VERITAS™

Four Ransomware Resiliency Challenges You Can Combat with Confidence

Ransomware is a growing threat to operational resiliency in all digital enterprises.

Report after report documents a rise in these attacks, during which malware encrypts operational data until an organization pays a ransom and yet sometimes still suffers catastrophic data loss.

These four stories describe typical challenges administrators may encounter, how they can lead to ransomware mistakes and how organizations might prevent these attacks.

Ransomware by the Numbers

11 seconds

An organization will be hit by a ransomware attack every 11 seconds in 2021[1]

+25%

Ransomware incidents rose 25 percent in Q1 2020 compared to Q4 2019.[2]

$84,000

The average cost per business to recover from a ransomware attack is more than $84,000.[3]

1

There's no such thing as failproof frontline protection.

"I thought our security software covered us from any malware impact, but somehow ransomware got through."

—IT Admin, International Telco Firm

The fact is that no solution can protect your data 100 percent of the time from 100 percent of criminal acts, including ransomware.

That's why you need a robust, multi-layered plan to protect against potential worst-case scenarios. Frontline defenses alone aren't good enough.

Instead, look for a multi-layer solution that lets you:

- Detect, monitor and remove any threats that may get through your frontline security defenses.

- Recover with minimal downtime and maintain data integrity even if an attack is successful without having to pay a ransom.

Tip: Use automated recovery testing.

One of the roadblocks to effectively preparing for a ransomware attack is the inability to develop and test a recovery plan. The Veritas Enterprise Data Services Platform provides all the components needed to create a reliable, end-to-end recovery plan that includes automated, non-disruptive testing with zero downtime.
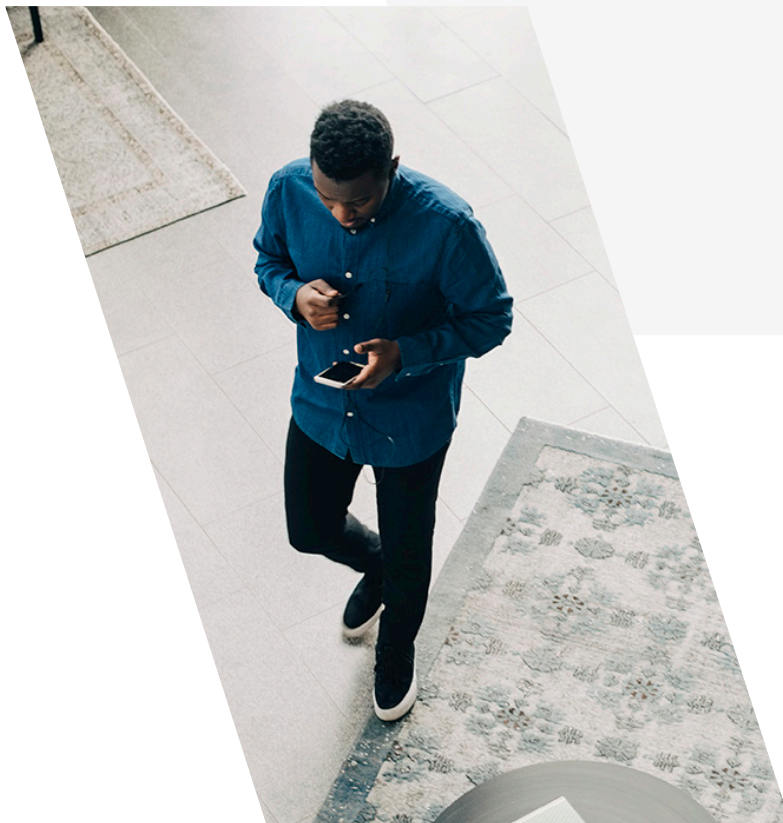
2 Balancing budget and scale is difficult.

"We had a burst of unexpected growth, which meant more data to protect. Unfortunately, the servers our data protection vendor gave us couldn't scale and we didn't have time or budget for new ones."

— VP Operations, Global Healthcare Organization

Digital enterprises need to be highly responsive to market changes—and their solutions need to support them every step of the way.

Operational resiliency requires protecting data volumes as they grow, no matter how or when growth happens.

With a software-defined data protection solution, you aren't limited when you need to quickly scale. Plus, the solution can expand heterogeneously to any servers, whether on-premises or in the cloud.

Globally, data will grow

175 ZB by 2025[1]

3

Decentralized point solutions create complexity.

"I inherited a mess of decentralized point solutions but didn't move fast enough to assess them and make changes. I put it on the back burner for a bit, and that's when the attack happened."

— IT Director, Financial Services Leader

Using a mix of decentralized point solutions for data security and recovery leaves a lot of holes for criminals to exploit.

It's also complex and complicated—another gamble because it's harder to achieve an end-to-end view of your complete infrastructure footprint and establish consistent security procedures.

True operational resiliency requires unified orchestration across all your systems with a set of tools that fits your organization's needs.

Tip: Find and fix your gaps.

Most enterprises have data spread across different virtual machines (VMs) and servers, and many have different security and backup solutions as well. A solution like Veritas APTARE™ IT Analytics, which provides visibility into data protection across a mix of point solutions, can help you discover what's actually covered where and by what.

4

Not all solutions offer full coverage.

"I prioritized a vendor that I had past experience with and didn't look closely enough at the enterprise-wide picture. Turns out this solution covered only some of our needs and not all of our data. I have a lot of explaining to do."

— Systems Analyst, U.S. Government Agency

Don't use yesterday's rigid technology to solve today's problems.

Today's architectures are dynamic and span on-premises, hybrid cloud and multicloud. That means one organization might require a software deployment for protection but another might need an appliance while a third might want both plus Linux.

Protect your data with proven, sophisticated solutions that are nimble and extensible so you can protect your entire data footprint from ransomware loss.

Yes
84.7%

Unsure
2.2%

No
13.1%

When asked if the cloud provider is responsible for backing up cloud data, most cloud admins agree (but they're wrong).

How can you stay ahead of ransomware?

To avoid your own ransomware mistake, you need to stay ahead of cybercriminals by preparing for the worst-case scenario with a comprehensive, flexible and proven platform that can cover all your needs—and all your data.

Learn more at veritas.com/ransomware

1. National Law Review, "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion, Feb. 13, 2020 (https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion)
2. Beazley Breach Response Services, "The enduring threat of ransomware," Jun 6, 2020 (https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html)
3. National Law Review, "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion, Feb. 13, 2020 (https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion)
4. IDC/Seagate, "The Digitization of the World From Edge to Core," November 2018 (https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf)
5. Veritas, "2019 Truth in Cloud Report" (https://www.veritas.com/solution/cloud/research)

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

1076 11/20