How to Respond to the 2020 Threat Landscape

Published 17 June 2020 - ID G00719273 - 20 min read

By Analysts John Watts

Initiatives: Security Operations

Assessing widespread security threat trends, such as ransomware and phishing, requires a continuous adaptive risk and trust assessment strategic approach. Security and risk management leaders must confront the threat landscape based on a continuous assessment of threat and business evolutions.

Overview

Key Challenges

- Organizations must be aware of how the threat landscape and the business landscape shift. In 2020, in particular, there have been swift changes to threats with increased remote work and targeted malware campaigns that take advantage of worldwide events, such as COVID-19.

- Phishing and other human-facing social engineering tactics remain the primary vectors of successful attacks; however, credential stuffing and scan-and-exploit tactics are also increasing.

- Although bigger trends remain similar, microtrends include changes in the threat landscape. More-destructive ransomware tactics; lower risk, but higher-impact phishing using business email compromise and deepfakes; increased supply chain vulnerabilities, including hardware providers; and collateral damage from nation state actions are prevalent.

- Organizations spend disproportionate amounts of resources and money to block a threat that can’t be blocked. For example, nation-state actors and criminal organizations operate with a level of sophistication that surpasses the preventative and detection capabilities of most security and risk management teams.

Recommendations

SRM leaders overseeing security operations must:

- Evaluate the macro trends and the microtrends associated with them to derive a high-level picture of how threats change.

- Use a continuous and adaptive risk and trust assessment strategic mindset to enable prediction and prevention, where feasible, and deploy detect and respond capabilities to adjust to changing threats.
Introduction

Understanding widespread security threat trends helps create security issue awareness, but often is not the best focus for security teams. Security and risk management (SRM) leaders must confront the threat landscape using a continuous and adaptive risk and trust assessment (CARTA) strategic mindset.

External risk is top of mind for many SRM leaders in 2020. In a recent Gartner survey, respondents ranked the evolving threat landscape as the top driver for their information security organization during the next three to five years (see Figure 1). Although risk can be calculated, it is difficult to take a rational view based on cognitive skills and emotions. It is more common to take irrational approaches shaped by our experiences and stories by overreacting to other risks, such as the C-suite, board members, or regulators overestimate, but ignore other risks that deserve our attention.

![Figure 1: The Evolving Threat Landscape](image)

Risks are never static and require a continuous, adaptive approach to be fully prepared. Similar to weather, risk is something we think we know, based on what we see before us; however, context is important. If you are in a tornado-prone area, you are likely to prepare differently than in another location. A tornado may strike quickly, but if you are fully prepared, then you have less overall risk.

---

- Organizations must continuously engage with multiple stakeholders to address unknown attack services, such as line of business owners for cyber-physical systems.

---

Drivers Impacting Information Security Function and Controls in Next 3-5 Years

Summary of Rank (1-3)

<table>
<thead>
<tr>
<th>Category</th>
<th>Rank 1</th>
<th>Rank 2</th>
<th>Rank 3</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT and Cyber Physical Systems</td>
<td>13%</td>
<td>14%</td>
<td>15%</td>
<td>43%</td>
</tr>
<tr>
<td>Increasing Regulations</td>
<td>14%</td>
<td>13%</td>
<td>13%</td>
<td>40%</td>
</tr>
<tr>
<td>Evolving Threat Landscapes</td>
<td>16%</td>
<td>10%</td>
<td>10%</td>
<td>37%</td>
</tr>
<tr>
<td>Business Leader Seeking Information Security as...</td>
<td>8%</td>
<td>12%</td>
<td>10%</td>
<td>30%</td>
</tr>
<tr>
<td>DevOps Driven IaaS Adoption</td>
<td>8%</td>
<td>9%</td>
<td>11%</td>
<td>29%</td>
</tr>
<tr>
<td>Business Initiatives</td>
<td>9%</td>
<td>9%</td>
<td>8%</td>
<td>27%</td>
</tr>
<tr>
<td>Business Driven SaaS Adoption</td>
<td>6%</td>
<td>9%</td>
<td>9%</td>
<td>25%</td>
</tr>
<tr>
<td>Budget Initiatives</td>
<td>9%</td>
<td>7%</td>
<td>8%</td>
<td>25%</td>
</tr>
<tr>
<td>Mobile Workforce</td>
<td>8%</td>
<td>7%</td>
<td>7%</td>
<td>22%</td>
</tr>
<tr>
<td>Staff Shortages</td>
<td>7%</td>
<td>5%</td>
<td>3%</td>
<td>16%</td>
</tr>
</tbody>
</table>

**n = 403, All Respondents, Excluding Don’t Know or Refused**

Source: Gartner 2020 Security & IAM Solution Adoption Trends survey

Q: What are your organization’s top 3 drivers that are likely to impact its information security function and controls in the next 3-5 years?

719273_C
Likewise, a bright sunny day may be more common and seem low-risk, but another threat, such as an earthquake or flash flooding, may be more relevant. For example, a company might see various risks mapped to the likelihood and impact, but those risks can change based on internal and external factors (see Figure 2).

Figure 2: Example of a Fictional Organization’s Risk Landscape

As SRM leaders attempt to assess the threat landscape, they need to acknowledge the cognitive bias that will distort the assessment, leading to a waste of money and suboptimal reduction of risks. Prevention is never 100% possible; therefore, we must take adaptive approaches to managing risks for an organization.

To address the mass of threats in a reasonable way, SRM leaders need to take a drastic approach to threat prioritization.

The most rational approach would be to “engineer” the threat landscape, dissecting its components, analyzing each of them and prioritizing each factor based on the limited known business context. This approach is costly, however, and takes time. It is often not flexible enough to adapt when new business practices arise or sudden events occur that require organizational agility.
to respond. It is also prone to error, because CISOs are forced to make too many assumptions about attackers’ motives or skill sets.

In an imperfect world, there are only incomplete solutions. This research explains how organizations should develop a continuous security posture assessment framework to adapt to today’s threat landscape. The following sections will address three flaws of more traditional approaches:

- Assume well-known threat vectors are covered by defense technologies that are often left in monitoring mode after unintended business disruption, due to false positives or misconfigurations
- Reuse old security approaches to secure new business
- Spend disproportionate amounts of resources and money trying to block a threat that can’t be blocked

Stronger prioritization enables CISOs and teams to better prepare for the threats that are more likely to hit them, but requires good communication skills inside and outside the security teams.

Analysis

Evaluate Macro and Microtrends

Ransomware

Ransomware has evolved beyond the commodity, widespread attacks intended to infect a single endpoint to include more advanced techniques, such as fileless malware and data exfiltration (see Figure 3). Data exfiltration is designed to blackmail companies that may not pay the ransom to negotiate with the malware writers to keep their sensitive data from leaking online. These new strains of ransomware make prevention and planning more important than ever to prevent ransomware attacks. Concurrently, ransomware authors are increasingly selling access to ransomware as service offerings that increase the number of attackers and the variants of malware.

![Figure 3: Advanced Ransomware in 2020](image)
As stated in our Tool Resource, "Defend Against and Respond to Ransomware Attacks," 90% of ransomware can be prevented. What about the other 10%? Follow the guidance in the Tool, such as isolating systems, initiating response plans, and deciding whether you will or won't pay a ransom. Integrating solutions that can automate a response to limit damage through isolation, such as using security orchestration, automation and response (SOAR) or integrated components through an extended detection and response (XDR) platform is key to preparing, defending and responding to these attacks.

**Phishing**

Phishing is still the No. 1 initial access vector for malware attacks; however, several techniques are closing the gap according to IBM Security's X-Force Threat Intelligence Index for 2020. Scan and exploit, as well as credential stuffing, are a close No. 2 and No. 3 (see IBM X-Force Threat Intelligence Index).

Spear fishing, as well as whaling using business email compromise (BEC) are becoming more common and, potentially, more destructive. The FBI reported that BEC accounted for more than $26 billion in losses from 2016 through 2019. In addition, the methods of phishing have expanded well beyond email to include voice, mobile and web channels, such as persistent chat applications.

In 2020, we now have evidence of the successful use of deepfakes to convince someone to wire money to a criminal's bank account. Even in a few short years, the quality of deepfake videos has improved, while the cost to create them is lower. Although spearfishing and BEC do not comprise the volume of traditional phishing, the financial impact of successful attacks is generally much higher (see “Protecting Against Business Email Compromise” for more insights).
Internet-Facing Service Scan and Exploit

Scan-and-exploit techniques take advantage of the move to the cloud and the result of careless configurations of services exposed to the internet. As stated in “How to Make Cloud More Secure Than Your Own Data Center,” cloud security comes down to configuration management. Through a combination of cloud security posture management (CSPM); cloud workload protection platforms (CWPP); SaaS security, via cloud access security brokers (CASBs); and cloud-based security for hosted applications, via web application and API protection (WAAP), organizations can monitor and fix these issues.

Through 2023, at least 99% of cloud security failures will be the customer’s fault. The FBI reports that remote desktop protocol (RDP) is still a widely abused application, because RDP does not use strong authentication schemes.

Virtual private network (VPN) services (see "FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips") are also vulnerable, and must be patched and updated regularly to prevent abuse (see "Vulnerabilities Exploited in VPN Products Used Worldwide"). Organizations that expose vulnerable services must work to reduce these to as few as possible, and pay extra attention to configuration and patching.

API attacks are also on the rise. As a result of this trend, OWASP released an API Security Top 10 in 2019. In “API Security: What You Need to Do to Protect Your APIs,” Gartner’s Strategic Planning Assumption states: “By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the user interface, an increase from 40% in 2019.” API discovery is key to knowing what APIs exist. Once identified, an organization must protect them using tools, such as a cloud-based WAAP product, to prevent abuses.

Account Compromise

A similar threat is credential stuffing. Data from Lastpass showing that on average, employees reuse a password 13 times (see “The 3rd Annual Global Password Security Report”). Therefore, a hacker who can purchase a valid account on the dark web can easily use stolen account credentials to gain access to critical services, such as SaaS applications. A best practice to help prevent credential stuffing is the use of single sign-on (SSO) through a federated identity provider with strong multifactor authentication (MFA) to require at least a second factor of authentication for access to accounts. (See the "Magic Quadrant for Access Management" for more details on the market and market trends for authentication with MFA.)

SIM swapping started as a way criminals could target owners of Bitcoin wallets by calling the mobile phone carrier and requesting a phone number transfer to a different SIM card (see “SIM Swap Fraud: What It Is, Why You Should Care and How to Prevent It”). This technique has expanded to include high-profile corporate targets. The primary means to prevent SIM swapping is to require a PIN to enable the transfer, but given thousands of corporate phone numbers, there is significant overhead in adding this protection to corporate accounts. Therefore, MFA must rely on
other techniques, such as biometrics or application push technologies, and not solely on SMS and a phone number as secondary factors of identification.

Supply Chain Risk

Supply chains are also increasingly vulnerable to attack. Hackers have targeted corporations’ supply chains as a means of access, because they act as “force multipliers” in gaining access to hundreds or thousands of companies with a single compromise. Two recent examples (see Figure 5) highlight this threat:

- Small, commercial PC utility programs
- MSP compromises

By attacking a widely distributed, but otherwise harmless utility program, hackers can gain a foothold in organizations. Often, these utilities are not fully supported or contain security flaws that remain unpatched. Hackers have been able to slip in malicious code that lies dormant until it can detect the presence of a target domain before activating (see “Avast Network Breached as Hackers Target CCleaner Again”). In this case, one way to defend this kind of attack is to have good software asset inventory to limit unsanctioned applications and detective controls, such as endpoint detection and response (EDR) or network detection and response (NDR), to detect when malicious software is trying to connect to download additional malicious payloads.

The second case, an MSP hack, has been observed with several large MSP suffering breaches. Hackers then have access to hundreds or thousands of customers through the MSP networks (see
“At Least 13 Managed Service Providers Were Used to Push Ransomware This Year”). Work with procurement on supplier management to limit risk by vetting vendors who are used to manage IT systems. In addition, limit network access where possible through the use of secure remote access systems such as zero trust network access (ZTNA) or virtual desktop infrastructure (VDI) products that allow access without fully connecting networks between managed service suppliers and the customers they support.

**Cryptojacking and Legacy Technology**

Organizations must pay attention to how threats grow and shrink over time. In 2019 and 2020, the threat landscape saw increasing numbers of successful cryptojacking attempts that can act as a leading indicator of vulnerabilities in the network that lead to more malicious malware vectors. Cryptojacking can drain company resources by taking compute power away for cryptocurrency mining activities and are usually classified as potentially unwanted applications (PUPs). Companies that pay attention to cleaning up these infections and patching vulnerabilities can prevent future, more-malicious infections.

Likewise, with improved continuous patching by web browsers and the upcoming retirement dates of Flash and Silverlight, common web malware vectors are not as commonly exploited using web exploit kits. Organizations that can remove these technologies from their internal applications can improve their overall risk posture, as the public use of these technologies continues to fall. As we see some common threats wane, others grow, as malware writers become more opportunistic in taking advantage of current events and technology trends.

**Apply CARTA to Identified Threats**

As 2020 has proved, risks move over time, because they are not static. Sometimes they move quickly, and, at other times, they move more slowly. Planning for risks that are on the decline may be as harmful as ignoring the risks that are growing for an organization. Organizations waste time on legacy security technologies that have lost efficacy or continue to needlessly tune effective controls. Signature-based antivirus is not effective against fileless attacks and modern evasive malware. However, rather than trying to continuously improve existing endpoint protection platforms (EPPs) to anticipate all possible threats, invest in detection and response. Detection can assist with unknown threats, as well as improve responses when prevention fails. Understanding the dynamic nature of the threat landscape, organizations must buy security solutions that are agile enough to rapidly change with threats.

Use a CARTA strategic mindset to help think about vendor products and how they can work to build up more adaptive defenses by applying the concepts of prediction, prevention, detection and response (see Figure 6).

**Figure 6: Prediction, Prevention, Detection and Response**
Below is a sample of how one organization might apply CARTA concepts to address ransomware in an organization (see Figure 7).

**Figure 7: CARTA and Ransomware**
Not every technology will apply, and each organization might approach ransomware differently. However, adopting a strategic CARTA mindset prepares organizations to replace one-time security gates that can fail and lead to catastrophic results with integrated and adaptive context-aware security systems to respond when prevention fails.

Organizations can apply CARTA to threat vectors such as phishing as well. In this context, CARTA considers people, processes and technology. Phishing requires a balanced approach to all three concerns to actively combat the threat vector it poses (see Figure 8).

**Figure 8: CARTA and Phishing**
Gartner recommends using the CARTA strategic mindset within information security programs. The key outcome of an organization applying CARTA is to improve the cycle of feedback to continuously improve the overall risk profile of an organization through context-aware, integrated and adaptive response systems. (For additional guidance on CARTA, see “Zero Trust Is an Initial Step on the Roadmap to CARTA” and “Seven Imperatives to Adopt a CARTA Strategic Approach.”)

The Impacts of COVID-19

In recent months, Gartner has observed through our client interactions and by reviewing multiple threat intelligence sources several changes to the threat landscape, due to COVID-19. In summary, the volume and sophistication of malware haven't changed, but the primary shift has been in the tactics used by malware actors for initial exploitation. However, this situation is evolving rapidly and will continue to change in the near future, as we move beyond the initial phases of the pandemic. The primary risks that have emerged during this crisis follow.

Risks of Home and Public Networks

Many home and public networks are vulnerable to attack or have compromised devices connected to them, and compromised routers connect them to the internet. This risk existed prior to the crisis, but has grown due to the sheer volume of users that are working from home and the level of data and critical transactions that are now completely outside the protected LAN. To Illustrate the scale of the work-from-home activity, Cisco Webex, saw an increase from 6 billion meeting minutes in January 2020 to 14 billion meeting minutes in March. Internet service providers (ISPs), such as

---

Gartner, Inc. | 719273
Comcast, have recorded abrupt changes in upload usage from home, and Cloudflare recently shared graphics showing the decrease of internet access from dense, commercial hubs and increases in outlying residential areas.

**Increasing Attacks on Remote Services**

As mentioned in the scan-and-exploit section, RDP and VPN are vulnerable services. As many organizations moved to remote work, the number of exposed RDP and VPN services increased in Shodan reports. RDP is unsecure and increasingly a favorite vector for malware writers looking to exploit it for access into an environment, as opposed to phishing. Remote patching of endpoints is a major challenge for many organizations increasing vulnerable services, because these endpoints may not be connected to corporate networks for extended periods of time.

Commercial and enterprise remote meeting services have expanded significantly, with attention placed on security vulnerabilities and poor default security settings. Good meeting practices and hygiene can limit the number of these events, as well as always patching software to the latest version to reduce vulnerabilities.

**BEC and Phishing Tactics Change**

Bad actors are changing BEC and phishing tactics to take advantage of the urgency and chaotic nature of the abrupt changes in working environments. The FBI has warned about BEC in a recent bulletin highlighting that $2.1 billion in losses are attributed to two cloud-based email services alone, which were weakly configured. As companies have moved to remote work, cloud-based services provide more flexibility and performance than traditional VPN connections to on-premises networks. However, they also open organizations to these types of attacks without proper configuration and security. The FBI highlights that these trends are likely to continue.

The United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) highlights a number of COVID-19-themed phishing attacks in its recent alert. These include smishing attacks (SMS phishing), credential theft, malware deployment and the vulnerabilities of exposed services. CISA and the NCSC from the U.K. are also actively publishing IOC lists in STIX and comma-delimited flat file (.csv) formats to combat the threat.

**Fake Websites Distributing Misinformation and Malware**

Starting early in 2020, there were many predictions in the information security industry that malicious actors might take advantage of current events, such as the U.S. election cycle and the Tokyo Olympics, to spread misinformation or malware. This quickly shifted to COVID-19-themed malware campaigns and fake websites. As noted in Krebs on Security, there has been an explosion of malicious domains related to COVID-19 registered since February. The U.S. government has requested as many as eight domain name companies to explain what they are doing to combat this threat.

**Increased APT Attacks on Healthcare and Essential Services**
DHS CISA and the U.K.’s National Cybersecurity Centre (NCSC) has released a joint alert highlighting increased nation state activity from APT groups targeting healthcare and essential services. The actors are looking to obtain bulk personal information, intellectual property, and intelligence that aligns with national priorities. The techniques used are scan and exploit, as well as password spraying to take advantage of unpatched vulnerabilities.

Security Requires an Internal and External Cross-Team Effort

Cyber-Physical Systems

As organizations continue to go through digital transformation and bring on new cyber-physical systems (CPS), the threats to that organization change as well (see Figure 9). In a recent Gartner survey, SRM leaders ranked the Internet of Things (IoT) and CPS as examples of top 3 drivers for information security organizations during the next three to five years.

![Figure 9: The Cyber-Physical Landscape](image)

Recent examples of attacks on CPS show that they are bidirectional, maturing and evolving to become more targeted:

- The Norsk-Hydro ransomware attack started in the cyber world and disrupted smelting operations in the physical world.
- Hackers targeted a casino lobby fish tank thermometer in the physical world to get to a high-roller database in the cyber world.
- GPS systems on ships are being targeted to blur the realities between the cyber and physical worlds.
In some organizations, IT is responsible only for the desktop, laptops and server rooms, while business units take care of CPS, such as industrial controls, operational technology, industrial IoT (IIoT), public cloud and line of business (LOB)-centric SaaS applications. An IT-focused configuration management database (CMDB) only discovers and tracks IT assets, whereas a security team needs a comprehensive asset inventory. Without this view, threats are missed and vulnerable assets are not addressed. This requires a partnership between IT and the LOBs to ensure that an adequate inventory of all assets is available and current.

This risk to CPS is based on the inputs that are open and susceptible to hacking. Novel hacks are starting to appear, such as using drones with signal jammers, social media disinformation campaigns, warshipping attacks and even performance art. In Berlin, Simon Weckert (see Figure 10) used a cart full of cellphones to fool traffic-mapping systems into thinking there was a traffic jam when there wasn’t (see “Facing New Vulnerabilities — Cyber-Physical Systems”).

**Figure 10: Simon Weckert in Berlin**

During the past six months, the U.S. Coast Guard, DHS and FBI have greatly increased warnings on attacks to CPS in a number of critical infrastructure, such as maritime operations, health devices or energy-related environments.

**Nation States**

In addition, organizations need to partner with local authorities to report and respond to threats that may be too large for an organization to handle by itself. Gartner research shows that more than half of CISOs do not work with government agencies (see “How to Prepare for Cyber..."
Warfare"). Nation-state actors are increasingly using tactics that may bleed into the private sector, often affecting organizations inadvertently.

For example, in 2019, a watering-hole attack launched by a nation state targeting a narrow demographic used multiple iOS zero-day flaws for two years (see “Massive iPhone Hack Targets Uyghurs”). Although targeted at certain users, it affected anyone who visited the watering-hole websites. Working with local authorities can help uncover these attacks and provide coordinated response to them.

Many nations are now actively helping organizations and identifying hackers of other nation states in an effort to unmask malicious actors behind common hacker groups. In addition, reporting breaches and malware attacks, such as ransomware, helps paint the picture of the overall threat landscape and provides government authorities the data they need to address problems at a national level.

Evidence

Gartner’s Security and IAM Solution Adoption Trend Survey, 2020: This study was conducted to learn what security solutions organizations benefit from and what factors affect their choice/preference for such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific (APAC) region. Companies from different industries were screened for having annual revenue less than $500 million. Respondents were required to be at the manager or above (excluding C-suite) and should have a primary involvement and responsibility in the risk management role for their organizations.

The study was developed collaboratively by Gartner Analysts and the Primary Research Team, which follows SRM.

Disclaimer: The results of this study do not represent global findings or the market as a whole; rather, they reflect the sentiment of the respondents and companies surveyed.

“Reported Meeting Minutes of Cisco Webex Worldwide in 2020”

“COVID-19 Network Update”

“Remote Work, Regional Lockdowns and Migration of Internet Usage”

“Trends in Internet Exposure”

“IBM X-Force Threat Intelligence Index”

“A Message to Our Users”

“Video Chat Apps Rise to Prominence Amid Pandemic”
“Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing U.S. Businesses More Than $2 Billion”

“Business Email Compromise the $26 Billion Scam”

“FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic”

“A Voice Deepfake Was Used to Scam a CEO Out of $243,000”

“COVID-19 Exploited by Malicious Cyber Actors”

“Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide”

“Sipping From the Coronavirus Domain Firehose”

“Simon Weckert Work About”

“Massive iPhone Hack Targets Uyghurs”

“APT Groups Target Healthcare and Essential Services | CISA”

**Document Revision History**

How to Respond to the 2019 Threat Landscape - 16 August 2019

How to Respond to the 2018 Threat Landscape - 28 November 2017

How to Respond to the 2017 Threat Landscape - 8 December 2016

**Recommended by the Author**

Defend Against and Respond to Ransomware Attacks

How to Make Cloud More Secure Than Your Own Data Center

Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services

Magic Quadrant for Access Management

Market Guide for Operational Technology Security

How to Prepare for Cyber Warfare

Leverage Emotions to Communicate Risk More Effectively

Protecting Against Business Email Compromise Phishing

Data Breach Calculator

How to Develop a Security Vision and Strategy for Cyber-Physical Systems

**Recommended For You**
Best Practices for Privileged Access Management Through the Four Pillars of PAM

Evaluate These Factors in a Global Manufacturing Site Selection Activity

HR Business Partner Career Diagnostic

Toolkit: Assess National and Organizational Attributes in Addition to Costs for Global Manufacturing Site Selection

Supply Chain Brief: Expand Capacity Planning Beyond Manufacturing for Feasible and Optimized Supply Plans

© 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."