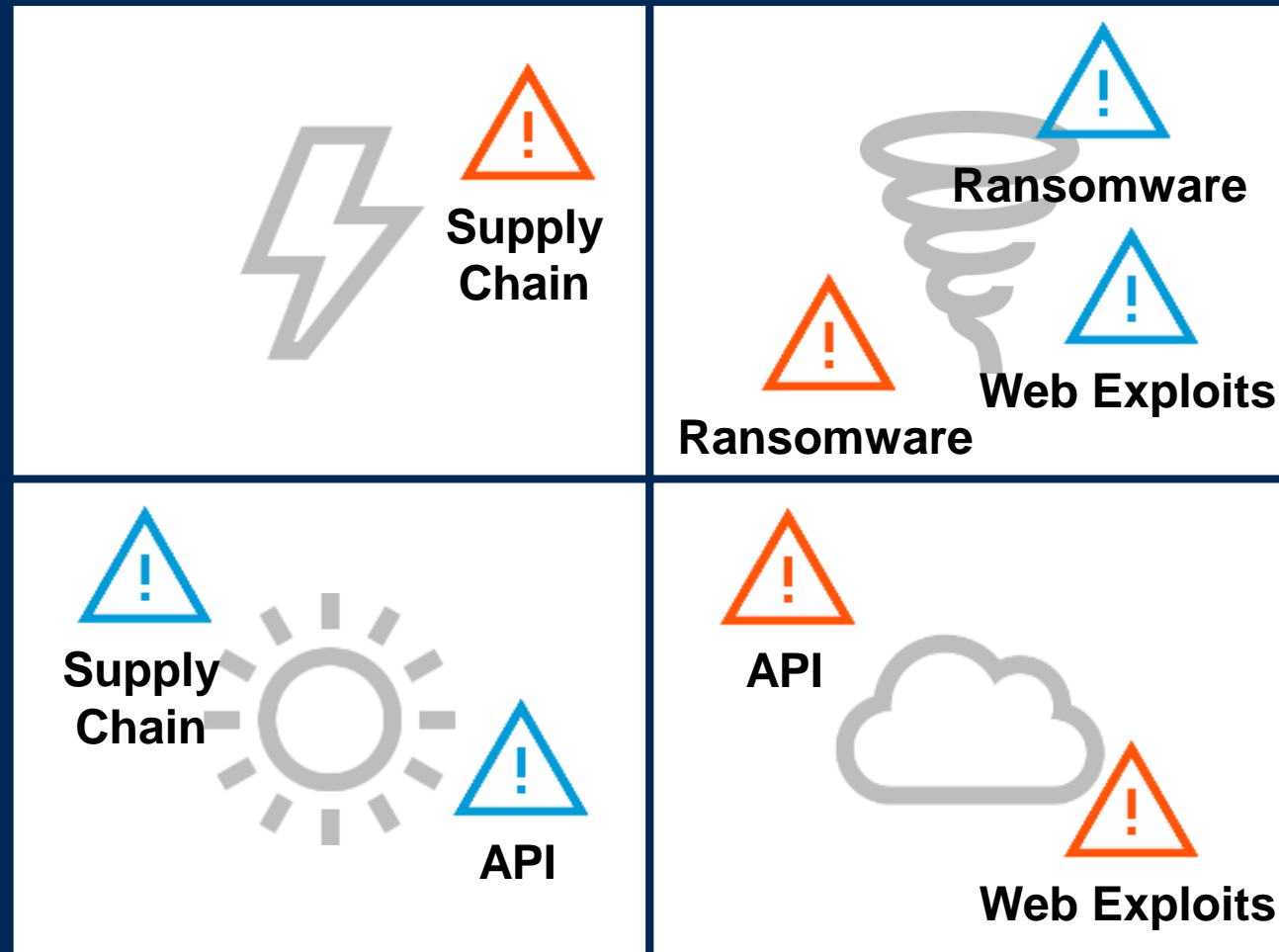
Threat Post: “\$5.3M Ransomware Demand: Massachusetts City Says No Thanks”

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”

High
↑
Impact
↓
Low



Perceived Risk
 Actual Risk

Low ← **Likelihood** → High

Short-Term Threat Forecast

Gartner®

Short-Term Threat Forecast

1

**Ransomware
and Phishing
Top the List**

2

**Supply Chain
Is a Weak Link**

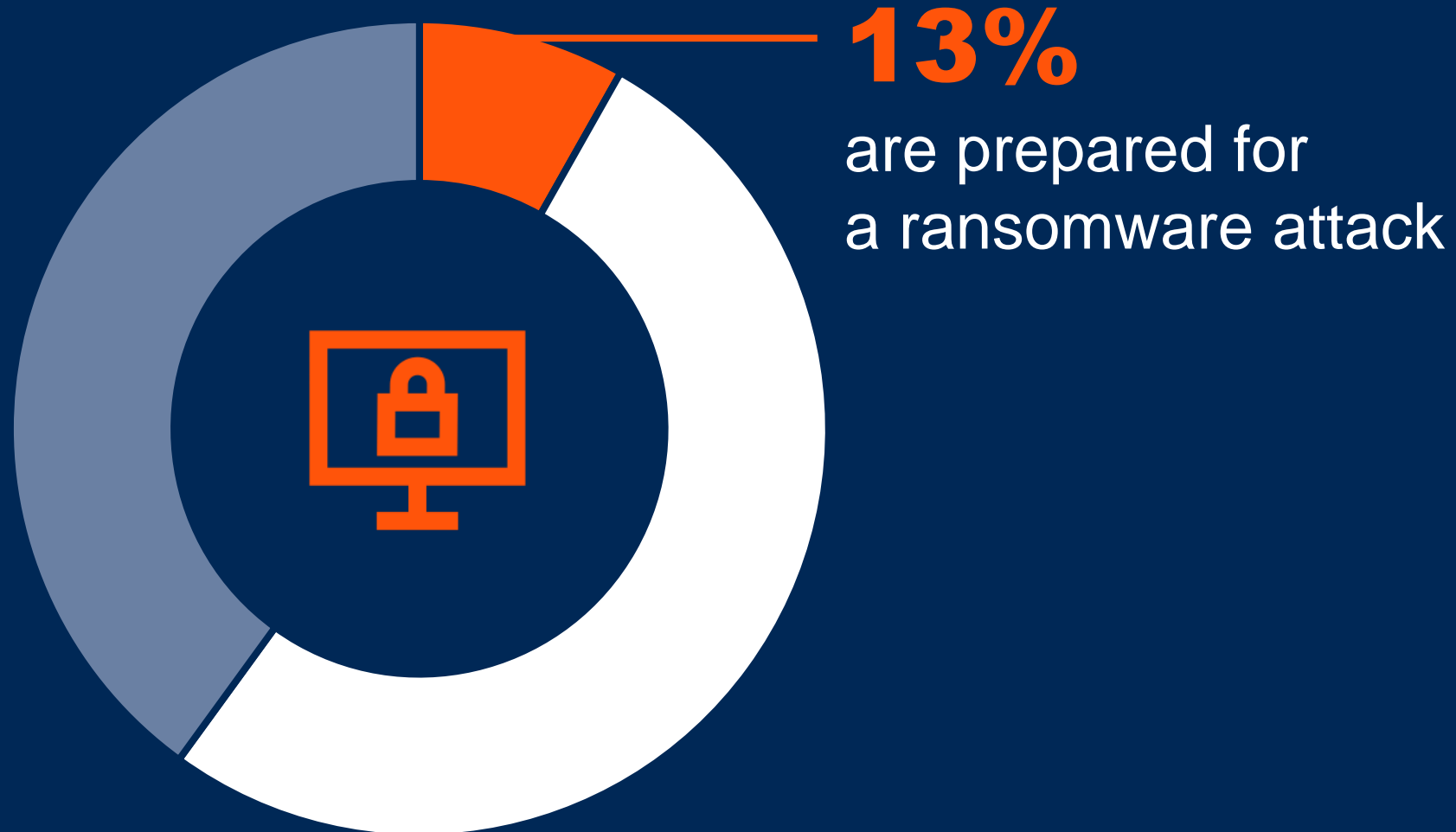
3

**Threats
Diversify**

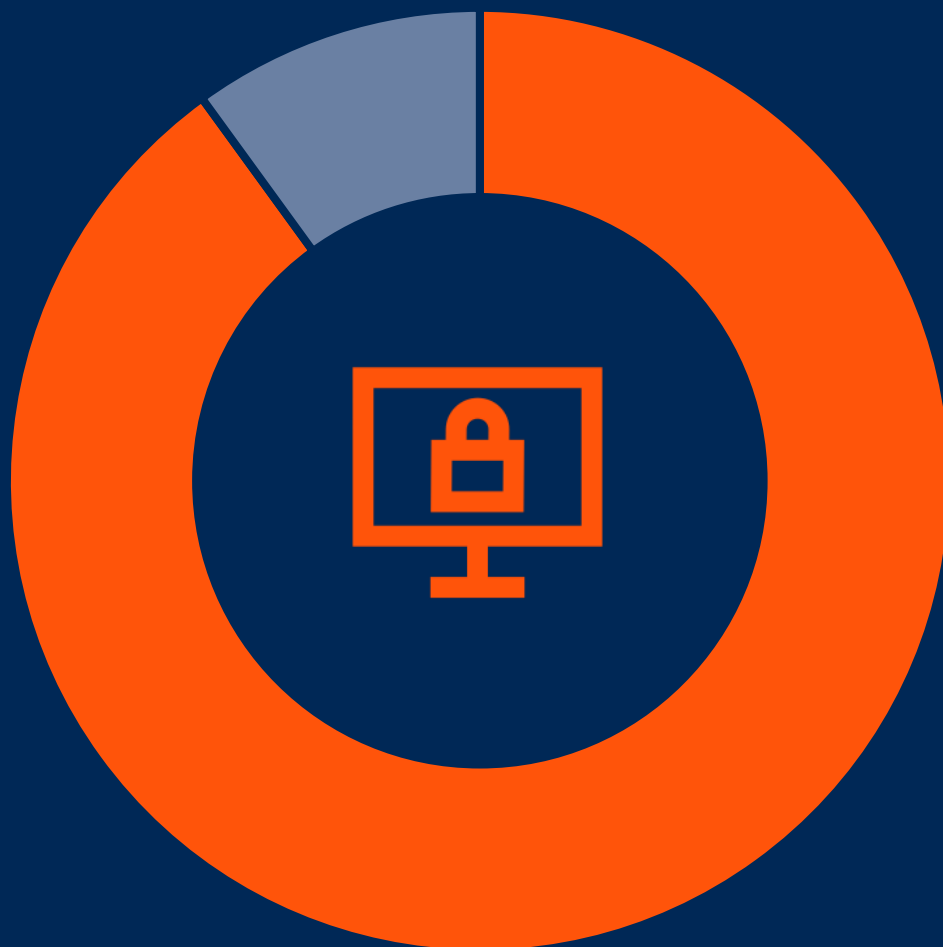


66%
of companies agree
ransomware is a
serious danger

Source: [“The Rise of Ransomware,”](#) Ponemon Institute



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

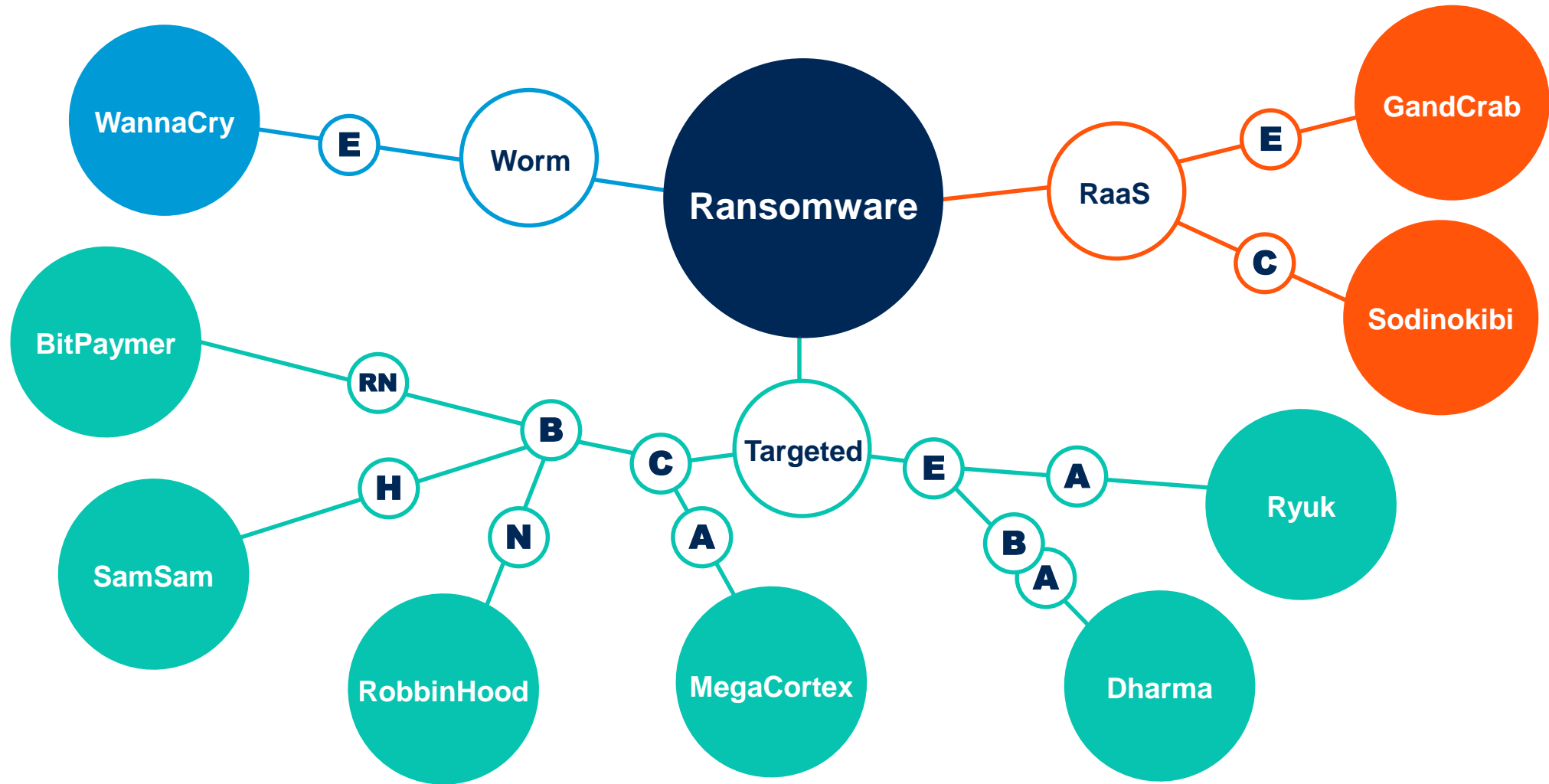
New Techniques

Data Exfil, Network Destruction



**Advanced
Ransomware**

There Is No Single Type of Ransomware

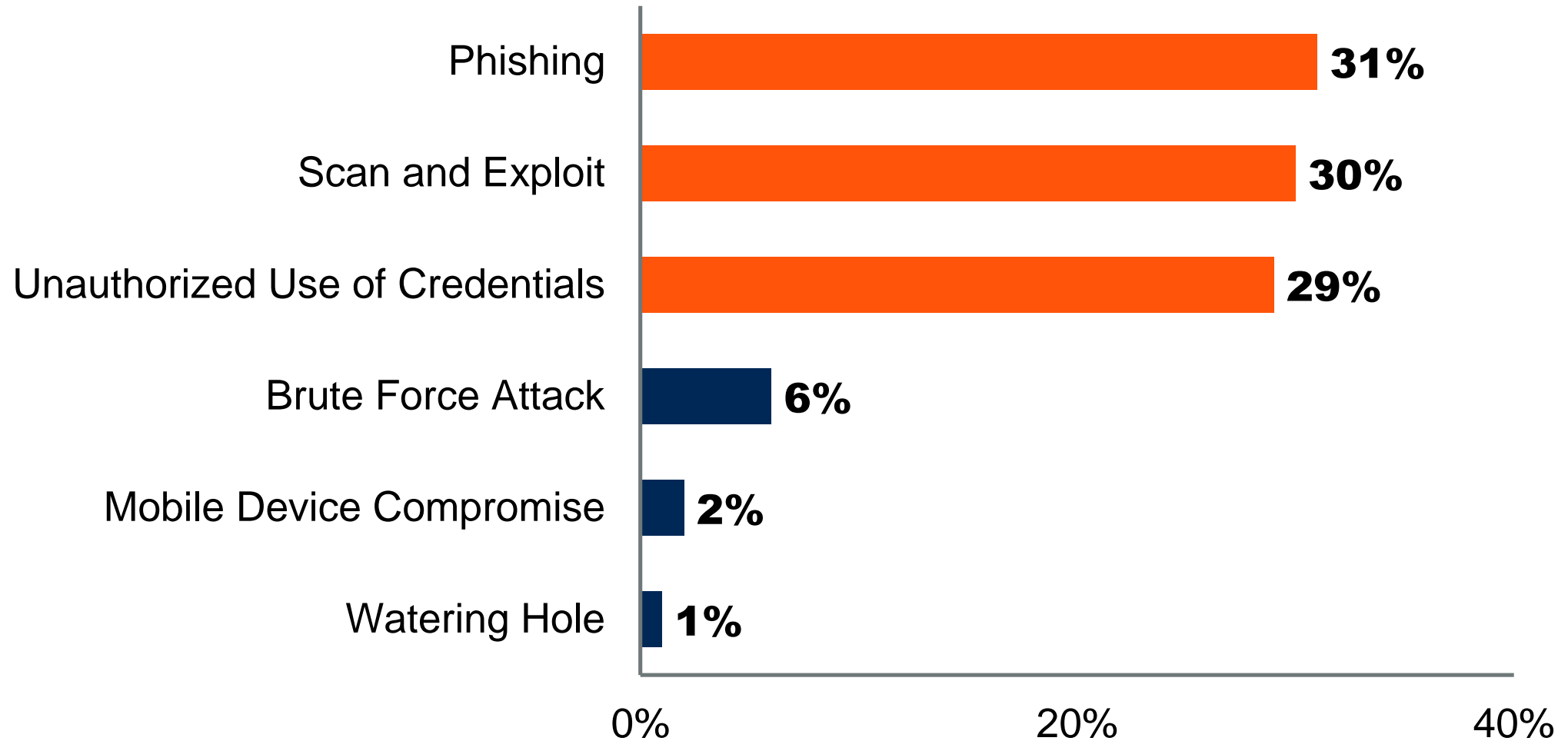


Source: ["Sophos 2020 Threat Report,"](#) Sophos

Note: Graphic reflects a sample of malware variants and not a complete list. The attributes visualized are

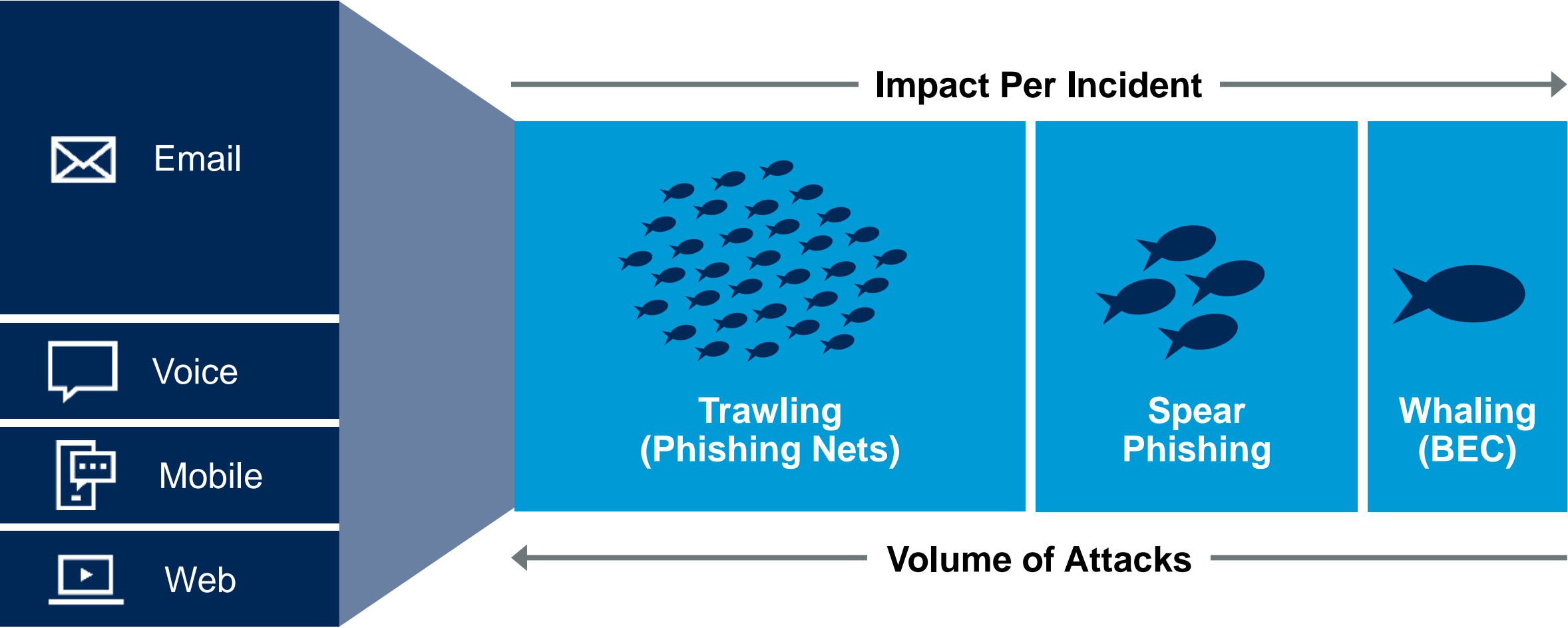
Privilege Escalation (E – Exploit, C – Credentials); Rename (B – Before, A – After); Key Blob (RN — Ransom Note, H – Header, N – New)

Top Initial Access Vectors



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

Phishing Is Complex!





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

Account Takeover and Credential Stuffing

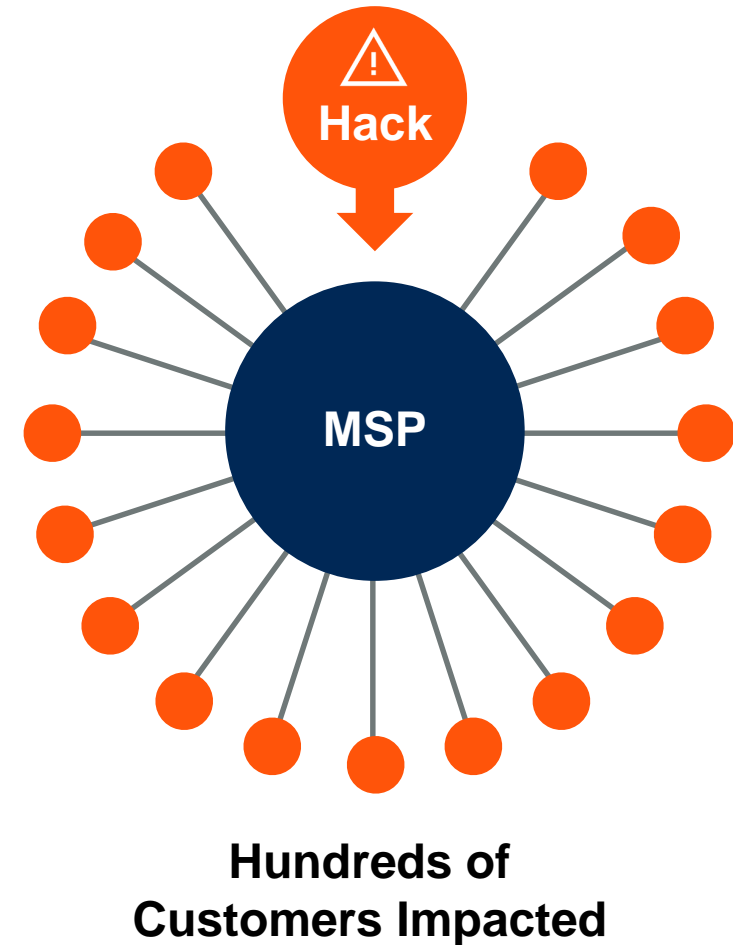
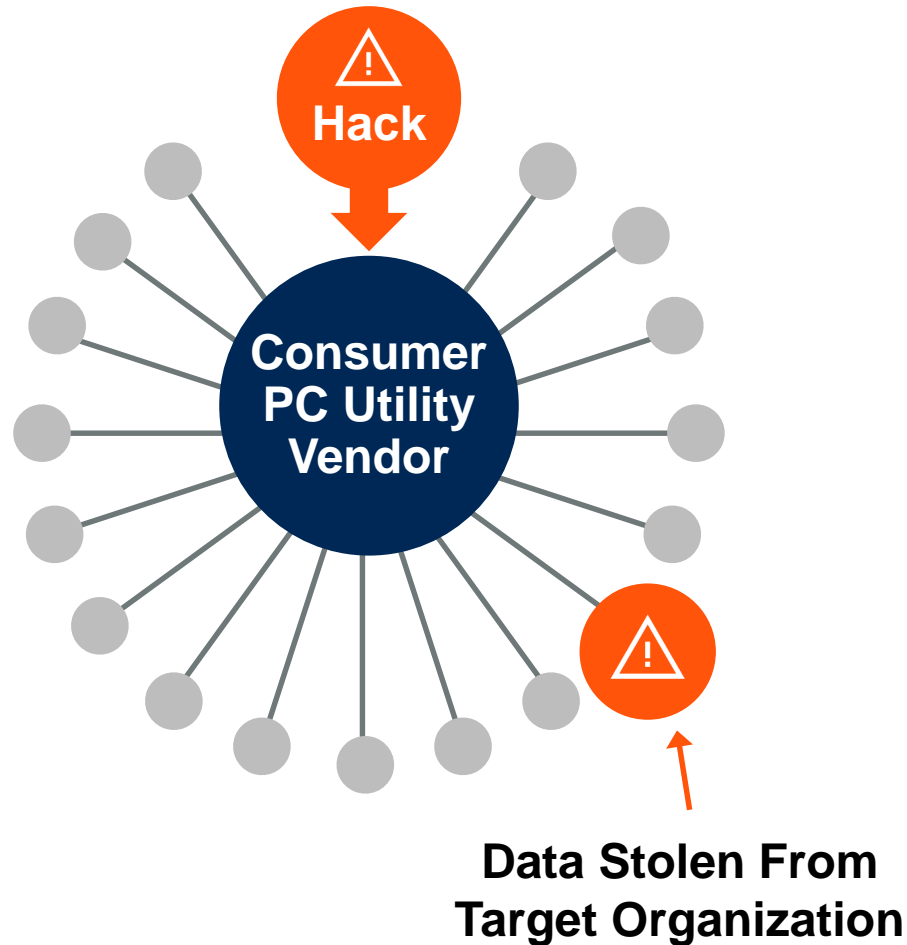


Cloud

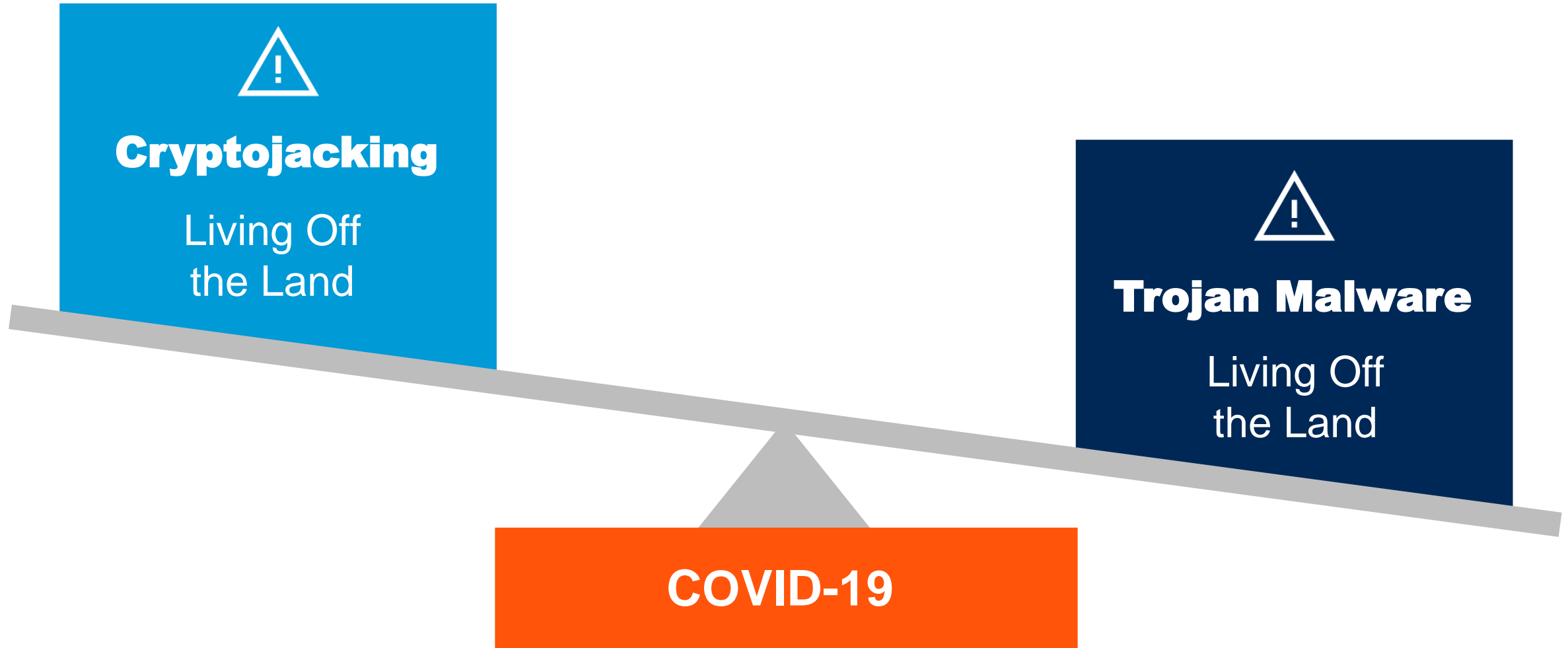


**Nontraditional
Threats**

Hardware/Software Supply Chain Security



Other Threats in 2020



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.

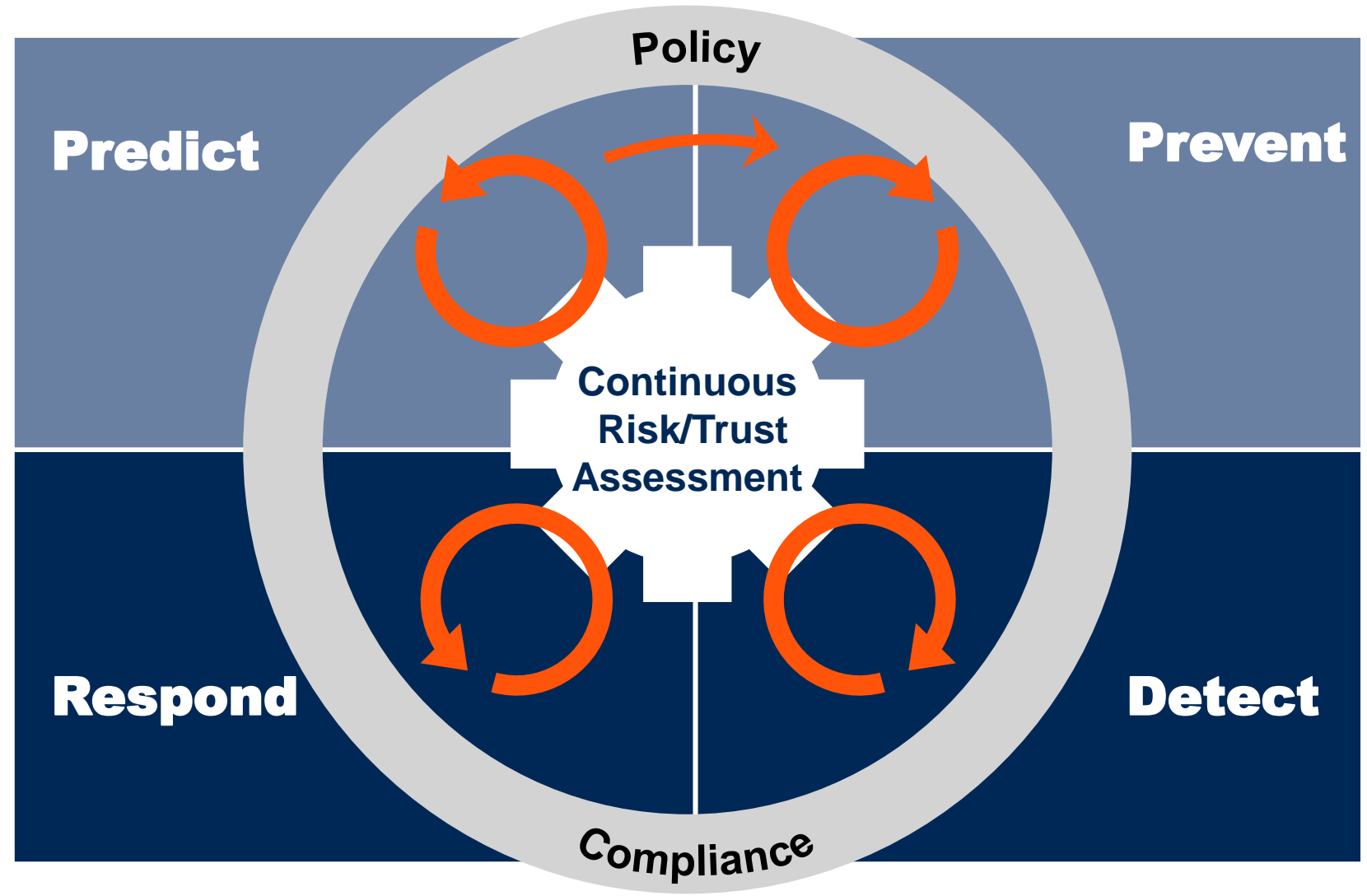


Take action now to retire obsolete technologies.

How to Prepare for Short-Term Threats Today

Gartner®

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

- 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

Prevent

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

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

Detect

CARTA — Ransomware Protection

Predict

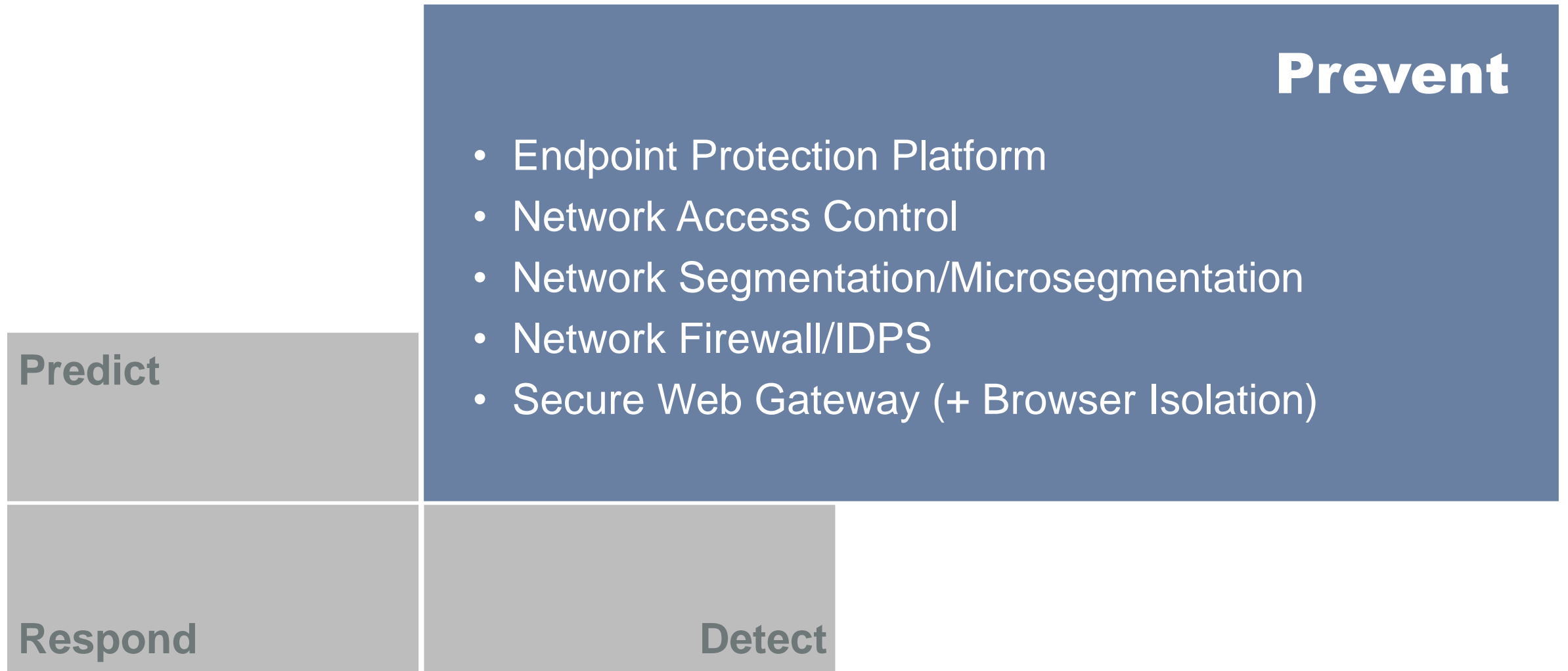
- Risk-Based Vulnerability Management
- Attack Surface Management
- Continuous Automated Attack Platforms
- Threat Modeling Threat Modeling (MITRE ATT&CK, P.A.S.T.A., etc.)
- Supply Chain Risk Assessment

Prevent

Respond

Detect

CARTA — Ransomware Protection



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

- 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

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!

A person is seen from behind, sitting in an orange kayak on a calm body of water. The person is wearing a black life vest and holding a red paddle. The water reflects the light from a bright sky with scattered clouds. In the background, there are dark, rocky cliffs. The overall mood is serene yet powerful, suggesting a journey or challenge.

Threats Evolve We Must Too

Gartner®

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.