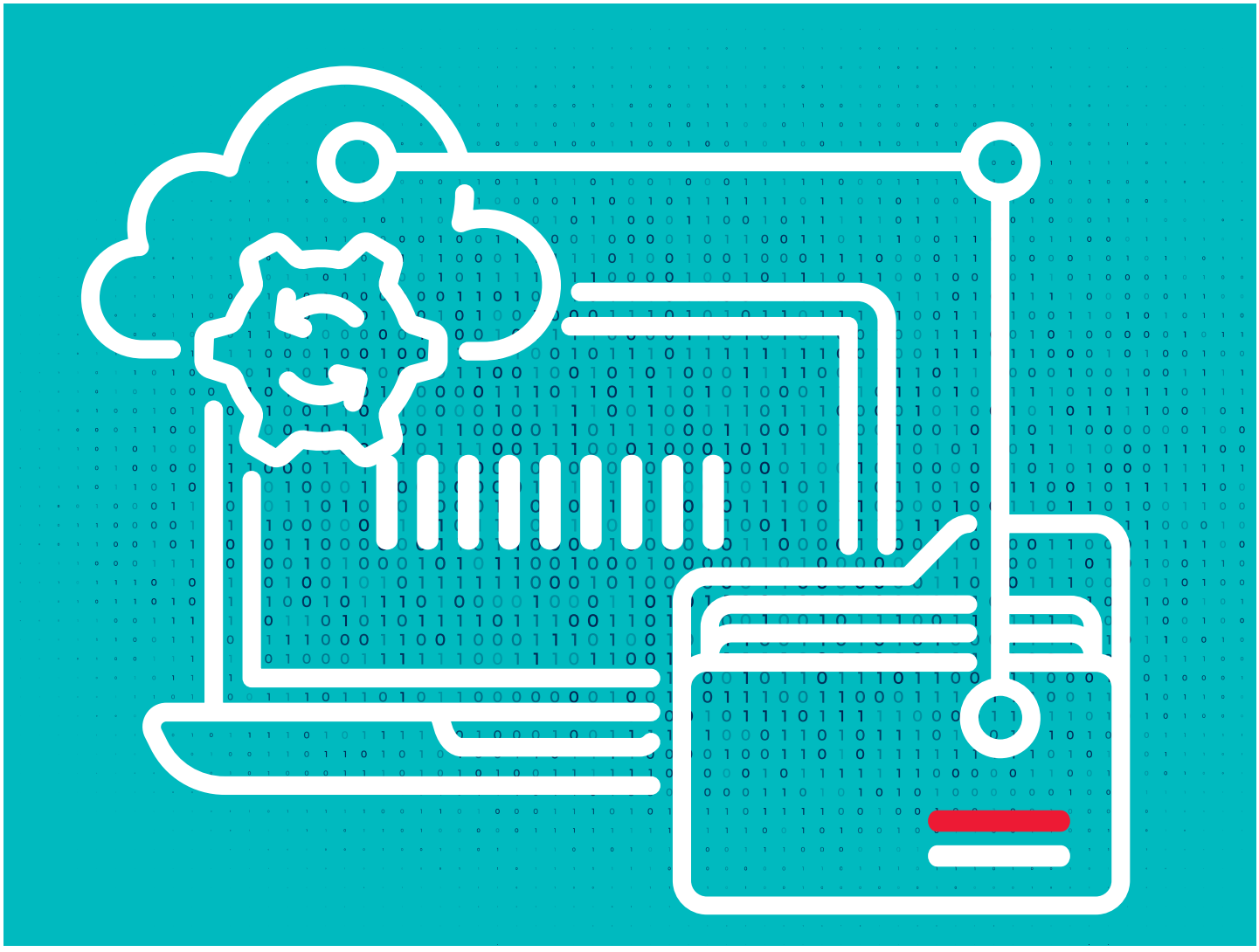
MIT Technology Review
Insights

Produced in association with

HITACHI
Inspire the Next

Organizations face pervasive and sophisticated cyberattacks, but modern data protection techniques can provide a multifaceted defense.

Cyber resilience melds data security and protection



Ransomware attacks – malware intrusions that block an organization's access to its own data until a ransom is paid – are taking on alarming new aspects. As people's work habits, daily routines, geographic locations, and trust in institutions have changed against a backdrop of global political shifts and the covid-19 pandemic, ransomware attacks have taken advantage of the opportunity to grow more sophisticated and pervasive.

Though the basic tools of ransomware remain the same, attackers are using global uncertainty as cover to evolve techniques that make extortion attempts more effective. In a "double extortion" attack, for example, bad actors both block the organization's access to data and threaten to release or sell that data. "Triple extortion" or "quadruple extortion" attacks, which additionally incorporate distributed denial of service (DDoS) attacks or threats to third parties, are now also part of the modern risk landscape, **according to Alexander Applegate of cybersecurity firm ZeroFox**.

Meanwhile, attempted attacks have also grown so prevalent as to be virtually guaranteed. According to a **2022 Sophos survey**, 66% of companies experienced a ransomware attack in the last year, nearly double the 2020 figure. A **2022 report by Enterprise Strategy Group (ESG)** put the figure at 79% of organizations affected in the last year.

ESG practice director and senior analyst Christophe Bertrand inserts this troubling addition: "I question the 21% who say they did not experience an attack, because I think the ransomware virus is probably dormant in their systems."

Key takeaways

1. Attempted ransomware attacks have become extremely prevalent. In addition to exacting ransom, bad actors are using extortion techniques that expose private data, take down networks, and extend the threat to third parties.
2. As bolder ransomware attacks target vital infrastructure, with direct public impacts, simple remedies such as data backups and ransomware insurance are no longer sufficient protection.
3. A strong multifaceted ransomware protection and recovery approach incorporates a zero-trust security framework, organizational readiness, and modern data protection techniques.

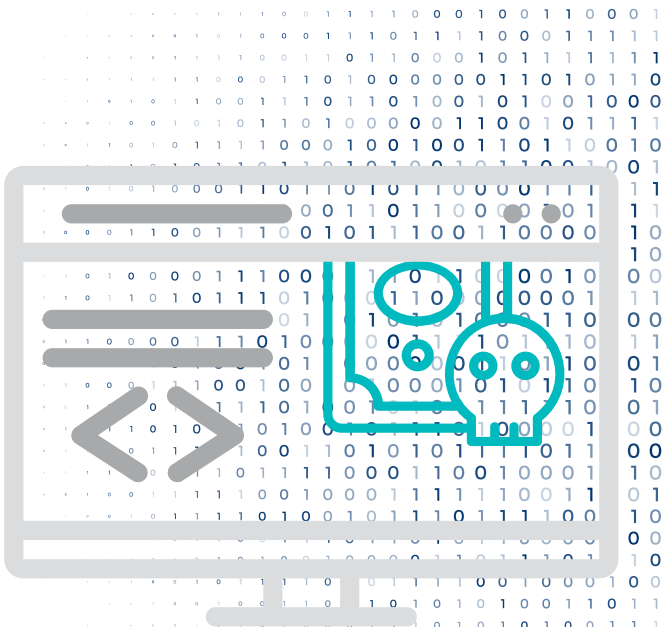
Ransomware attacks have grown more virulent

Ransomware threats have become more damaging in several dimensions: attacks are on the rise, cybercriminals are demanding more ransom, successful intrusions are being leveraged to compromise multiple data streams, and attacks are spreading beyond IT systems into critical infrastructure essential to business functioning.

A **2022 Sophos report** identified a new trend: a franchise business model ("ransomware-as-a-service") in which gangs sell ransomware kits to other cybercriminals,

"When ransomware started, it was a small business picking on users who weren't sophisticated and who would probably pay a couple of hundred dollars to get their data back. Now the game has changed dramatically."

Hu Yoshida, chief technology officer, Hitachi Vantara



who launch the attacks and then return a portion of the proceeds back to the gang. “When ransomware started, it was a small business picking on users who weren’t sophisticated and who would probably pay a couple of hundred dollars to get their data back,” says Hu Yoshida, chief technology officer at Hitachi Vantara. “But now the game has changed dramatically.”

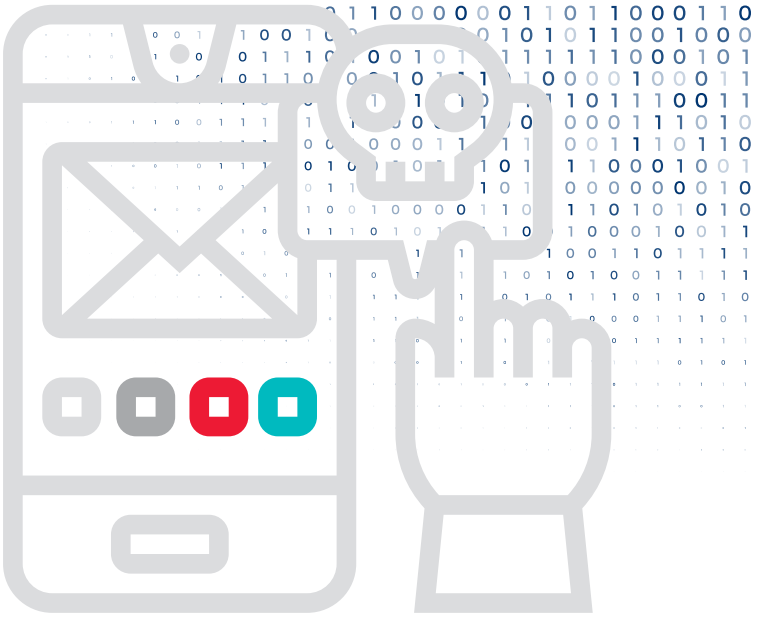
The utility industry has become an enticing target, as disrupting power, water, or critical infrastructure can be detrimental to the public. The 2021 **ransomware attack against Colonial Pipeline**, for example, spurred gas shortages in the northeastern United States. And though Colonial Pipeline paid the $4.4 million ransom, the decryption tool provided by the hackers was so ineffective that the company ended up using its own business continuity systems to slowly get back up and running.

Governments and public services also have become ransomware targets. A **U.S. Senate committee report** noted more than 2300 known ransomware attacks on local governments, schools, and healthcare providers in the U.S. in 2021. In April and May 2022, a series of ransomware attacks crippled dozens of Costa Rican government agencies, including the Ministry of Finance and the social security system, spurring the president to declare a national emergency.

Implications of attacks go far beyond monetary costs

Some organizations might assume that their data backups are sufficient protection from risk, or that paying a ransom is the cost of doing business in today’s cybersecurity climate. Yoshida says, “Sometimes people think, ‘Well, I’ve got a backup, so I’m protected.’ Or ‘I have insurance, so we could just pay and get our data back.’”

But data recovery shouldn’t even be your primary consideration. “Your first thought should be to realize that the bad guys have breached your security systems and are able to do more harm,” says Yoshida. “You need to immediately take your systems off the net and determine what you need to do to prevent any further intrusion.” Once a hacker group has opened a back door into your systems, they can sell that hack to bad actors who want to access your systems for other nefarious purposes, such as using your servers for cryptocurrency mining.



Ransomware myths

Myth: Ransomware attacks start when a user mistakenly clicks on a phishing email.
Fact: Though phishing emails are one route, the top points of entry for ransomware attackers are software vulnerabilities, incorrect user permissions, and device misconfigurations.

Myth: Backing up data to the cloud will protect you from losing data to ransomware attacks.
Fact: If hackers gain access to administrative passwords, they can get to cloud backups. Additionally, new ransomware specifically targets backup servers in an attempt to eliminate that recovery option.

Myth: Ransomware is an external threat launched by foreign hacker groups.
Fact: System insiders may also pose a threat. In a recent Hitachi ID study, 65% of executives and employees admitted to being contacted by hackers seeking to bribe them into helping with insider-based ransomware attacks.

Your data can also take on a life of its own outside of your systems. Even if you retrieve your data from backups, Yoshida adds, "if they have taken your data and they've exfiltrated your data, who knows what happens to the data. Who's going to get it? Or are they going to use it for the next attack, or attack somebody else?" Double extortion creates a second revenue stream by allowing criminals to auction off stolen data on the dark web.

When organizations pay the ransom to recover their data, they often don't get all their data back. In ESG's report, of those respondents who admitted to paying a ransom, 61% were extorted again and paid more the second time, says Bertrand. More importantly, only 14% of respondents fully recovered their data after paying the ransom. "Paying the ransom is not only bad behavior that you're creating," he adds, "but it's also not going to get your data back, and it's untenable." The British jeweler Graff, for example, agreed to a $7.5 million ransom demand following a 2021 attack – and subsequently **pursued legal action against its insurer for declining to cover the loss**.

Bertrand emphasizes that ransomware is not just an IT problem; it's a business problem. "All of this has a business impact that's significant," he says. "It creates downtime. It creates vulnerabilities that could be exploited repeatedly, costing your business or your shareholders more and more money."

Additionally, new consumer-related regulations, such as General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA), will require companies to improve their responses: "Ransomware attacks create reputational issues," Bertrand notes, "but they also create compliance issues."

Companies lack defense training and tools

Though 80% of C-level leaders identify "ransomware preparedness" as a top-five business priority in ESG's research, most companies are unprepared for the multipronged ransomware attacks launched by well-organized hacker groups. Many fail to implement advanced data protection measures that could halt or at least mitigate the damage caused by a ransomware attack.

ESG rated companies on their attack readiness, prevention, response, recovery, and business continuity, assigning them to four preparedness stages. Only 15% of companies were ranked "leaders," while 29% fell into the lowest "novice" category. "If you look at the whole sample, the overall market is essentially at stage two, 'aspiring,' which is not that great," says Bertrand.

Bertrand says that implementing a solid defense is challenging because many complex factors are involved, including basic data hygiene, minimizing data silos, identifying and classifying sensitive data, and having strong data recovery processes.

Ransom payments

46%
ORGANIZATIONS THAT PAID THE RANSOM AFTER AN ATTACK

$812,360
AVERAGE RANSOM PAYMENT

11%
ORGANIZATIONS THAT PAID MORE THAN $1 MILLION

Source: The State of Ransomware 2022 (Sophos)

"Paying the ransom is not only bad behavior that you're creating, but it's also not going to get your data back, and it's untenable."

Christophe Bertrand, senior analyst, ESG

Yoshida adds that lack of funding is an issue, particularly when hardening operational technology systems, which don't typically come under the IT department's security budget. "It's also a question of education," adds Yoshida. Many organizations exhibit a lack of knowledge and understanding of the potential severity of a ransomware attack.

The companies ESG rated as most prepared come from across industries and verticals but show a shared maturity in their approach to ransomware defense. They differentiate themselves because "they have a better understanding of the issue," says Bertrand. "They have put in place better tools to measure and understand the nature of the problem. They have people who are better trained. And they're investing more money in technology, people, and processes to improve their preparedness."

'There is no easy way out of this'

The most successful organizations adopt a multifaceted approach to ransomware protection and recovery. The U.S. National Institute of Standards and Technology provides a **cybersecurity framework** that can guide organizations to identify, protect against, detect, respond to, and recover from attacks. Recommended practices include such techniques as instituting zero-trust architectures, locking up sensitive data with immutability techniques, protecting one copy of their data with air gaps (isolated from an external connection), and using forensics to identify potential attacks.

"There is no easy way out of this," says Yoshida.

The first step in setting up a defensive strategy is understanding the enemy. "Ransomware is not magic," says Yoshida. Attackers find their way into an organization's systems by exploiting a vulnerability, then they gain access to administrative privileges, so they can load their ransomware packages and encrypt data.

Yoshida outlines a three-pronged strategy to combat attackers at each of these points: a zero-trust security framework, organizational readiness, and data protection.

Zero-trust security assumes that traditional perimeter defenses no longer work because the wall that separates "outsiders" from the confines of the corporate office no longer exists when workers are remote and

For effective security, employ zero trust

The covid-19 pandemic accelerated the ongoing transition to remote work, school, and leisure. As millions of people worldwide shift formerly on-site activities to their homes, IT departments face the new challenge of providing their users secure remote access to scores of systems and applications. Because they can no longer count on their users working inside a single highly defended network perimeter, a new approach is necessary.

Users also increasingly require network access on personal devices that their IT departments cannot fully control. These devices may employ lax security precautions and might even be infected with malware.

IT leaders have responded by implementing a zero-trust security framework. Zero trust means that "you don't trust anybody; you assume everybody is going to hack you. When you grant authorization or privilege, it's on a contextual basis based on the work that needs to be done," says Hu Yoshida, chief technology officer at Hitachi Vantara.

In a zero-trust security framework, access to network applications and services requires that users prove their identity, even if they are within a known network or have verified their device previously. Access policies and controls make available only the exact resources required for users' work. Network segmentation can wall off different parts of the network, so, for instance, student access is fully separated from medical center access within a university, while machine learning systems proactively monitor user actions for anomalies that might indicate an insider attack.

data and applications live in the cloud. Because of this, it makes sense to assume that hackers are already inside your network and that attacks may originate from inside the organization.

Yoshida says organizations need to set up privileged access management and identity access management that trusts no one until they can authenticate and verify their identity. The zero-trust system also needs to be dynamic, Yoshida says, to monitor employees' actions and ensure they're not attempting something that might indicate an attack.

Companies can deploy machine learning systems to spot anomalies and alert security professionals to investigate suspicious activity. Infrastructure monitoring applications analyze unusual data storage activities, such as abnormal data exfiltration or data encryption operations. These events could indicate a ransomware attack in progress.

Organizational readiness is also key to any data protection program. Companies should require employee education and training on cybersecurity best practices: not clicking on phishing emails, not sharing passwords, not connecting from unsecure locations, and keeping devices updated and patched. Companies also need to conduct penetration testing on a regular basis, have a strong incident response system in place, and continually test data recovery systems.

Data recovery is rarely complete

Source: The Long Road Ahead to Ransomware Preparedness (ESG Research)

Because data is the target of any ransomware attack, no business or industry is immune. Implementing data protection techniques to secure and monitor your data are a critical preparedness step.

Applying strong data encryption, a best practice for data privacy and for compliance with data-protection regulations, will also boost your ransomware protection. Encryption makes it very difficult for bad actors to attempt double extortion, as any data they steal will be useless to outsiders without the encryption key.

Data immutability techniques prevent data from being altered. If an attacker tries to encrypt data that has been locked in this way, the data remains unchanged and an alert is sent to data administrators. There are both hardware and software methods for implementing data immutability.

Because data is the target of any ransomware attack, no business or industry is immune. Implementing data protection techniques to secure and monitor your data are a critical preparedness step.

> "The overall management system is key, because it sees everything and can identify abnormalities that may be caused by malware actors."
>
> Hu Yoshida, chief technology officer, Hitachi Vantara

Often referred to as (write-once, read-many) WORM storage, an immutable storage system does not allow data to be changed, just for new versions to be created. Storage that pairs WORM with version control also provides a robust recovery option: if malware does create an encrypted version of a file, the old version remains in the system and can be easily retrieved.

Making your backup data inaccessible to outsiders is also important. Old-school tape backups of data can be stored with third-party companies whose business model is built on safely protecting data. This technique of physically isolating a copy of critical data from networks that can be attacked is called air gapping.

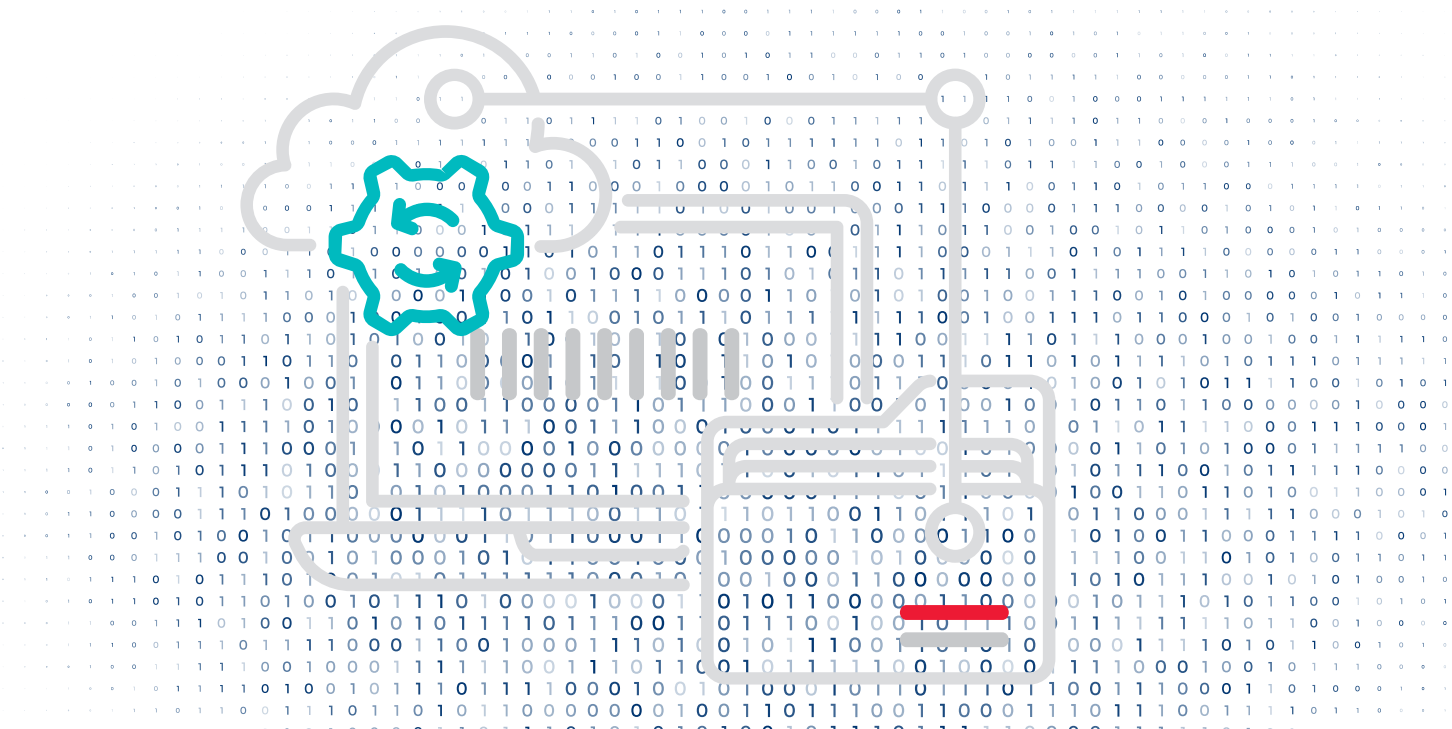
Bertrand also suggests scanning for anomalies in the backups. "From a data protection perspective," he says, "validation of backup integrity is key." Organizations can also use sandboxing techniques to isolate data sets, and then traverse those sets and look for anything abnormal.

The final piece of the puzzle is an overarching data management platform that monitors the entire infrastructure, both in the cloud and on-premises. Associated artificial intelligence can help identify ransomware-associated patterns.

"The overall management system is key, because it sees everything and can identify abnormalities that may be caused by these malware actors," says Yoshida.

Even as ransomware attacks increase, Bertrand is optimistic about the future. He is encouraged to see the most advanced organizations leading change by requiring ransomware protection and recovery best practices down through their supply chains and to the third parties they do business with.

"Every organization works as part of an ecosystem, a supply chain of other companies, and a lot of the requirements, the regulations, and the mandates get rolled down the hill," Bertrand says. "So I expect there will be a virtuous cycle of the leaders starting to apply best practices all the way down the chain, because it's just good business practice."



"Cyber resilience melds data security and protection" is an executive briefing paper by MIT Technology Review Insights. We would like to thank all participants as well as the sponsor, Hitachi Vantara. MIT Technology Review Insights has collected and reported on all findings contained in this paper independently, regardless of participation or sponsorship. Laurel Ruma, Jenn Webb, and Teresa Elsey were the editors of this report, and Nicola Crepaldi was the publisher.

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the U.S. and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Insights Panel, Insights has unparalleled access to senior-level executives, innovators, and entrepreneurs worldwide for surveys and in-depth interviews.

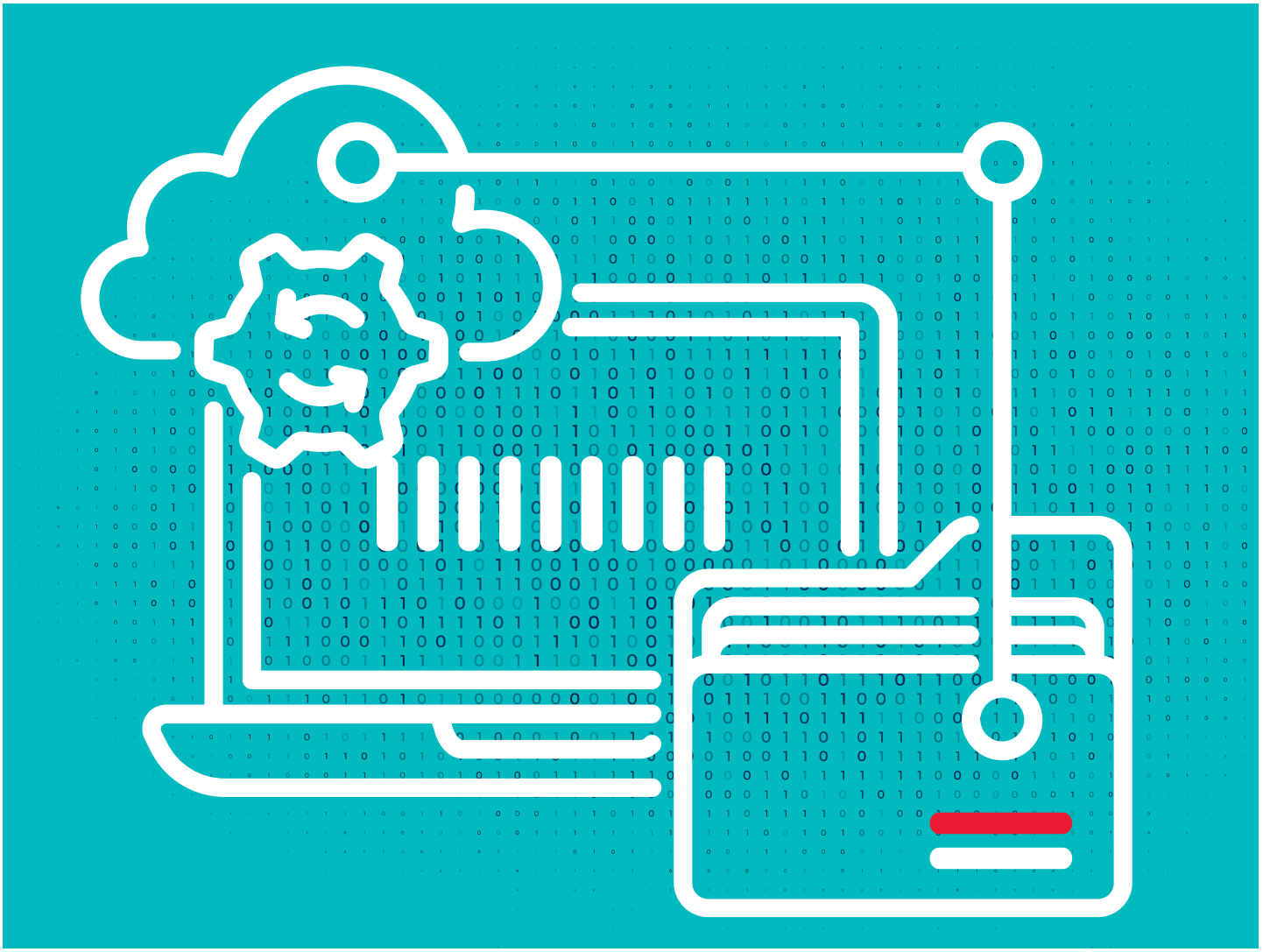
From the sponsor

Hitachi Vantara, a wholly owned subsidiary of Hitachi, Ltd., helps data-driven leaders find and use the value in their data to innovate intelligently and reach outcomes that matter for business and society – what we call a double bottom line. Only Hitachi Vantara combines over 100 years of experience in operational technology (OT) and more than 60 years in IT to unlock the power of data from your business, your people, and your machines. We help enterprises store, enrich, activate, and monetize their data to improve their customers' experiences, develop new revenue streams, and lower their business costs. Over 80% of the Fortune 100 trust Hitachi Vantara for data solutions.

Visit us at **www.hitachivantara.com**.

HITACHI
Inspire the Next

Illustrations
Cover art and spot illustrations created by Chandra Tallman with icons by The Noun Project.



MIT Technology Review Insights

www.technologyreview.com

@techreview @mit_insights

insights@technologyreview.com