Four Technologies Combine To Protect You From Ransomware Attacks

by Naveen Chhabra

October 18, 2019

Why Read This Report

As the ones responsible for recovering from outages, infrastructure and operations (I&O) pros have successfully managed recoveries from all failures but one: ransomware. Ransomware attacks do not result in the familiar type of outage; they often put the backup infrastructure itself under siege. It's not about just recovering from a backup; I&O pros need to work closely with their security and risk (S&R) peers to ensure that they are recovering from an uninfected copy. Together, they can deploy four technologies to improve resilience against ransomware.

Key Takeaways

Lack Of Visibility Adds To I&O's Woes

I&O pros have tools and technologies to quickly recover from any backup instance, but they have no way to identify the most recent backup copy that also remains uninfected.

Add Four Technologies To Your Arsenal To Boost Confidence And Recoverability

I&O pros must use proactive strategies and combine four technologies: write once, read many (WORM) storage; data resiliency solutions; immutable file systems; and multifactor authentication. These technologies are not new; I&O pros use them to meet a variety of business requirements. Employ these technologies to improve your confidence and recoverability after ransomware attacks.

Four Technologies Combine To Protect You From Ransomware Attacks

by Naveen Chhabra
with Glenn O'Donnell, Amanda Lipson, and Bill Nagel
October 18, 2019

Ransomware Attack: A Reality Check Requiring Proactive Prevention

Ransomware continues to paralyze public and private enterprises globally.[1] The World Economic Forum includes cyberattacks in the top 10 global risks in terms of the likelihood of occurrence and impact, but firms are often caught unprepared.[2] After an attack, business leaders look to the I&O team to recover data using backup or archive copies.[3] Law enforcement discourages firms from paying ransoms, instead recommending that they invest in prevention and improved recoverability.[4] Backups are essential but not enough; ransomware does collateral damage by besieging your last line of defense — the backup infrastructure — along with production systems. Since they first appeared three decades ago, ransomware attacks have become:

- **More targeted to deliver maximum returns — for the crooks.** Cybercriminals are increasingly turning away from indiscriminate campaigns and toward targeted ransomware attacks. Recent examples show that attackers are going beyond easy targets; in the past year, attacks on city councils and state governments have grown significantly.[5] Attackers exploit commonly unaddressed vulnerabilities to enter a victim's environment. The driving force behind this change in approach is the return on investment: A successful attack on a specific company or vulnerability can be much more lucrative than a generalized one.
- **Significantly more potent, frequent, sophisticated, and intense.** In the past few years, organizations have witnessed a significant increase in the number of ransomware attacks. Attackers use sophisticated technologies and get more precise with every attack, with much harsher consequences for the victims. One medical practice in Michigan decided to shut its business after being attacked.[6]

FORRESTER®

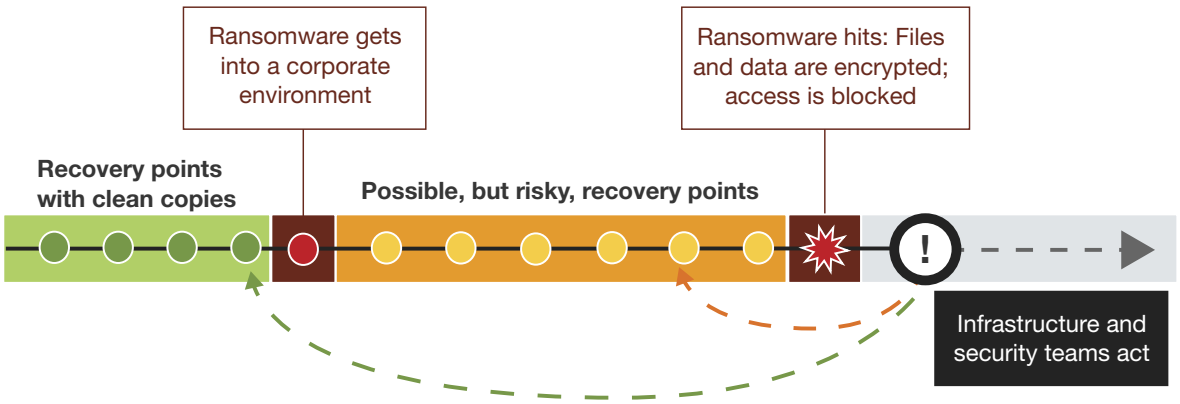
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Recovery Visibility And Confidence Are Challenges

Enterprises are on a digital transformation journey. Digital transformation integrates applications that aim to serve customers 24x7 more tightly by stitching together business processes. But tighter integration can make applications more vulnerable, as any unaddressed vulnerability can become a firm's Achilles' heel and disrupt service. Ransomware attacks cause outages that are quite different in terms of recovery plans, data and infrastructure availability, cross-team collaboration, and the risk of not recovering data. Critically, IT leaders lack a way to measure recoverability independently, hindering visibility into the state of recovery and undermining confidence in recoverability.[7] Time and again, business losses from outages show that IT leaders need to invest more in resiliency, as the losses from an attack far outstrip the spending required to improve resiliency.[8]

- **Ransomware creeps into IT environments and sticks around.** Malware enters corporate IT infrastructure in subtle ways. Once in, attackers want to maximize its impact by infecting as many systems as possible. To do that, malware infiltrates the environment slowly, living in stealth mode so it stays off the radar. Ransomware tends to lay dormant in an environment for weeks or months, usually invisible to security teams (see Figure 1).[9] The infrastructure security team at Bayer reportedly identified malware in its IT environment more than a year ago; the malware didn't activate, and Bayer continuously monitored its movements.[10] But few organizations can successfully detect ransomware infection and movement, adding to I&O pros' woes: The lack of visibility into when and how the environment got infected limits their ability to successfully recover uninfected.
- **IT leaders must take a deterministic, not probabilistic, approach.** Backup infrastructure is the last and best line of defense against ransomware attacks. Malware's dormant nature makes it almost certain that backup copies of infected systems are also infected. Recovering to an infected copy will just give ransomware control of systems again. I&O pros will usually use an arduous trial-and-error approach, recovering each preceding backup copy and testing it for infections and other vulnerabilities. The process continues until they find the last clean backup copy. This probabilistic approach is impractical; I&O teams don't have endless time and hardware to plod through many attempts. To support recovery efforts, S&R teams must trace ransomware infections. I&O and S&R teams need to collaboratively identify the latest uninfected backup instance using a deterministic approach. While business stakeholders like this approach, as it handles recovery operations effectively, very few firms have established a collaborative partnership between their I&O and S&R teams.[11]

FIGURE 1 Anatomy Of A Ransomware Attack



Four Technologies Will Boost Visibility And Confidence

Firms must change their strategic thinking to face increasing cyberthreats. They can pay the ransom, lose business data and transactions as I&O pros struggle to recover from recovery points that may not be recent, or invest in strengthening security and recovery capabilities. Firms that decide to pay the ransom must consider whether the perpetrators will restore all of the data. They may come after you again; cybercriminals are very likely to attack paying victims again, and you have no assurance that they won't leave malware behind.[12] Firms that decide to recover from older recovery points may lose significant amounts of business transactions — data loss that presents significant financial and legal liability. The decision to invest in effective protection depends on your firms' current security posture and risk appetite. I&O pros have few options for detection of, protection from, and quick, confident recovery from ransomware attacks.

Use Known Technologies To Boost Detection, Remediation, Protection, And Recovery

An ounce of prevention is worth a pound of cure. Every level of every organization's infrastructure has vulnerabilities.[13] Despite the vast array of security tools and human skills available, firms have proven ineffective at identifying ransomware. Firms should add infrastructure capabilities — platform, hardware, or software — to improve their odds of malware detection, protection, and recovery. Firms must enable collaboration between the I&O and S&R teams so they can act together during crises. To strengthen their capabilities, I&O pros can include the following technologies:

- **WORM storage ensures that data can't be corrupted.** I&O pros have long used WORM storage for to make data archives secure and unalterable. WORM storage puts a retention lock on data; data can be written to it only once and cannot be modified thereafter. A new write operation writes new data to unused storage blocks. WORM storage meets regulatory compliance requirements like SEC

Rule 17a-4, HIPAA, and PCI DSS.[14] On-premises storage vendors like IBM and NetApp and public cloud storage providers like Amazon Web Services, Google Cloud, and Microsoft Azure offer this class of storage. Putting backup copies of business-critical apps on WORM storage saves it from fraudulent changes, ensuring that you can be confident of recovering uninfected copies of data.

- **An immutable file system works hand in hand with WORM storage.** Implementing an immutable file system with underlying WORM storage will make the system watertight from a ransomware protection perspective. But you can't implement it for all business application data, as your need for storage capacity will grow uncontrollably. Depending on the application and your data risk profile, save backup data with specific retention requirements on an immutable file system at a defined frequency and then save incremental backups on traditional storage. A meticulous design using immutable systems will boost data resiliency.
- **Data resiliency tools with anomaly detection trigger proactive notifications.** Modern data resiliency tools can examine backup copies to recognize possible ransomware actions and infections.[15] Typical ransomware attacks include actions like encrypting or deleting data files, altering file extensions, or modifying files in ways that are inconsistent with a user's or application's normal activity. Without proactive analysis by data resiliency tools, these actions will go undetected. These tools can monitor backup data for such activity and alert the IT or security operations staff. The downside is that these tools can also raise false alarms — but false alarms are better than no detection capability.
- **Multifactor or multiperson authentication ensures that rogue actions are blocked.** Multifactor authentication is an effective, proactive way to address identity and access management issues, strengthen security, and ensure data consistency, reliability, and availability. I&O pros can introduce multifactor and multiperson authentication to ensure that backups are not compromised and to strengthen the control of critical tasks governing protected data. Even with stolen admin privileges, attackers will not be able to delete backups.

Recommendations

Develop A Tight I&O And S&R Partnership To Combat Ransomware

Protecting the firm from ransomware is a joint responsibility of I&O and S&R pros — but working in silos has not strengthened enterprises' ability to deal with these attacks. Cross-team collaboration is one of the strongest imperatives to effectively and efficiently handle outages caused by ransomware attacks. Some of the recommended technologies, like WORM storage and an immutable file system, fall squarely within I&O's domain; others, like multifactor authentication, are more in the S&R remit. However, there's an increasing need for these two domains to collaboratively solve problems by:

- **Identifying how to work together to fortify security.** I&O pros know the data resiliency domain very well. It's time to identify opportunities to collaborate with S&R and leverage the expertise of both to fortify security. Consider this: I&O pros can deploy WORM storage but need S&R's expertise to establish multifactor authentication controls. Without multifactor authentication, WORM storage can still be accessed by rogue elements.
- **Developing a common recovery plan for ransomware attacks.** Recovering from ransomware-induced outages is a joint responsibility that combines perspectives: Identifying a clean, uninfected backup copy; defining a recovery infrastructure, process, and plan; evaluating the security of recovering instances; and ensuring that there are no remaining or new vulnerabilities after recovery. The I&O and S&R teams must agree on a recovery plan that both teams can follow.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Cohesity
Commvault
Rubrik
Spinbackup

Endnotes

[1] The first ransomware attack was identified in 1989; for decades, the number of known ransomware attacks did not grow much. However, starting in 2016, these attacks have become much more prevalent and each attack has increased in its intensity, frequency, and impact.

Source: "Ransomware," KnowBe4 (https://www.knowbe4.com/ransomware).

[2] Source: "The Global Risks Report 2019: 14th Edition," World Economic Forum, January 2019 (http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf).

While respondents that mentioned they are confident of recovery during ransomware attacks, their team organization, people, and processes don't add up to that confidence. Incidents in the industry also conclude otherwise. See the Forrester report "Ransomware Is A Business Continuity Issue."

[3] Norsk Hydro lost all of the IT systems that support plant operations to a ransomware attack. Executive management declared that it would not pay ransom but depend on its backup systems to recover. Source: Eduard Kovacs, "Norsk Hydro Restoring Systems, But Not Paying Ransom," Security Week, March 20, 2019 (https://www.securityweek.com/norsk-hydro-restoring-systems-not-paying-ransom).

[4] The US Federal Bureau of Investigation discourages organizations under ransomware attack from paying the ransom. Source: Josephine Wolff, "They Stole Your Files, You Don't Have to Pay the Ransom," The New York Times, August 14, 2019 (https://www.nytimes.com/2019/08/14/opinion/ransomware.html).

[5] Source: Kara Frederick, "The Rise of Municipal Ransomware," City Journal, September 3, 2019 (https://www.city-journal.org/ransomware-attacks-against-cities).

[6] Source: Marianne Kolbasuk McGee, "Medical Practice to Close in Wake of Ransomware Attack," Bank Info Security, April 2, 2019 (https://www.bankinfosecurity.com/medical-practice-to-close-in-wake-ransomware-attack-a-12321).

[7] See the Forrester report "The State Of Business Technology Resiliency, Q2 2017."

[8] Major airlines have lost millions of dollars to outages.

Source: Naveen Chhabra, "Lessons Learned From The Recent British Airways Outage," Forrester Blogs, June 15, 2017 (https://go.forrester.com/blogs/17-06-15-lessons_learned_from_the_recent_british_airways_outage/).

Source: Leslie Josephs, "Delta: Atlanta power outage cost it up to $50 million," CNBC, January 3, 2018 (https://www.cnbc.com/2018/01/03/delta-atlanta-power-outage-cost-it-up-to-50-million.html).

[9] Bayer detected infectious software in its IT infrastructure and tracked its movement, actions, and interests before clearing it from its systems. While Bayer managed to detect its ransomware, not all organizations have that maturity and capability. Source: Phil Taylor, "Bayer hit by extensive, year-long cyber-attack," Securing Industry, April 5, 2019 (https://www.securingindustry.com/pharmaceuticals/bayer-hit-by-extensive-year-long-cyber-attack/s40/a9646/).

[10] Source: Patricia Weiss and Ludwig Burger, "Bayer contains cyber attack it says bore Chinese hallmarks," Reuters, April 4, 2019 (https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN1RG0NN).

[11] Few firms have an established practice of fostering partnership among their I&O and S&R teams. See the Forrester report "Ransomware Is A Business Continuity Issue."

[12] See the Forrester report "Forrester's Guide To Paying Ransomware."

[13] Examples include NotPetya and other attacks that traditional security tools did not cover.

[14] Source: FINRA (https://www.finra.org/sites/default/files/SEA.Rule_.17a-4.Interpretations_0_0.pdf).

[15] See the Forrester report "The Forrester Wave™: Data Resiliency Solutions, Q3 2019."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
- Infrastructure & Operations

Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

150915