Overall we score your organization as:

Vulnerable

Detect

Respond

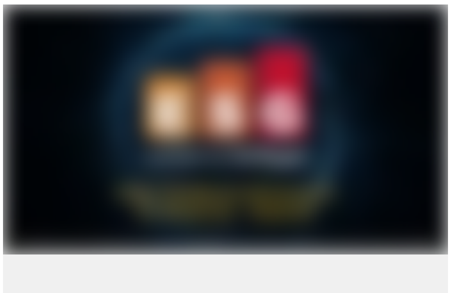
Recover

When it comes to proactively protecting your organization with detection best practices, you are rated as:

Vulnerable

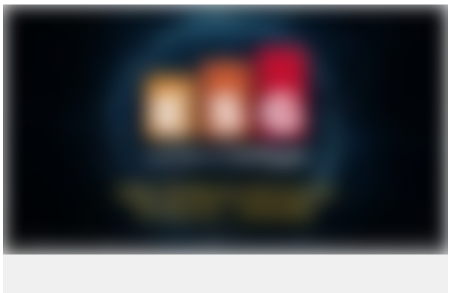
When it comes to responding quickly and effectively to a cyber incident to limit the damage / negative impact you are rated as:

Exposed



When it comes to recovering your data and resuming operations after a cyber incident, you are rated as:

Vulnerable



Your Customized Cyber Resiliency Report

Thanks for taking the Dell Technologies Cyber Resiliency self-assessment powered by ESG. The goal of this assessment is to help you understand how vulnerable your organization is to ransomware and other sophisticated cyber-attacks today, identify areas of vulnerability, and explain what you can do to address these risks. To do so, we evaluate your organization's preparedness in three key areas: proactive threat detection, agile threat response, and completeness of recovery capabilities.

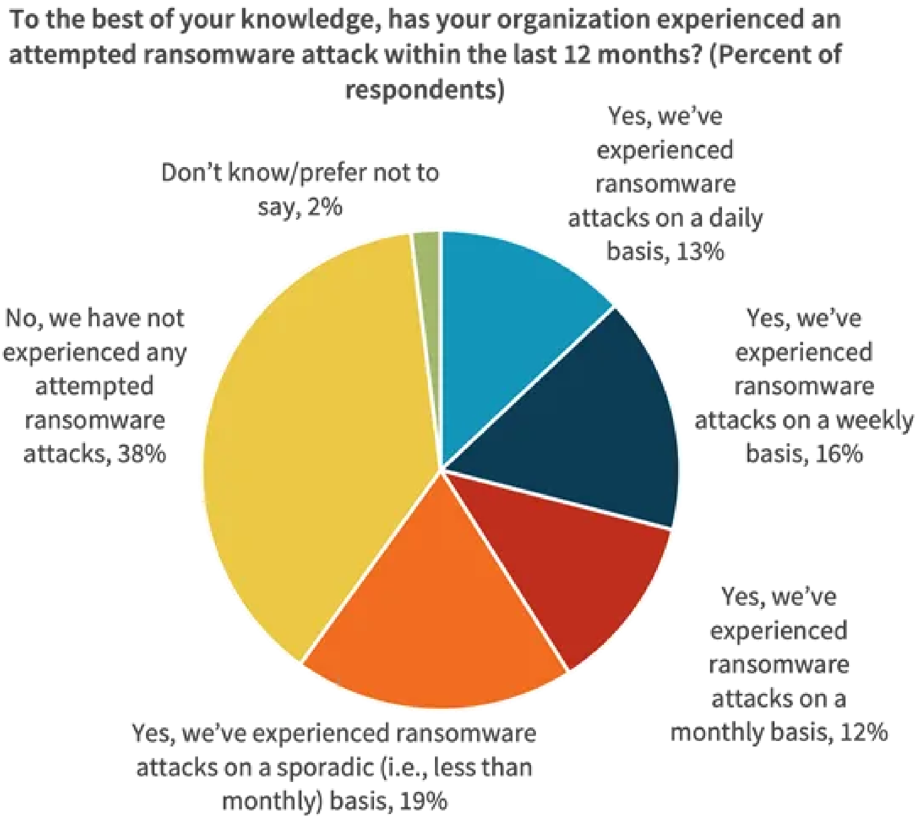
Based on your responses to the assessment across each of these areas, we categorize your organization as **Vulnerable**. This is the **Middle** tier of preparedness in this assessment. The following pages detail why your organization received this rating and include recommendations for your organization to consider.

Detection

The first pillar of the assessment focuses on proactive threat detection—that is, the technologies and processes in place at your organization to detect and prevent a cyber-attack or ransomware-related incident. Considering just this pillar, your organization was rated as **Vulnerable**, the **Middle** tier of preparedness in this assessment.

- **To begin the assessment, we asked about threats your team is focused on. This is important because as ESG's 2020 spending intentions research showed, many organizations are under a constant barrage of ransomware and other forms of sophisticated cyber-attacks (see Figure 1).** As the complexity of the threat landscape continues to increase, attackers commonly leverage multiple attack vectors to compromise and breach organizations. Like other organizations who are prioritizing ransomware; advanced, multi-stage attacks; and insider threats; your focus aligns with some of the hardest hit vectors impacting organizations today. While detection and prevention are critical to defending against these attacks, response and recovery are equally important, including rehearsed, incident response plans and reliable backup strategies.

Figure 1. Frequency with which Organizations Face Ransomware Attacks



Source: Enterprise Strategy Group

- **We also asked you to consider your organization's ability to meet its compliance mandates.** Your organization is making progress but has work to do. Making an organization fully compliant is a challenge shared by many of your peers, and seems like a never-ending effort as new mandates and more data keep coming your way. Here's the good news: you are working on it and taking some steps to get to a more complete level of compliance. Other important areas to look into include your data management practices, your air-gapped or isolated recovery infrastructure (fully secure data copies are must-haves for any compliance effort), the training of your staff, and continued commitment from your leadership. Keep investing in technology to optimize and automate your compliance processes. Not only will it make your organization more operationally efficient, it will also continue to improve your business risk profile.

- **The assessment touched on your organization's use of risk frameworks to guide your security program.** Risk and security frameworks are foundational to successful security programs. In addition to providing a roadmap for your program, these frameworks should enable your organization to benchmark and measure program improvements over time. While highly regulated industries govern through auditing, most less regulated industries are finding real value in frameworks, guiding investments that strengthen overall security posture and risk management.

- **Next, the assessment touched on endpoint, cloud, and network visibility.** As you are well aware, based on your ongoing investment in operational visibility tools, securing your infrastructure begins with a deep understanding of the devices and workloads within it. When visibility gaps exist, adversaries find their way in, putting data and assets at risk. With most organizations reporting some level of visibility gaps, operational backups are more important than ever, protecting against ransomware and other malicious activities. Strengthening asset discovery and inventory processes and infrastructure can help both IT and security teams ensure software and configurations are patched as well as close gaps created by rogue devices and workloads. Investment in advanced detection and response capabilities can help stitch together security telemetry from these assets to uncover more advanced threats.

- **Finally, the assessment focused on the efficacy of controls in place to prevent a ransomware attack specifically.** Preventative security controls are the foundation of modern security programs. While most report a rapidly expanding attack surface and the use of emerging cloud workload capabilities from a variety of providers, ensuring controls are intact and aligned with security policies continues to be a challenge for most. Cybercriminals are exploiting visibility gaps caused by rogue or unpatched devices to facilitate ransomware attacks across many industries. Modern endpoint security controls offer reliable ransomware protection, but only when configured and operating properly. Machine learning and other advanced detection techniques will further help, but only when operating consistently across the attack surface. Reliable data recovery solutions can help close those gaps and mitigate their risks.

Response

The second pillar of the assessment focuses on agile threat response—that is, the technologies and processes in place at your organization to respond to a security or ransomware incident quickly, limiting its impact. Considering just this pillar, your organization was rated as **Exposed**, the **Lowest** tier of preparedness in this assessment.

- **We asked you what your most likely response to a successful ransomware attack would be.** You said you weren't sure. Planning your response to a potential attack is a critical step your organization should be taking right now.

- **Next, we asked you how much time, effort, and budget you have allocated to protecting secondary data copies.** Successful corruption of the backups is an existential business risk in the context of a successful ransomware attack. You should consider continuing your investments in technology to deter cyber attackers who are increasingly and specifically targeting backup sets in addition to production data. That's where you could deploy an "air-gapped" or isolated recovery infrastructure, one that ensures your data is physically and/or logically separated from normal production and backup systems.

- **When it comes to response preparedness,** building and implementing a well thought-out incident response (IR) plan is critical to incident preparedness. While plans are good, running IR exercises can iron out gaps in the plan and can help further prepare the entire team to jump into action. Like other types of security, IR include people, process, and technology, so it is key to have detailed plans and testing for all.

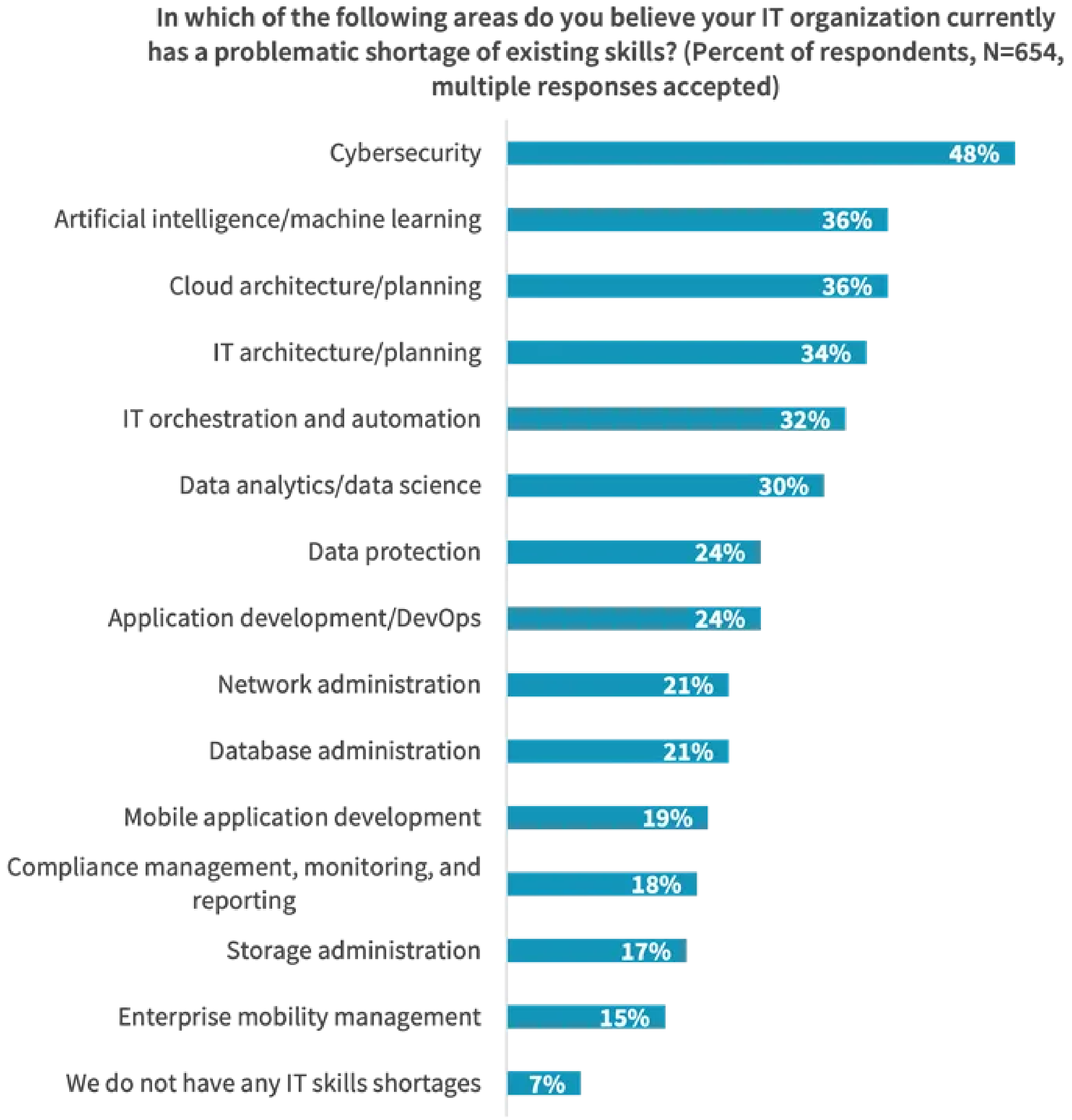
- **Getting to specific preparedness actions, the assessment prioritizes actions like incident planning and recovery testing.** With your recent activities in incident preparedness, your organization will likely fare better than most.

Recovery

The third and final pillar of the assessment focuses on completeness of recovery capabilities. That is, the technologies and processes in place at your organization to recover all your data and enable resumption of normal operations in a timely fashion. Considering just this pillar, your organization was rated as **Vulnerable**, the **Middle** tier of preparedness in this assessment.

- **Having the right people in place to recover from a cyber-attack is critical.** You are not alone in struggling to deploy the right people and skills to combat ransomware and other cyber threats. ESG's 2021 IT spending intentions research shows that cybersecurity is the number one area of technology in which skills sets are lacking (see Figure 2). It's hard to cover all your bases, but cyber-criminals are relentless. Continue to invest in training and skills acquisition, as they will be needed in the next attack. Additionally, looking to increase automation with solutions that leverage machine learning can help offload tasks from over-burdened or under-skilled staff.

Figure 2. Where Organizations Have Skill Gaps Today



Source: Enterprise Strategy Group

- **We asked how much of your data you believe you would be able to recover in the event of an attack.** Your ability to recover all data after a cyber event from a "gold copy" (i.e., a copy with assured integrity, confidentiality, and availability) is critical to enable the resumption of business operations. While your organization still has work to do to get to full recoverability from a disruptive cyber event, you are on your way. From an IT standpoint, placing all your data in an air-gapped infrastructure could help improve your business resumption capabilities.

- **The assessment touches on your organization's investment in isolated or air-gapped infrastructure for copies of critical data.** The most effective way to truly isolate data and backup sets from the risk of destruction or corruption is to leverage an air-gapped solution. While you are early in the process and still at significant risk of data corruption or loss, your interest in investing in "isolated-recovery" infrastructure is a good first step.

- **Finally, regardless of whether your organization has isolated infrastructure, we asked how much of your data you think should be protected in that type of environment.** Protecting mission- or business-critical applications and data is key to success and paves the way for business activities resumption should data be compromised by a cyber-attack. The rule of thumb is simple: if it is business-critical, it has to be protected and recoverable. Based on your answer, you are significantly underestimating the task at hand since best practices suggest that, ideally, 100% of business-critical applications must be protected.

How Dell Technologies Can Help

Dell Technologies strives to build trust and a secure, connected world. We work tirelessly to keep your data, network, organization and customers' safety top-of-mind – with cyber resilience and security engineered end-to-end into all our products, solutions and services. From Dell Endpoint Security solutions and VMware Carbon Black Cloud to Dell Trusted Devices and Dell EMC PowerProtect Cyber Recovery, we help you create and maintain a secure and resilient organization even as new threats emerge.

Based upon your assessment and current score we have made prioritized recommendations to help improve your resilience. Our Security and Trust Center provides easy access to additional resources and solutions to help you quickly find answers to your consumer and enterprise security questions.

From the edge, to the core, to the cloud—our industry experts offer strategic guidance and proven practical capabilities to help you protect your business and preserve your reputation from cyber threats – Trust Dell Technologies.

How Dell can help you improve your detection capabilities:

- Endpoint Security & Devices: The number of end users who are working remotely and on-the go has increased exponentially. With breaches now happening both above and below the OS, you need intelligent solutions that prevent, detect and respond to threats wherever they occur.

- VMware Carbon Black™ Cloud: Cybercriminals constantly update tactics and obscure their actions within common tools and processes. You need an endpoint platform that helps you spot the minor fluctuations that hide malicious attacks and adapt prevention in response.
- PowerEdge Proactive Resilience: Embed trust into your digital transformation with an infrastructure designed for secure interactions and the capability to predict potential threats.

How Dell can help you improve your ability to respond:

- Managed Detection and Response: Managed Detection and Response powered by Secureworks® Taegis™ XDR leverages advanced analytics and expertise to investigate potential compromise and provide remediation if a threat is identified.
- Business Resiliency Services: Dell Technologies Services enables organizations to be highly resilient as their business relies more heavily on cloud-based IT services, alongside increasing pressure from stakeholders and regulators.
- Cyber Recovery Services: Dell Technologies Services enables organizations to increase their cyber resilience through a holistic cyber recovery program which brings together technology, process and people to form a last line of defense for your organization.

How Dell can help you recover from an attack:

- PowerProtect Cyber Recovery: PowerProtect Cyber Recovery protects and isolates critical data from ransomware and other sophisticated threat so you can recover known good data and resume normal business operations with confidence.
- Business Resiliency Services: Dell Technologies Services enables organizations to be highly resilient as their business relies more heavily on cloud-based IT services, alongside increasing pressure from stakeholders and regulators.
- PowerScale with Superna Eyeglass Ransomware Defender: Superna Eyeglass® Ransomware Defender is a highly scalable, real-time event processing solution that employs user behavior analytics to detect and halt a ransomware attack.

ESG, a division of TechTarget, is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.