# 5 Ways to Defend Data from Ransomware

VERITAS™

By 2021, it's estimated a new organization will fall victim to ransomware every 11 seconds, costing businesses a predicted $20 billion globally.[1]

A robust frontline defense is the first step in preventing ransomware attacks, but it's not enough. As cybercriminals grow more sophisticated, companies are realizing it's no longer a matter of "if" ransomware strikes, but "when."

How can you maintain operational resiliency when that day comes? Applying each of these five notable protection points, you can take on ransomware knowing your organization's data is protected, with the ability to detect malicious activity and ultimately recover from an attack.

## 1. HARDEN HARDWARE AND SOFTWARE

The complex, interconnected nature of today's IT systems often provides ransomware the ability to wreak havoc on all of an organization's data through a single point of entry, like a phishing email delivered to an unsuspecting employee.

To fortify against such vulnerabilities, you can reduce your IT attack surface with hardware and software hardening best practices like multi-factor authentication, risk-aware password management and role-based access.

## 2. SECURE BACKUPS WITH IMMUTABLE STORAGE

Backups offer a last line of defense against ransomware, and cybercriminals are increasingly targeting them to limit their victims' ability to recover. If an attacker gains access to backups, an organization has little recourse against paying a ransom. Arm yourself with immutable storage capable of writing data so it cannot be altered or deleted.

Should ransomware penetrate your organization's frontline defenses, data written with Write Once Read Many (WORM) protections is safeguarded from encryption or erasure. Data is impermeable to the threat of ransomware and available for recovery.

## 3. PROTECT DATA WITH AIR GAPPING

Network-connected backups are vulnerable to cybercriminals because any connected system can be targeted and penetrated. Protect data by creating a physical space between stored data and the networked system—literally, an air gap. Offline backups offer one of the few failproof measures to prevent malicious data access and encryption.

Seek a solution that facilitates the duplication and replication of data to storage media that can be air-gapped, then automate its disconnection from the network. Equally important, your chosen solution should be able to call back air-gapped media when needed for ready recovery.

## 4. SET UP ALERTING AND REPORTING

Today's cybercriminals target the entirety of an organization's data and infrastructure. Awareness and control of data, infrastructure and user activity is critical to detecting vulnerabilities and threats.

Look for a solution that presents infrastructure in a single view. It should have the ability to identify protection and security gaps, scan data across backups and storage, and gain a baseline standard for system activity and user access and behavior.

Once IT teams have this reference for data and infrastructure, including expected data activity and cross-system permissions, they'll benefit from tools that automatically alert them to changes. Among them, suspicious spikes in activity or telltale behavior that can indicate the infiltration of ransomware.

## 5. IMPLEMENT AN AUTOMATED, ORCHESTRATED RECOVERY PROCESS

A ransomware attack rarely impacts a single system. What starts as one corrupted end-user device can quickly spiral and endanger an entire datacenter. Today, many IT teams are building hybrid multicloud infrastructures to satisfy the needs of the modern enterprtise. That complexity can compound recovery; enterprises with hundreds or thousands of servers cannot quickly manually recover data.

Maintain control in the face of an attack with an automated, orchestrated recovery process that works across all environments. Automation and orchestration facilitate rapid, reliable data recovery at scale.

Additionally, a solution that enables non-disruptive testing allows you to prepare for recovery by conducting frequent, comprehensive tests without negatively impacting production. When ransomware strikes, such a solution can also test backup data to ensure that it's malware-free before you proceed with full-scale recovery.

## TAKE ON RANSOMWARE WITH CONFIDENCE

Potentially devastating ransomware attacks are a harsh reality. By applying our five notable protection points, you can develop a resiliency strategy that reinforces your organization's data and infrastructure against modern malicious threats so you can confidently take on ransomware.

Improve ransomware readiness by putting technologies in place to support IT system protection, detection of malicious activity and strategic recovery if needed. Armed with these tools you can gain peace of mind knowing your organization is prepared to recover from today's data-damaging threats.

Learn more about maintaining operational resiliency at www.veritas.com/ransomware.

[1] The National Law Review, "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion," Feb. 13, 2020.

## ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. 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 supports more than 500 data sources and over 150 storage targets, including 60 clouds. 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