FORRESTER®

Organizations Are Missing Critical Ransomware Recovery Capabilities

Why Ransomware Specific Recovery Tools Are Needed To Guard Against Modern Cyberattacks

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY VMWARE | JULY 2024

Traditional Backup And DR Are Not Enough To Recover From Ransomware

In 2023, ransom payments hit a record $1.1 billion. This was driven in large part by the fact that 75% of ransomware attacks are now fileless — meaning attackers are infiltrating companies without the malicious files that scanning services detect. Traditional recovery methods focus on scanning for malicious files, which leaves newer fileless threats undetected and the potential for unmitigated ransomware threats to be returned to production. To spot malicious activity and recover from fileless threats, organizations must power on workloads in isolated clean environments and analyze data over time. VMware commissioned Forrester Consulting to conduct a survey of 186 IT, I&O, and S&R respondents at organizations using a server virtualization platform to understand the changes they are making to ransomware prevention and recovery efforts amid the current threat landscape.

Key Findings

Ransomware recovery capabilities are missing. Immutable backups, DR orchestration, and file scans aren't enough. Guided restore point selection, isolated clean rooms, and behavioral analysis are key.

Recovery strategies aren't designed for ransomware. Creating an isolated recovery environment and process is hard and unpredictable, leading to legal, financial, brand, and talent attrition impacts.

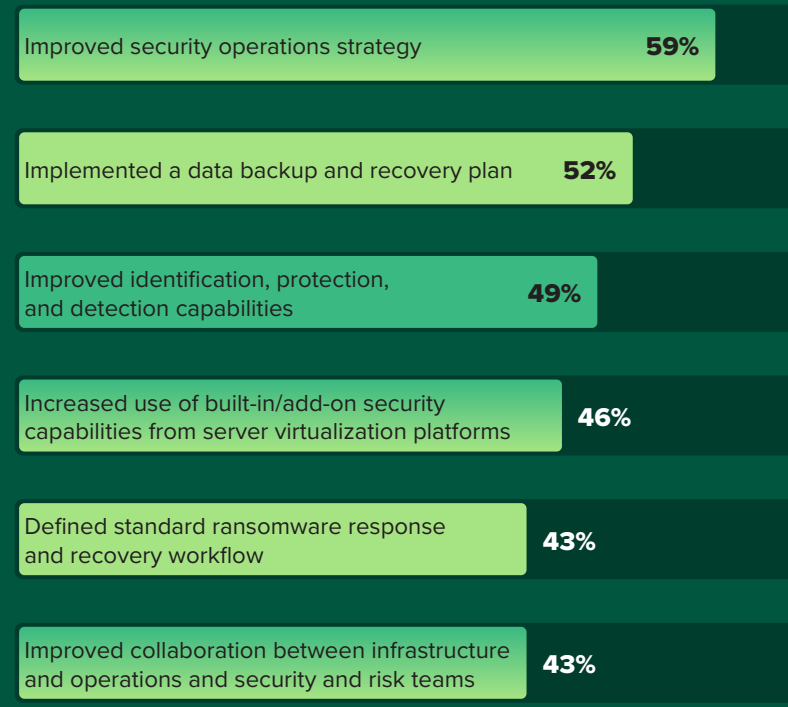
Solutions that integrate ransomware prevention and recovery capabilities can help. IT teams are able to more successfully identify and validate restore points and quickly recover workloads.

Improvements To Prevention And Recovery Strategies Are Far Too Reactive

After experiencing an attack, the majority of leaders focused on strengthening their organization's ransomware prevention and recovery strategies. This suggests that many lacked an awareness of the capabilities needed to protect their organization and recover from modern ransomware before they were attacked.

After an attack, more than half of leaders reactively improved their organization's security operations strategy and implemented a ransomware data backup and recovery plan. Nearly half improved their identification, protection, and detection capabilities; increased their use of built-in/add-on security capabilities from their organization's server virtualization platform; defined a standard ransomware response and recovery workflow; and improved collaboration between I&O and S&R teams.

Actions Taken To Improve Cyber Prevention And Recovery Plans



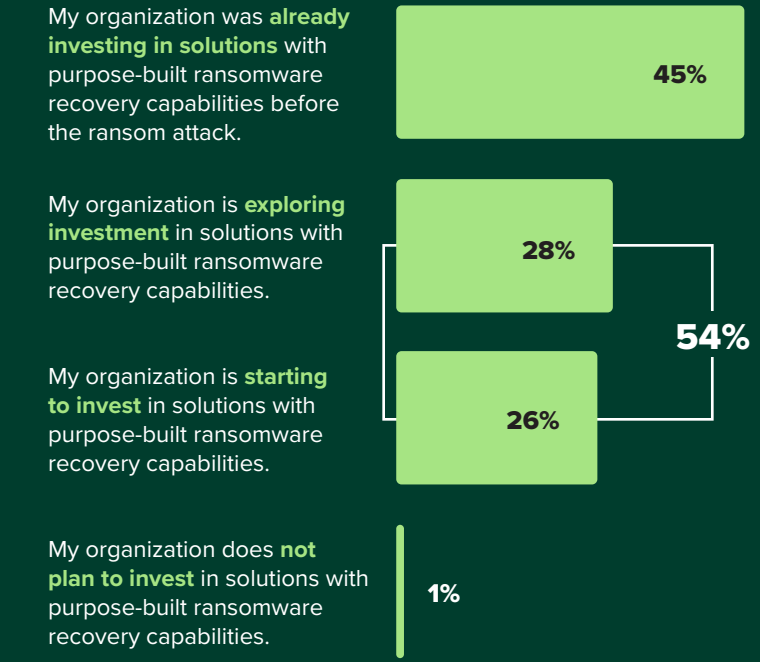
Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Note: Showing top six responses
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Many Organizations Wait Until After An Attack To Bolster Ransomware Recovery Strategies

Purpose-built ransomware recovery solutions bolster leaders' confidence in cyber recovery by ensuring their organizations have a set of critical capabilities in place to help orchestrate a successful cyber recovery process and mitigate the negative consequences of an attack.

However, among leaders whose organizations experienced a ransomware attack in the past three years, less than half reported they had purpose-built ransomware recovery solutions in place before the attack. This means that many organizations lack a standard set of critical cyber recovery capabilities needed to help them recover quickly, safely, and efficiently.

"Which of the following statements best describes how your organization is investing in solutions with purpose-built ransomware recovery capabilities after the attack?"



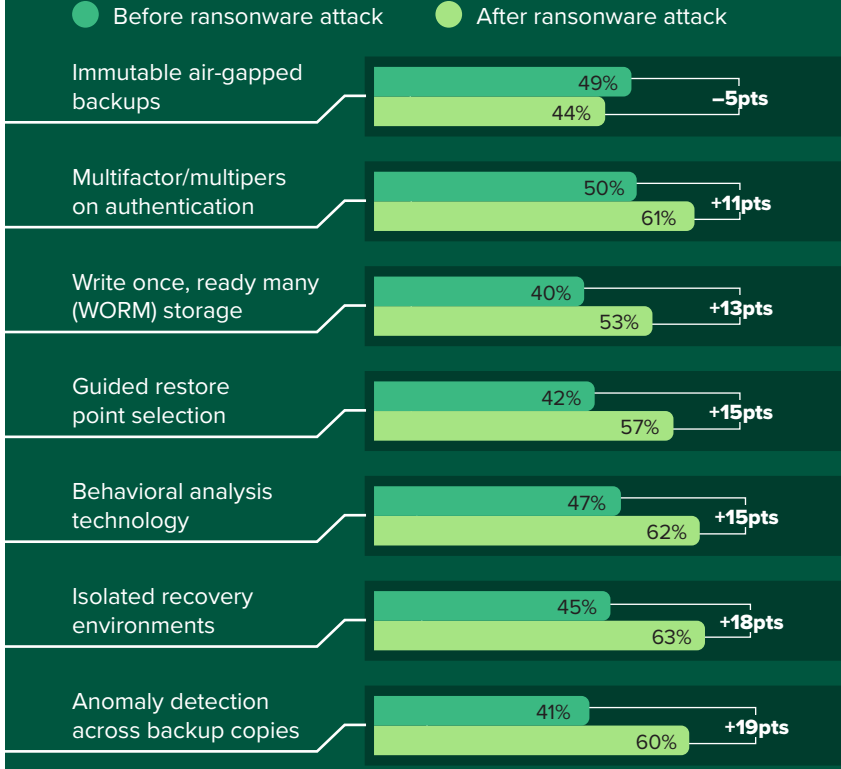
Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Critical Ransomware Recovery Capabilities Are Missing At The Time Of Attack

Because many organizations don't have a purpose-built ransomware recovery solution with a suite of capabilities in place before experiencing an attack, many are left without the critical capabilities needed to help facilitate a cyber recovery process.

Prior to the ransomware attack, leaders indicated their organizations were most likely to use multifactor/multiperson authentication and immutable air-gapped backups to recover. After experiencing the attack, they significantly increased the use of anomaly detection, isolated recovery environments (clean rooms), behavioral analysis, guided restore point selection, and write once, read many (WORM) storage capabilities — a strong indication that technologies like immutable backups are not enough to facilitate cyber recovery.

Ransomware Capabilities As Part Of Recovery Strategies Before Vs. After A Ransomware Attack



Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Note: Sorted by the point difference between "Before ransomware attack" and "Today."
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Poor Communication And Insufficient Resources Challenge Organizations' Ability To Recover

In addition to missing capabilities when an attack hits, many organizations also lack an orchestrated process between IT, security, and business leaders to initiate recovery actions at the time of the attack. This adds friction to the recovery process and has a direct impact on downtime and remediation costs.

The majority of leaders indicated that the solutions their organization uses for ransomware recovery are only optimized for disaster recovery. This poses a critical problem, as the validation of recovery points only includes file-based scans of static backup copies, leaving fileless malware undetected and causing increased damage and reinfection.

The Top Challenges Experienced With Ransomware Recovery Efforts

46%

Lack of an orchestrated process in place between IT, security, and business leaders for responding and recovering

38%

Inability to effectively identify good recovery point candidates

38%

Inability to prevent reinfection during the recovery process

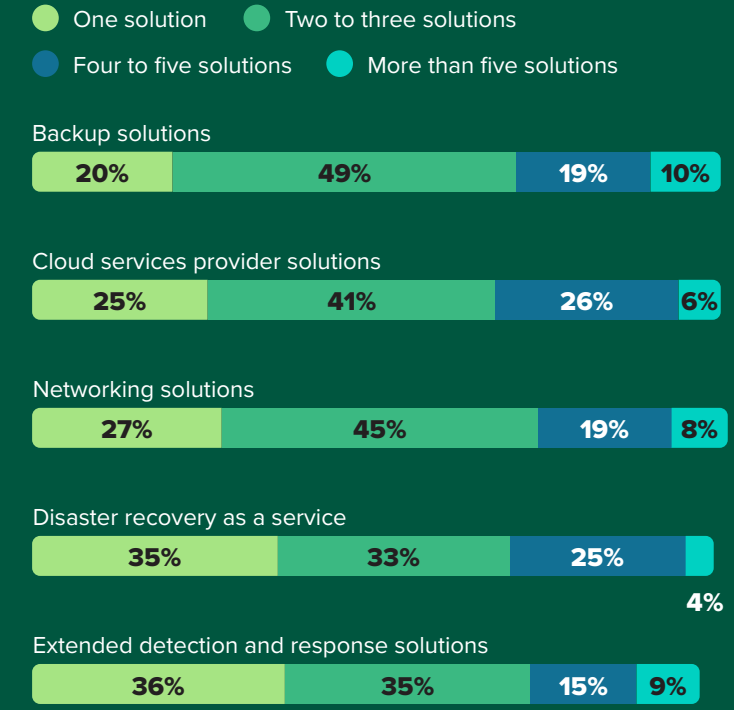
Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Organizations Are Forced To Patch Together Multiple Solutions To Enable Ransomware Recovery

Approximately three in five leaders indicated that their organization's ransomware recovery required many tools and processes — which made orchestrating a recovery process even more challenging.

The majority of leaders reported using more than one solution to enable recovery across each of the following categories: backup, cloud infrastructure, networking, disaster recovery as a service (DRaaS), and extended detection and response. Not surprisingly, patching these solutions together and creating an isolated recovery environment to iteratively test and validate recovery point candidates is not a straightforward process, resulting in an unproductive use of IT resources, increased downtime, and higher overall costs.

The Number Of Solutions Required Across Each Category For Ransomware Recovery In Server Virtualization Environments



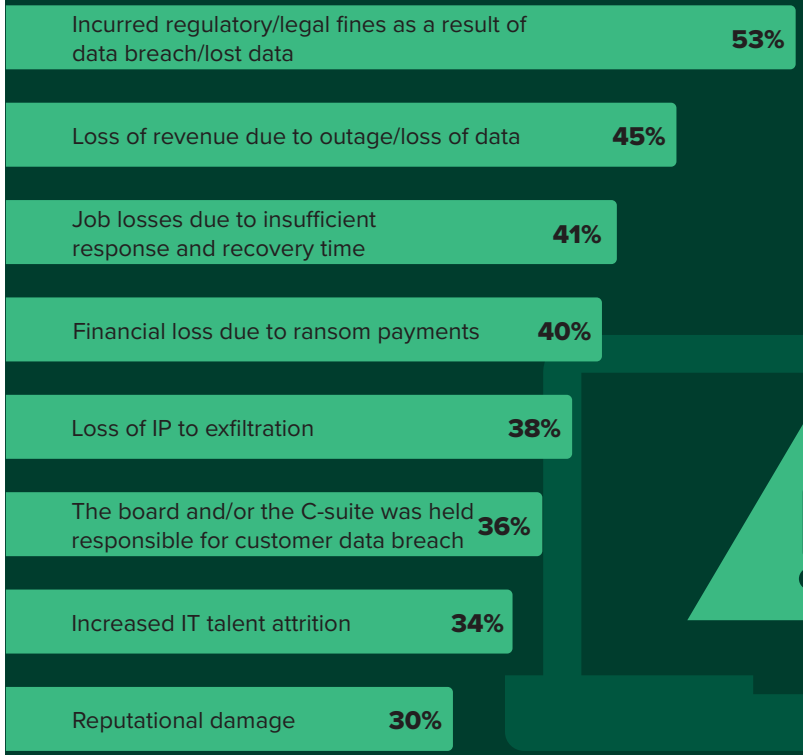
Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Leaders Can't Ignore The Risks Of Not Improving Prevention And Recovery Capabilities

By failing to proactively modernize and adapt ransomware prevention and recovery capabilities for an increasingly sophisticated threat environment, leaders open up their organization to serious consequences, such as legal and regulatory penalties, revenue losses, job losses, financial losses, IP losses, the board/C-suite being held responsible for customer data breaches, and reputational damage.

Some 99% of leaders whose organizations have faced a ransomware attack indicated they experienced at least one serious consequence; 77% indicated their organizations experienced three or more as a result, highlighting the level of urgency leaders face in improving their prevention and recovery capabilities.

The Consequences Experienced As A Result Of A Ransomware Attack



Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

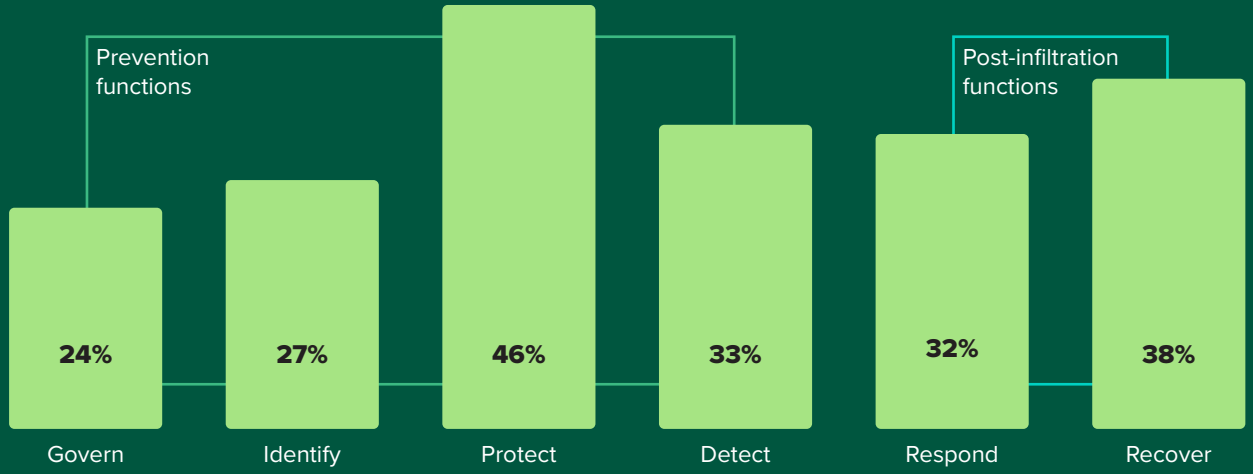
Organizations Need More Help To Improve Ransomware Prevention And Recovery Strategies

While leaders recognized the urgency to improve their cyber prevention and recovery capabilities after experiencing widespread damage, less than half had high confidence in the changes that their organization was making to improve after experiencing an attack.

The low level of confidence in the changes being made is indicative of organizations' talent and capability gap; this inhibits their ability to successfully protect and recover their data in the current threat landscape should they be hit again.

Confidence In The Ability To Execute On NIST 2.0 Cybersecurity Framework Functional Areas Based On Changes The Organization Has Made After Experiencing A Ransomware Attack

(Showing "9/10 Much more confident today")



Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

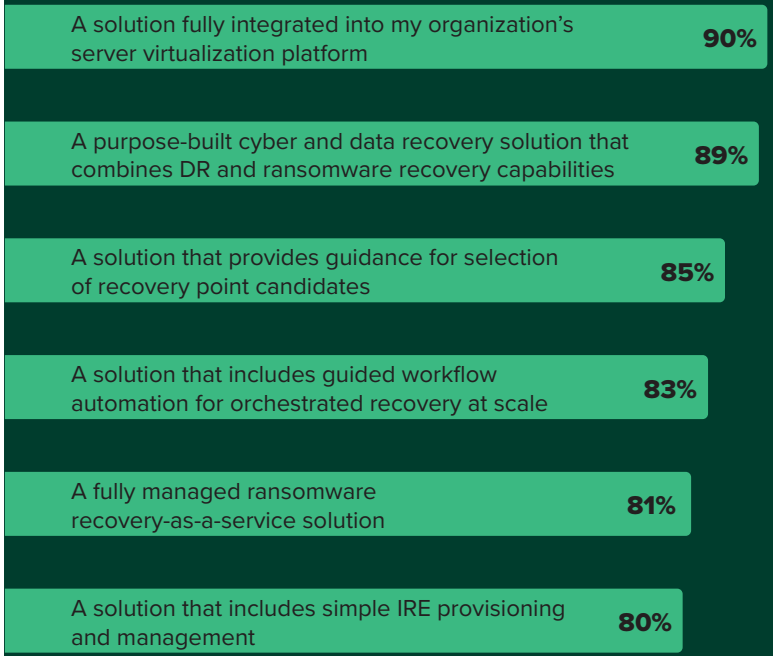
Organizations Need Integrated Ransomware Recovery Solutions

Based on the low level of confidence leaders had in the changes their organizations were making to prevention and recovery strategies after experiencing a ransomware attack, it's clear they need more help to enable confident, quick recovery from modern cyberthreats. Solutions that streamline ransomware response — guiding businesses through recovery point selection/validation, isolated clean room deployment, and the network isolation of virtual machines at recovery to prevent reinfection — enhance an organization's ability to recover from an attack.

Ransomware solutions that fully integrate into an organization's server virtualization platform, combine traditional disaster and ransomware recovery capabilities, and offer a fully managed recovery service are also vital for improving the ability to recover from attacks.

The Importance Of Ransomware Response And Recovery Solution Attributes To The Ability To Recover

(Showing "Important/Very Important")



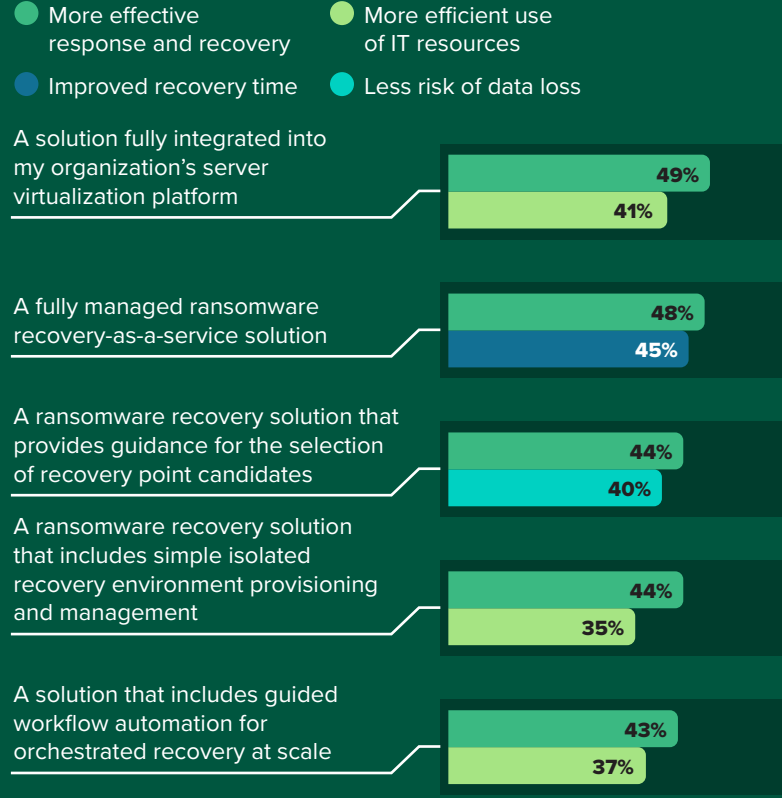
Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Simplified Cyber Recovery Delivers Huge Benefits

Guided workflow automation, embedded recovery point validation for both file-based and fileless attacks, and isolated recovery environment (IRE) provisioning and management drive increased success in response and recovery operations, enable more productive use of IT resources, and reduce the risk of data loss.

The most significant benefit, however, lies beyond the individual capabilities needed for successful cyber recovery. The ability to integrate these critical capabilities into a single solution that can be seamlessly managed and deployed to a virtualized infrastructure removes the need for the deployment, integration, and maintenance of separate siloed solutions. This has the most significant impact on improving the ability to successfully recover, IT resource productivity, and time to recovery.

The Top Benefits Of Ransomware Recovery Solution Attributes



Base: 186 global manager+ cloud infrastructure decision-makers in IT, I&O, and security and risk
Note: Shows the top two options for select solution attributes; sorted by "More effective response and recovery"
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2024

Conclusion

Based on the responses to this survey, several solution attributes can help solve critical cyber recovery challenges:

- **Guided recovery point selection and validation.** These solutions help locate good recovery points and integrate behavioral analysis to identify fileless malware. They accelerate the recovery process and improve IT and security collaboration.
- **IRE provisioning.** Setting up, securing, and managing the isolated clean room for recovery point validation uses unnecessary IT resources. Solutions that seamlessly deploy and manage an IRE simplify recovery operations.
- **The integration of multiple point products.** A platform that integrates recovery point selection, validation, and restoration at scale removes the need for organizations to manually stitch together disparate products and makes recovery faster.

Resources

Related Forrester Research:

Effective Ransomware Response Requires Coordination Between I&O And Security, Forrester Research, Inc., September 9, 2021

The State Of Ransomware Attacks And Defenses, Forrester Research, Inc., February 2, 2022

Related Blogs/Webinars

Brian Wrozek, The US Government Is Here And Really Wants To Help Protect You From Ransomware, Forrester Blogs

April 5, 2022, The State Of Ransomware Attacks And Defenses, Webinar

Project Team:

Ben Anderson,
Demand Generation Consultant

Contributing Research:

Forrester's Technology Architecture & Delivery and Security & Risk research groups

Methodology

This Opportunity Snapshot was commissioned by VMware. To create this profile, Forrester Consulting conducted an online survey of 186 ransomware recovery decision-makers whose organizations use a server virtualization platform with hybrid or private cloud. Decision-makers also must have indicated that their organization has experienced a ransomware attack over the past three years to take the survey. Respondents were offered a small incentive as a thank you for time spent on the survey. The custom survey began and was completed in April 2024.

Demographics

GEOGRAPHY	
United States	51%
United Kingdom	19%
Canada	9%
Singapore	8%
India	6%
Australia	4%
New Zealand	3%

COMPANY SIZE	
500 to 999 employees	38%
1,000 to 4,999 employees	43%
5,000 to 19,999 employees	17%
20,000 or more employees	2%

INDUSTRY	
Financial services/ insurance	28%
Healthcare	25%
Education	24%
Government	23%

DEPARTMENT	
IT infrastructure and operations	68%
Security and risk	32%

TITLE	
C-level	16%
Vice president	7%
Director	24%
Manager	53%

Note: Percentages may not total 100 due to rounding.


FORRESTER®