Table of Contents

**Resilience** ................................................................. 1
An If-When Statement ................................................. 2
Why Resilience Matters .............................................. 5
Cyber Resilience ......................................................... 10
Cyber Readiness and Cyber Recovery Crossroads .............. 12

**Readiness** ................................................................. 14
Cyber Threat Preparedness .......................................... 16
The Approach ............................................................ 18
Ransomware Readiness .............................................. 20
Cyber Strategy and Roadmapping ................................. 22

**Recovery** ................................................................. 24
Cyber Recovery Solution ............................................. 26
Initiate ......................................................................... 30
Assess .......................................................................... 32
Implement ..................................................................... 36
Support ......................................................................... 38
The Bottom Line ........................................................ 39

Conclusion ................................................................... 40
Notes ............................................................................ 42
Related Assets ............................................................ 43

Category Icons

In an effort to make certain types of information easier to find, the main entries in this field guide are designated with category icons.

**People**
Entries with this icon have information relevant to individuals and may be helpful in professional and personal contexts.

**Processes**
Used with entries that are helpful to small- to mid-size teams.

**Technology**
These entries provide actionable steps that go toward securing the entire organization.
Resilience

Speed is the new business differentiator. To stay competitive, organizations are adopting and accelerating digital transformation initiatives at breakneck speed. But as our digital world grows, so too does the attack surface. To survive and thrive in such a dynamic and fast-changing threat landscape, enterprises must think beyond traditional business continuity and build cybersecurity resilience.
An If-When Statement

Our world is increasingly digital. Two thirds in fact.

IDC estimates that 65% of the global GDP will be digitized in 2022, driving upwards of $7 trillion in digital transformation investment.¹

The COVID-19 pandemic further squeezed companies to fast-track digital transformation initiatives. The efforts to accelerate network interactability, flexibility and productivity, on top of enabling work from home environments, introduced another layer of complexity…and opportunity for bad actors of every ilk.

Today, the odds of dodging a cyberattack indefinitely are not in your favor. What was once considered an alarming albeit slightly vague “what if” is now an imminent reality for every single organization on the planet. The World Economic Forum’s 2021 Global Risks Report even lists cybersecurity failure as one of the top biggest threats to humanity.²

The multi-million-dollar question then becomes, how does your organization approach resilience?

Since an organization’s products and services define its core mission and objectives, approaching these with resilience means assuming their delivery will eventually be interrupted. That’s why a truly resilient approach should ready an enterprise not only for an attack occurs, but also how to recover when such an event inevitably comes to pass.

The Baseline of Business Continuity

This is more than your basic business continuity plan. It’s more than disaster recovery too. Yes, operational resilience supports business continuity – but it’s more than just upgraded business recovery procedures. It’s a shift in mindset, culture and approach that drives the implementation of cybersecurity resilient measures and practices throughout an organization.

To begin, organizations must determine how much of a disruption they can handle before the impacts become intolerable, then develop a plan to mitigate them. This strategy should identify the most critical products and services, then make them – plus the business processes, systems, technology, applications, people, assets, data and locations that support them – more resilient.

Once established, resilient models help vanquish their reactive predecessors. They instead shift an enterprise to a proactive posture that’s poised to bounce back from adversity and overcome threats in their myriad forms.

³ Cybercriminals can penetrate 93% of company networks.
“There are only two types of companies: those that have been hacked and those that will be hacked.”

– Robert Mueller, former director of the FBI

Why Resilience Matters

With threats multiplying and intensifying, the future is bound to make you show your mettle. The best you can do is be prepared to call its bluff.

Now, let’s get down to the brass tacks: why, exactly, do we believe building resilience into your enterprise should be a top security priority?
First, Ransomware...

...is all the rage these days. Our contemporary cybercriminal’s go-to tactic is putting the squeeze on a business – and they’re getting pretty good at it, too. After a successful breach (with ransomware typically delivered via phishing emails, RDP vulnerabilities and software vulnerabilities4), bad actors can encrypt operation-critical data and systems until an arbitrary ransom payment is forked over. More recently, compromised organizations have been strong-armed into paying said ransom twice to prevent their data from being released on the dark web – a risk with its own spate of expensive and/or brand-damaging consequences.

And ransomware practitioners don’t even have to be hackers anymore. The growing Ransomware as-a-Service (RaaS) industry’s user-friendly variants are now hot commodities on the dark web, making this extortionist malware easily accessible to legions of minor league cybercriminals as well. This effectively means that it’s open season on every legitimate organization operating today, a troubling trend reflected by recent statistics.

A ransomware attack happens every 11 seconds or less5

---

7 Coveware, ‘Ransomware payments fall as fewer companies pay data exfiltration extortion demands’, 2021, https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
Tomorrow’s Attack Surface...

...is less predictable than the weather. Any number of intersecting variables, cause-and-effects or black swans can and will alter the digital landscape many times over. Add the rippling effects of climate change, rising geopolitical tensions and the potentially job-disrupting reign of automation, and it’s anyone’s guess what shape the future’s threats will take.

For the forward-thinking organization, however, it’s not the exact forecast that matters. What matters is that organization’s ability to deal with and recover from any threat, in any form, whether it be today’s ransomware or tomorrow’s offspring. This ability will be the determining factor for sustaining operations and staying competitive amid uncertain times.

“By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coincident threats from cybercrime, severe weather events, civil unrest and political instabilities.”

Cyber Resilience

Simply put, cyber resilience is an organization’s ability to withstand cyber threats. Building it effectively, however, requires a thorough understanding of your enterprise’s singular risks. As digitization continually renovates the attack surface, organizations should consider:

✓ How they secure their backups
✓ Updating their processes to recover the systems necessary for keeping operations up and running

This of course comes at a time, post-pandemic, when digital transformation keeps changing the rules at a fast clip, and surfacing a few persistent pain points for today’s average enterprise:

• While most organizations have developed strategies to access their most critical data during disruptions like natural disasters and power outages, it’s less common for these strategies to take cyberattacks into account
• The increasing interconnectivity of users, servers and cloud devices (coupled with continuous web access) has created a complex environment that’s easier for cybercriminals to attack, significantly disrupt operations and/or take an entire network hostage
• Organizations working with real-time data have turned to high-availability solutions. But when these solutions are hit with an attack, organizations risk replicating malware to redundant locations and backup centers

Optiv’s Cyber Resilience service addresses these common challenges by dispatching the ongoing necessary elements to help enhance your protection, detection and response capabilities, in turn driving your ability to rapidly recover if and when you are attacked (more on the rapid recovery piece later).

Combining our Cyber Readiness and Cyber Recovery offerings, this service focuses on shifting enterprises from reactive models to proactive ones, putting them in a better position to handle potential cyberattacks. Our customized strategies and evaluations of current abilities and gaps help you identify and protect mission-critical assets, while simultaneously enabling rapid recovery to a secure state in the event of an attack. And regular testing maintains your resilience in step with the world’s fast-changing threat dynamic.

Implementing a solid cyber resilience framework, which we’ll detail more in the Recovery chapter of this guide, the service can also enhance existing recovery capabilities by determining:

• Where existing recovery solutions are adequate
• Where integrating enhanced security controls (i.e., data-isolated, air-gapped, vaulted solutions) are required
• Visibility to business-critical data for adequate and efficient backup workflows

To recap, Optiv’s end-to-end Cyber Resiliency service reduces risk holistically and programmatically while supporting your organization’s capability to identify, protect, detect, respond and recover in a radically changing threatscape.

Data breaches cost an organization $4.24 million on average.¹⁰

Cyber resilience lies at the nexus of cyber readiness and cyber recovery. The **readiness** factor **prepares and hardens your organization’s defenses**. Should something ever get through, the **recovery** element **gets you back to a secure state of full operation**.

“**Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive.”**

– James Cascio, author and futurist

In the chapters ahead, we’ll take a closer look at both readiness and recovery, including how Optiv’s Cyber Readiness service and Cyber Recovery Solution (CRS) support and augment an enterprise’s overarching resiliency program.
Readiness

To defend from external threats, we must first look within. Readiness refers to your current state of preparation. It’s realizing where you presently stand, setting your target destination, then charting a path to reach it. Ready to begin?
Cyber Threat Preparedness

Cyber readiness, or incident response readiness, addresses how to prepare if an adversary goes to attack an environment.

It asks two main questions:

✓ How do you prepare for, detect and respond to cyberattacks?
✓ How ready are you to combat adversarial activity?

The answers begin with visibility.

Optiv’s Cybersecurity Readiness service deploys a holistic strategy to develop a clear picture of your organization’s current capabilities and security gaps (especially those not spotted by your staff) to understand its cyber threat preparedness. From there, the stage is set to proactively improve its cybersecurity operations.

Our Incident Readiness experts assess your response framework, management structure, tools and technologies. The follow-on, customized recommendations and roadmap describe the actions you can take to improve your incident response readiness and cyber maturity.

Regardless of your current posture, we can apply a formal incident response framework, industry best practices and threat intelligence to your cyber readiness initiatives, helping you build muscle memory and develop your A-game against any ifs.

Here’s how:

1. We start at the kill chain – analyzing what the adversary is doing and what they’re capable of doing within breached environments
2. We layer this with your desired organization framework (typically NIST CSF)
3. We look across people, process and technology to support overall business objectives
The Approach

Optiv’s Cyber Incident Readiness Assessment looks at every cyber domain both quantitatively and qualitatively to help find the gaps and position it to protect, detect and respond to a cyberattack. The process is two-fold: simulate adversary tactics, techniques and procedures (TTPs) in your environment and evaluate your strategies already in place.

Quantitative
Optiv’s threat team simulates an attack by:
• Identifying vulnerable systems
• Escalating privileges
• Moving laterally
• Imitating ransomware detonation

Qualitative
Optiv’s architecture and engineering team assesses your current:
• Incident response plan, playbook and document review
• Automation opportunities
• Asset and security logging posture
• Roles, responsibilities and escalation review

Our Process

Access

Actions on Objectives

Persistence

Persistence

Expanding Presence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persistence

Persiste
Ransomware Readiness

Ransomware is the perennial weapon of choice for today's cybercriminal. If you've had an eye on the news in the past few years, you've probably noticed that ransomware actors are upping the ante on how frequently they attack, the total number of systems they can impact and the amount they demand for ransom. In 2021, ransomware racked up a bill of $20 billion globally, and by 2031, that's expected to rise to $265 billion. As adversaries get craftier and more capable, they're more likely to go straight for a target's throat – aka the most critical data and backups – to increase the chances of a big payout.

Optiv's Ransomware Readiness Assessment is strategically designed to prepare organizations for ransomware threats. Focusing our Cybersecurity Readiness approach, it evaluates your current people and processes while at the same time simulating TTPs to attack your environment just like an adversary would. This approach yields a comprehensive security strategy to prepare you for a ransomware attack, reduce system compromise and integrate backup services that enhance security controls.

Other benefits include:

**Risk Reduction**
Get expert help developing a cybersecurity culture and mitigating insider risks associated with ransomware.

**Faster Response**
Implement a cutting-edge threat intelligence, monitoring, detection and incident response methodology to reduce threat detection time while automatically mobilizing your team to remediate ransomware events.

**Resilience**
Build a proactive and well-documented ransomware business resiliency plan spanning across risk management, business operations and technology capabilities.

**Reputational Protection**
Strengthen reputational smudges with layered safeguards.

**Better ROI**
Significantly reduce the cost of ransomware from impact to remediation. Transform budgets for ransom payments into investments for your organization's future.

The largest known ransomware payout to date was made by an insurance company in 2021. It was $40 million.12

---


Cyber Strategy and Roadmapping

Cyber Awareness Meets Cybersecurity

After understanding where you are on your journey toward cybersecurity maturity and incident readiness, we’ll help you chart a path to reduce your risk.

Optiv’s Cyber Strategy and Roadmap offering helps you establish a holistic cyber strategy program that aligns with your business requirements and risks. Think of it like a map and a compass, not only revealing where you want to go, but also exactly how to get there. On the way we’ll include stakeholders across your organization, help you measure and reduce cyber risks and provide you with actionable recommendations to reach your target state.

“...to find where you are going, you must know where you are.”

– John Steinbeck

Disruption is only a matter of time in our ceaselessly shifting world. There may even come the time, when, gripped by ransomware, your entire environment needs to be turned over. How would you make that happen? Think of recovery as a comprehensive approach to recovering a critical business process. Moreover, it refers to your ability to minimize impact, restore operations and get back to a secure state.
Cyber Recovery Solution

Cyber recovery addresses how to respond and recover when an adversary attacks an environment.

It asks:

✓ How quickly can you recover to a secure state?
✓ How can you lower risk in your environment and ultimately get your network back up and running?

Reducing the Risk of When

Organizations commonly use high-availability solutions to keep their systems and data accessible during an outage. These solutions create snapshots of production environments and quickly replicate them to failover environments for use when the network is impacted.

But because replication often happens in real time, failover systems can be corrupted if the primary systems are attacked by ransomware, which can unintentionally assist cybercriminals in their attacks.

“Many organizations design their backup systems so they can be easily accessed, but that’s a huge mistake,” says IT Director Jon Booth of the Bear Valley Community Healthcare District, who’s witnessed an exponential increase in ransomware attacks on the healthcare industry. “Recovery speed is important, but if achieving that means you make it possible for the backup also to be breached, you have a catastrophe instead of a recovery.”


With complete network architecture overhaul being unfeasible for many, organizations are seeking a thoughtful approach to maintain their existing high-availability environment while simultaneously enhancing the protection and recoverability of their most valued systems and data.

Approaching from a resilient standpoint, Optiv’s Cyber Recovery Solution (CRS) helps identify and protect mission-critical assets that must be shielded from cyberattacks while enabling rapid recovery to a secure state.

More specifically, CRS helps organizations classify the interdependencies between their systems, data, applications, storage, cloud infrastructure, etc., map them, then build out step-by-step playbooks and plans to recover critical business processes. Integrating backup services and enhanced security controls with associated governance and recovery procedures, CRS streamlines visibility to business-critical data for efficient backup workflows.
The CRS Approach

Optiv’s CRS provides the professional experience and technical capability to deliver a truly resilient solution for your crucial systems and data. By developing a proactive cyber resilient framework and integrating backup services that enhance security controls – such as an isolated, air-gapped, vaulted solution – we stand ready to support your recovery capabilities through and through.

The Cyber Recovery Process

1. **Data Categorization**
   - Identify and categorize critical data aligned with business priorities.

2. **Strategy Development**
   - Develop a comprehensive strategy to enhance security controls around critical business processes and technology assets, and transition data backups to a secured solution.

3. **Implementation**
   - Implement a vaulted, data-isolated, air-gapped backup solution that mitigates the risk of data corruption and/or loss.

4. **Maintain and Test**
   - Maintain and test cyber recovery processes and procedures to continuously enhance recovery capabilities.

---

Lost business accounts for **38%** of data breach costs.14

---

Initiate

1. Collect documentation
2. Identify relevant stakeholders
3. Distribute questionnaires
4. Set interview schedules
5. Gather information on security initiatives and events

Outcomes:
- Program kick-off
- Document request list

“A single critical system can support a business operations process that drives between 80 and 95 percent of an organization's annual revenue.”

Optiv cybersecurity strategy team benchmark
Assess

1. Review documentation and responses
2. MAO/RTO validation
3. Evaluate tools
4. Conduct interviews

Outcomes:
- Systems and data recovery visualization
- Assessment findings
- Recovery strategy plan
- Governance document

When everything’s critical, nothing is.

CRS assessments identify the truly mission-essential business processes, visualize and categorize their supporting systems and data, then develop a recovery strategy plan to competently restore operations in the event of an attack.

Using our CBP Discovery Model, Optiv identifies and classifies operating landscapes and reflects business processes by criticality.

**Level 0: Process Classification**

Leverages an underlying tiering system to define the roles of business capabilities and their operations within the organization. Each tier identifies the type of support provided by each critical capability.

**Level 1: Business Capability**

Organizational business capabilities refer to an enterprise’s abilities, that is, what it can and must do to fulfill its core mission. These illuminate the big picture activities needed to generate and drive revenue. Each business capability consists of multiple critical business processes.

**Level 2: Business Process**

Overarching processes within each business capability govern the company’s business operations. These processes also include a risk category to determine if they are mission-critical or operational support.

**Level 3: Critical Assets**

Critical technology assets that allow business processes to operate. These are an enterprise’s primary applications and systems, required to be available to fulfill the enterprise mission.
Recovery Playbooks

Optiv’s CRS develops custom playbooks with step-by-step response plans to enable recovery to a secure state in the event of a cyberattack. These “hands on keyboard” plans are granular and include step-by-step instructions with screenshots to help organizations understand exactly what they need to do to recover.

Primed to evolve, recovery playbooks are designed to identify, document and test resilience processes to ensure system and data accuracy and improve response and recovery continually.

“What are the top-level business processes you have? Let’s recover those.”

– Jessica Hetrick
senior manager,
cyber strategy, Optiv
Air-Gapped Backup

A core component of CRS involves integrating backup services with enhanced security controls, or in other words, storing backups in a data-isolated, air-gapped, vaulted and/or a remote cloud-based solution that safeguards your data’s confidentiality, integrity and availability.

How It Works

1. Critical data, applications, core systems and integrations are categorized and marked for backup in the vault. Optiv builds the technical foundation to make recovery possible and streamlined. The right individuals are identified in the right order to take charge when needed.

2. Critical assets are stored in an immutable worm vault using automated workflows to help stop corrupt data from entering. Data is locked to protect against destruction or deletion.

3. Whether you opt for a cloud solution or a physical solution, your critical data is backed up frequently and securely. After uploading, the connection is severed to create an “air-gap”

4. Golden versions of business-critical data are available for a configurable pre-determined period that aligns with your organization’s BCP and SLAs, as well as any regulatory requirements.

5. In the case a recovery effort is needed, the vaulted data is put into play along with associated governance and procedures, allowing the organization to resume critical businesses operations quickly.

Outcomes:

- Air-gapped backup solution through technology partners
- Immutable data solution via on-prem or cloud

Implement

1. Distribute executive summary
2. Identify gaps
3. Align security initiatives
4. Provide roadmap
Support

1. Carry out testing of developed Cyber Recovery Solution to ensure efficacy

2. Continuous monitoring and maintenance as required

Outcomes:
- Test results
- Updates to recovery plan

As threats evolve fast, established solutions require maintaining and testing cyber recovery processes and procedures continuously to keep up. Optiv’s CRS tests results programmatically to update recovery plans, adjusting these to satisfy the requirements in your environment to help you drive down your recovery risk at that time.

The Bottom Line

We’ve covered all the pieces. Now let’s talk results.

Optiv’s CRS:
- Gives your security team a **solid understanding of business-critical data and processes**, as well as associated systems
- **Mitigates the potential loss of critical data and intellectual property** from business interruptions due to a cyberattack
- **Aligns** your business objectives with technology recovery
- **Reduces the overall risk** of downtime during a significant cyberattack on your organization
- Helps you **become cyber resilient** to anticipate and weather cyberattacks for business continuity
Conclusion

Cybersecurity resilience is more than business continuity. Achieving it across people, processes and technology is an operational imperative to survive and thrive in our ever-changing digital world.

At Optiv, we believe in meeting organizations where they are along their unique journey of security and resilience. Together, let's partner to manage cyber risk so you can secure your full potential.

Encompassing all Optiv’s Cyber Readiness and Cyber Recovery offerings, here’s a high-level recap of our Cyber Resilience service.
Related Assets

Video
C-FAR

Field Guide
Ransomware: Yesterday, Today, Tomorrow

Service Brief
Ransomware Readiness Assessment

Infographic
Cyber Recovery Solution

Explainer Video
Cyber Recovery Solution
Want to learn more?

Visit www.optiv.com/contact-us

Secure greatness™

Optiv is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential. For more information, visit www.optiv.com.

©2022 Optiv Security Inc. All rights reserved. Optiv is a registered trademark of Optiv Parent Inc.

No part of this publication may be reproduced, stored in a retrieval system, stored in a database and/or published in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.