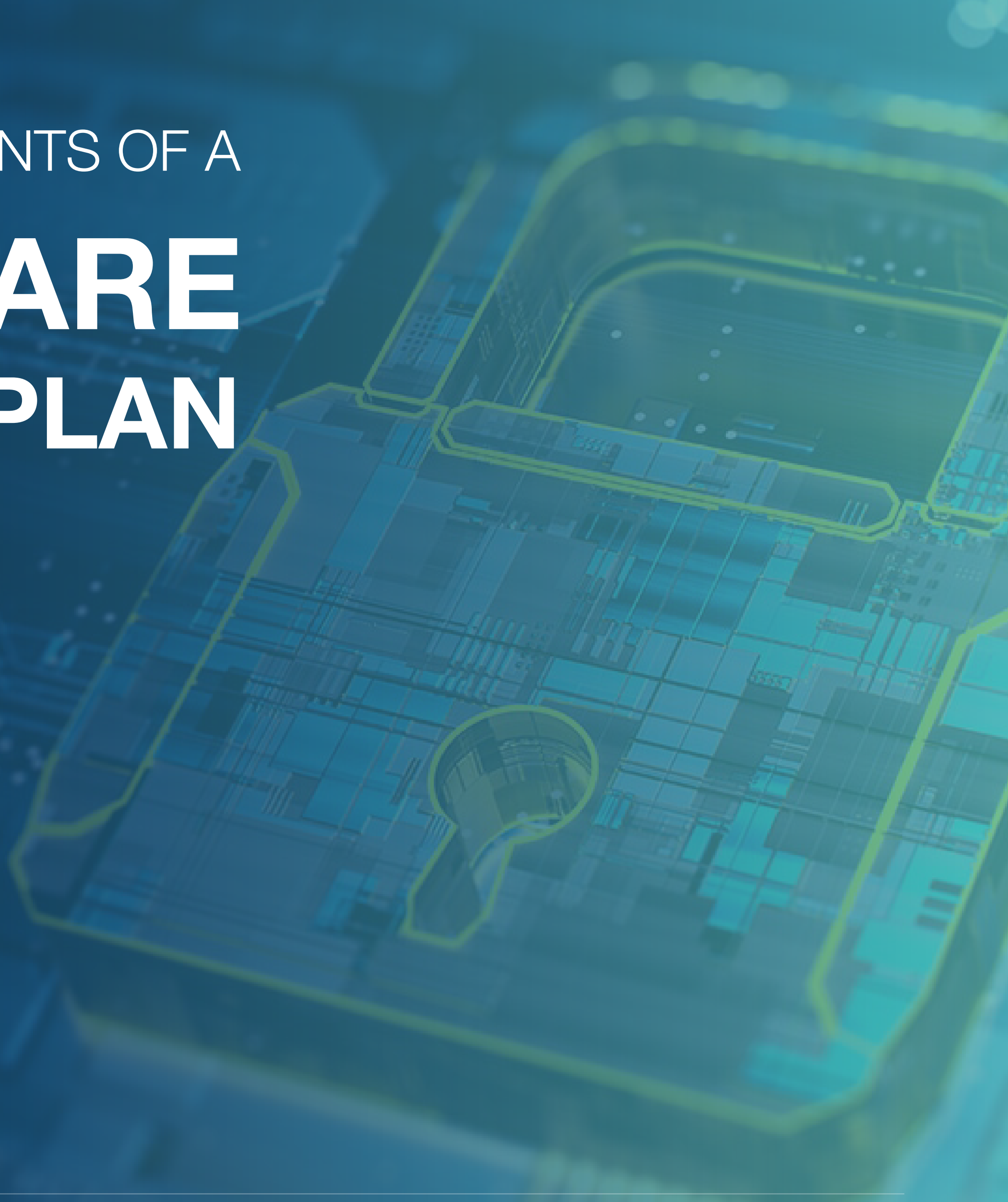
5 ESSENTIAL COMPONENTS OF A RANSOMWARE PROTECTION PLAN

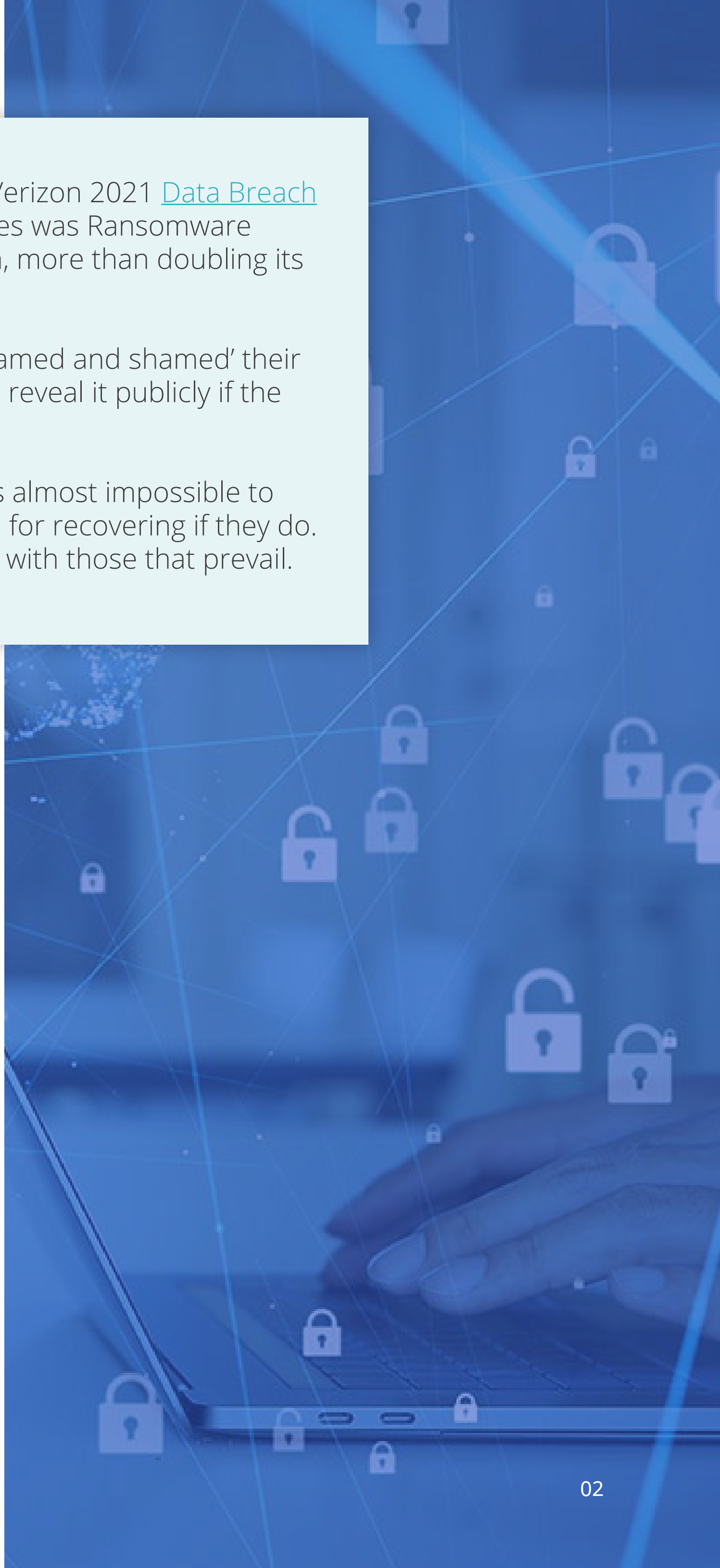


Infrascale™

Ransomware attacks continue to be a threat to organizations of all types and sizes. The Verizon 2021 Data Breach Investigations Report (DBIR) states, "The major change this year with regard to action types was Ransomware coming out like a champ and grabbing third place in breaches (appearing in 10% of them, more than doubling its frequency from last year)."

The report authors propose this could be due to, "the shift in tactics of the actors who 'named and shamed' their victims. These actors will first exfiltrate the data they encrypt so that they can threaten to reveal it publicly if the victim does not pay the ransom."

Ransomware has indeed been a "champ" in that it often defeats and surpasses rivals. It is almost impossible to stop every infection. The best plan is to prevent attacks from succeeding and have a plan for recovering if they do. In this brief guide, we'll cover the top tips for preventing ransomware attacks, and coping with those that prevail.



Organizations of All Sizes and Types Are Being Targeted

Often, SMBs believe their small size provides a level of protection, since larger enterprises with larger budgets are more attractive targets. But 43% of cyberattacks are aimed at small businesses. Attacks are rarely publicized since many SMBs aren't subject to the same reporting regulations as larger enterprises.

Organizations of all kinds have suffered ransomware attacks, including Baltimore County Public Schools and the Athens Independent School District, which paid a ransom of $50,000 to recover its data in addition to delaying first day of school.

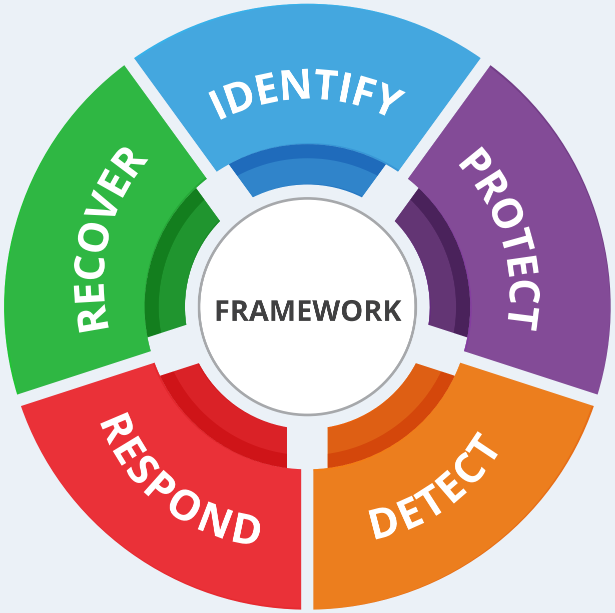
According to the McAfee Threats Report: June 2021, *"Victims are paying the ransoms, and criminals are introducing more Ransomware-as-a-Service (RaaS) schemes as a result."*

Data of All Kinds is Being Targeted

While it's important to protect payment data, it's not the only data attacks are targeting. The Verizon 2021 DBIR states, "Attackers are less likely to purely target payment data and are more likely to broadly target any data that will impact the victim organization's operations. This will increase the likelihood that the organization will pay up in a Ransomware incident."

5 ESSENTIAL COMPONENTS OF A RANSOMWARE PROTECTION PLAN

Plans for preventing and responding to ransomware attacks can be broken into five core components, which align with cybersecurity best practices, specifically, the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) Cybersecurity Framework.



01 IDENTIFY

Start with a thorough understanding of the scope of your assets, systems, data, people, and capabilities. Risk tolerance varies for different organizations, so you must consider the risks to your organization, and the specific impacts of different systems being rendered inoperable. Consider any needs to comply with regulations such as PCI DSS.

NIST CSF states, “Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.”

Determine your approach through an analysis, weighed against the desired risk tolerance of your business. Building from the foundation of this assessment, you can prioritize the investment of funds and time to establish the security posture that’s ideal for your organization.

02 PROTECT

Create technical and administrative safeguards to prevent a potential cybersecurity incident which can impact the delivery of critical services and business processes.

Create Safeguards

Safeguards must incorporate all the ways your business operates, and be appropriately sized, based on your assessment and risk tolerance, as defined in step one.

A crucial cybersecurity tenet, least privilege means giving people only the permissions they need to get their job done. Role-based access controls restrict system access to authorized users, and further restricts what each user can access. Not only users, but systems should also have least privilege, for example, an AWS Lambda function that reads a database should have no privileges beyond reading. Least privilege inhibits the ability for attackers to spread laterally throughout your infrastructure to hunt for sensitive data and spread infections.

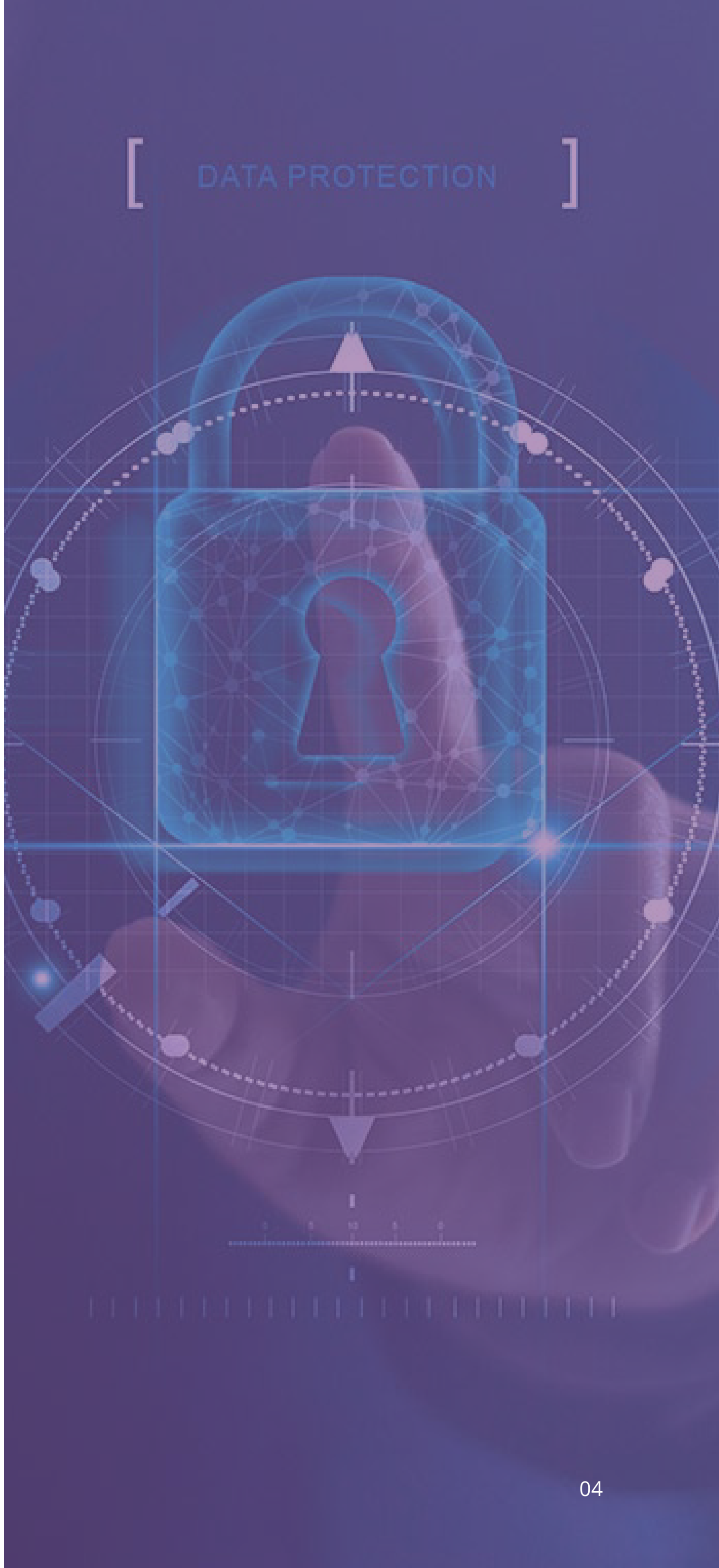
Other vital protection measures include:

- ✓ Processes for reviewing vendors
- ✓ Utilize multi-factor authentication, among the FBI's best practices to minimize ransomware risks
- ✓ Ensure your security solutions are up to date
- ✓ Antivirus (AV) software

Minimize Risks with Controlled Access

Stiving for a Zero Trust methodology improves risk posture, further reducing the risk of ransomware. Gartner's "Guide to Network Security Concepts," states, "Zero trust architecture (ZTA) is a true paradigm shift in network security, but don't try to go out and buy it. As a product, it does not exist, even though many vendors market their products as 'zero trust."

While Zero Trust can mean different things to different people, it's a security framework focused on securing applications and data, rather than securing only the network.



02 PROTECT (cont.)

Secure Common Ransomware Entry Points

Endpoints, specifically employee endpoints, are compromised more easily and are common ransomware attack vectors. This makes endpoint protection one of the most important components of ransomware prevention. The McAfee Threats Report: June 2021 states, "When it comes to the actual ransomware binary, we strongly advise updating and upgrading your endpoint protection, as well as enabling options like tamper protection and rollback."

Keep your operating system and application software updated and patched. This might sound obvious, but endpoints (like a laptop or desktop computer) are not as sophisticated as servers when running. End-user computers typically run many applications from different vendors. IT policy management tools can help administrators and end-users manage patches and enforce policy around software application versioning.

Be Prepared by Backing Up Your Data

Since "un-hackable" doesn't exist, every organization needs a comprehensive backup and disaster recovery solution. Just like platforms and software applications, disaster recovery is available "as a service." DRaaS is a service model that provides backup and recovery via the use of a third-party cloud environment, whereby all of the disaster recovery functionality, including orchestration, are provided as-a-service. Be sure your recovery plan also includes backup for the data in your SaaS applications, endpoints, and servers.

Prepare and Ensure You're Prepared by Conducting Drills

Don't just implement backups but test them regularly. Conduct drills to battle-test your organization's risk management and incident response.

Educate Employees

Employees must fully understand the threats posed by attacks such as phishing. According to the McAfee Threats Report: June 2021, "Spear Phishing (Link and Attachment) moved back to the top 5 used Techniques." Training helps users determine which emails not to open, and how to identify malicious senders and suspicious attachments, reducing their risk of falling prey.

03 DETECT AND CONTINUALLY IMPROVE

Implement the appropriate actions to identify abnormal or malicious activity in your environment. Detection enables timely discovery of cybersecurity events and includes security continuous monitoring.

Monitor Constantly

The ability to detect attacks, both attempts and successful breaches, is vital to preventing business disruptions and mitigating risks. Continuous, integrated monitoring capabilities are needed.

Anomaly detection can provide early warnings, enabling companies to quickly isolate a ransomware infection, revert to a clean backup, and recover important data before the entire network freezes.

Endpoint Detection and Response (EDR)

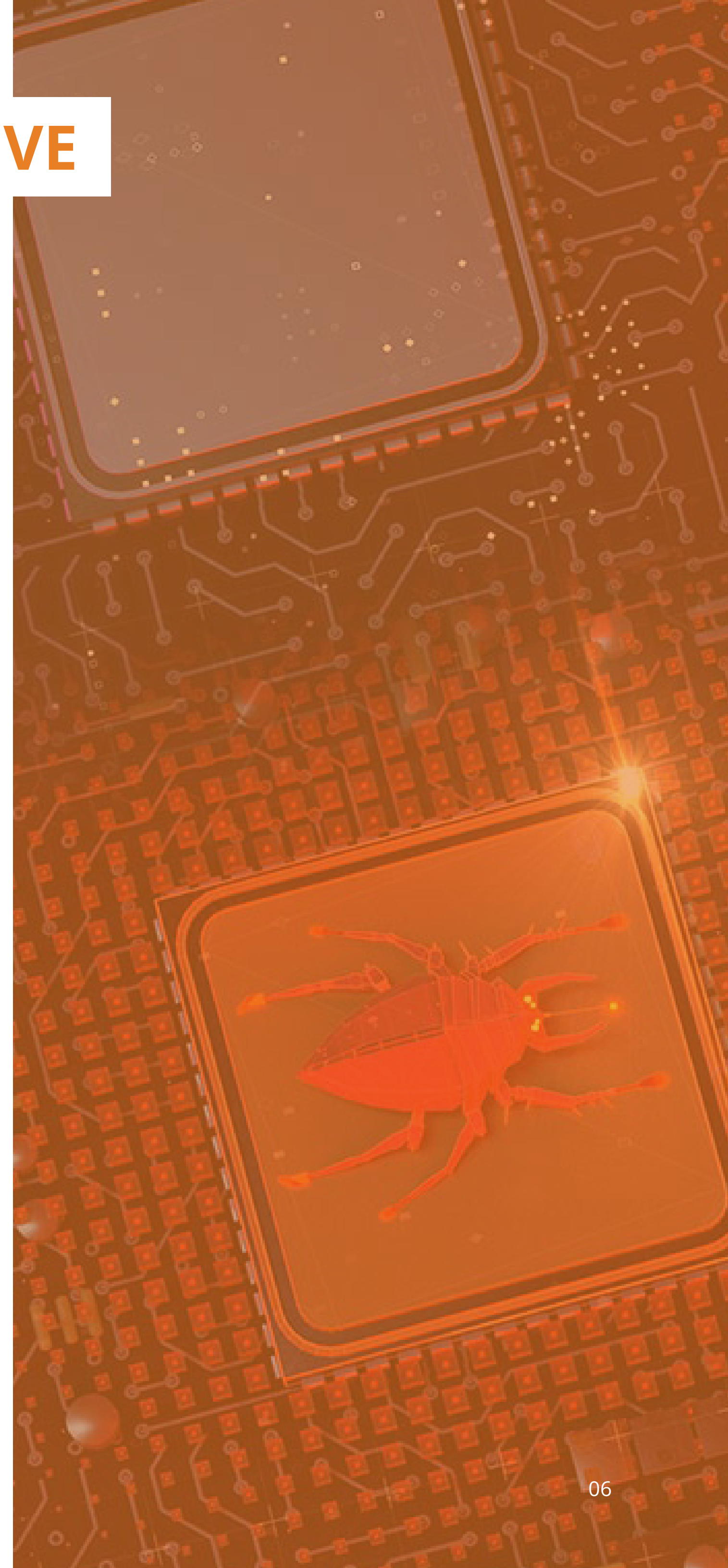
As bad actors continually adapt their attack techniques, they can be successful in circumventing AV software. This is where Endpoint Detection and Response (EDR) can help by looking for bad behavior and alerting the end-user or administrator.

Earlier warning of infection increases response time to stop the spread of the infection – and better yet – illuminate the exact timestamp of infection so that the exact recovery point is known.

Continually Improve

Info security programs must be continually amended and updated. The NIST CSF framework is displayed in a wheel, visualizing this concept of constant improvement and adaptation.

Incorporate continual improvement plans to address gaps in your visibility and protections. Evaluate all of your alarms and monitors and confirm your responses and processes are optimized. For example, if you're seeing numerous alarms for spam or malware, revisit step two and implement new security tools or alter your existing tools to improve your protections in light of these threats.



04 RESPOND

Develop and practice an incident response program within your organization that can be activated to help contain the impact of security events, including ransomware. You need not only visibility, but processes for responding, in addition to practicing your established processes.

Determine When the Infection Started

Before you can restore your clean files from backup, you need to know how far back to go to ensure a clean restore. The timeline for discovering breaches continues to shrink, and with ransomware, attackers notify victims of the attack. (A necessary step in order to demand ransom.) Many recent ransomware attacks have featured a countdown timer, badgering victims to pay before time runs out. Still, so you can't rely on being informed promptly and could have been infected for weeks prior to receiving the ransomware message. Attackers aren't known for their reliability, and they may deliberately wait for the infection to spread.

Minimize the Damage

Systems such as Endpoint Detection and Response (EDR) must immediately generate warning notifications to enable administrative action in real-time.

Identify, isolate, and remove the infected computer(s). Disconnect from the network immediately, so ransomware cannot spread to shared drives and connected systems.

Inform employees

Ensure that all employees are aware that a ransomware attack is in process and direct them to the processes and procedures needed to protect their data. Provide a timeframe for restoration of affected systems.

05 RECOVER

Build a cyber resilience program, including a back-up and restoration strategy to restore core functionality and avoid the expense of hours of downtime. This must include protecting not just data stored on-premises, but in various cloud and SaaS providers. Your data should always be protected and always available... on your time. To fully recover from disaster requires the ability to backup mobile devices, laptops, or remote offices.

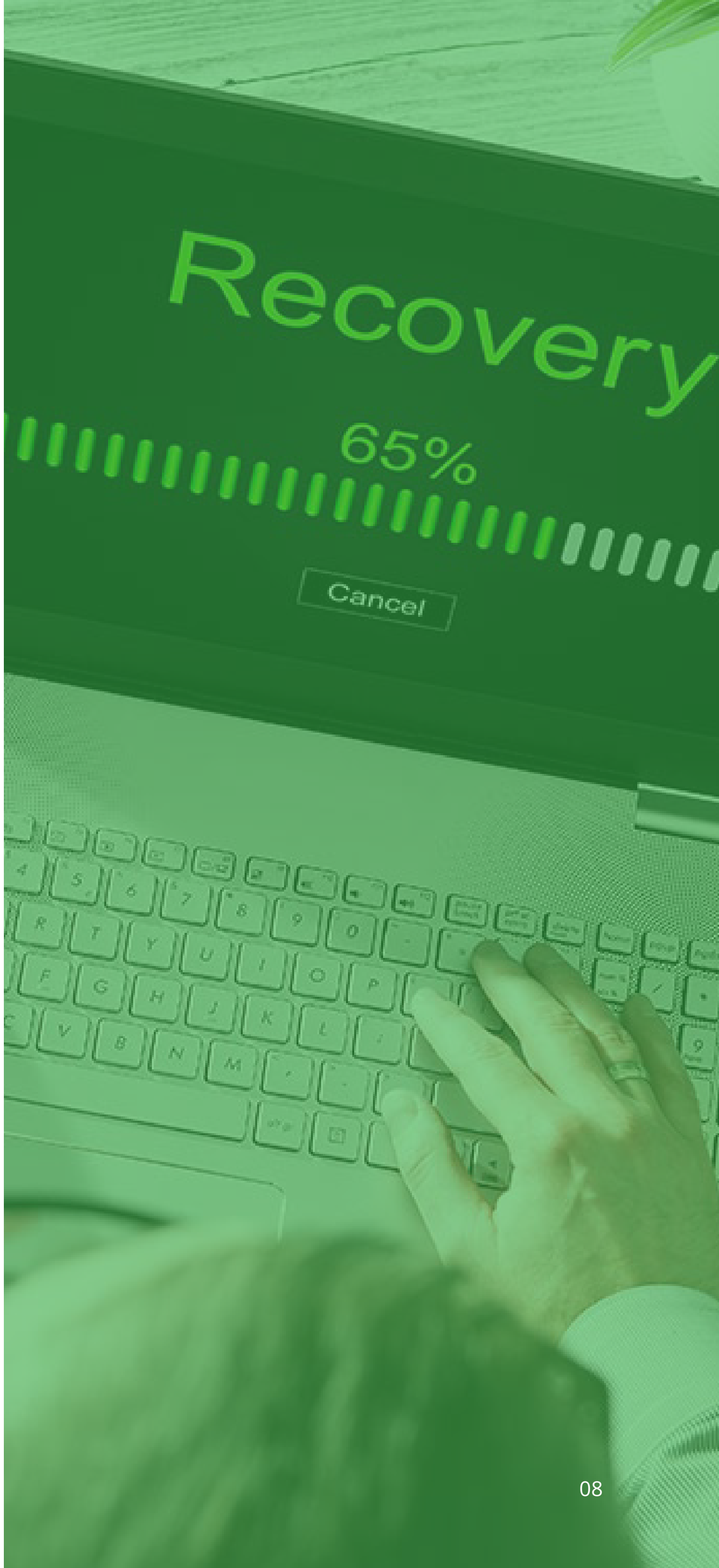
With a backup and DR plan in place, you won't need to pay the ransom to access your data and continue operations.

Restore the Data

Look for solutions such as Infrascale Cloud Backup (ICB) that are easy to deploy, install, and manage directly from one unified console. The Infrascale Dashboard is designed with efficiency in mind, with simple single-pane-of-glass management of SaaS backups. IBDR also provides the option to lease the BDR hardware with no upfront CapEx, or purchase the equipment if desired.

Prevent Reinfection

Businesses often pay the ransom and get the decrypt key but find themselves faced with re-encryption and a new ransom demand a month later. Victims must ensure complete removal of the ransomware to avoid a continuous infection cycle.



CONCLUSION

As hard as IT pros are working to thwart attackers, attackers are dedicating efforts to circumventing their protections. Additionally, many attackers succeed simply due to human error rather than their own sophistication. Protecting against ransomware involves both establishing a secure posture to increase resistance to attacks, while also expecting those defenses to fail and being prepared with backup and disaster recovery.

Ransomware Protection with Infrascale Cloud Backup (ICB)

Infrascale Cloud Backup (ICB) is a direct-to-cloud endpoint backup solution that protects business devices including laptops and desktops – as well as servers including Microsoft Exchange and SQL databases – all in one solution. ICB offers unlimited data retention and version history for an unlimited number of endpoint devices, captures real-time changes via Live Protect, and safeguards against ransomware threats with advanced anomaly detection.

About Infrascale

Founded in 2011, Infrascale provides comprehensive, cloud-based data protection by delivering industry-leading backup and disaster recovery solutions. Combining intelligent software with the power of the cloud, Infrascale removes the barriers and complexity of secure, offsite data storage and standby infrastructure for real-time disaster recovery. Trusted and recommended by leading independent industry experts, Infrascale equips its customers with the confidence to handle the unexpected by providing greater availability, better security, and less downtime when it comes to their data.