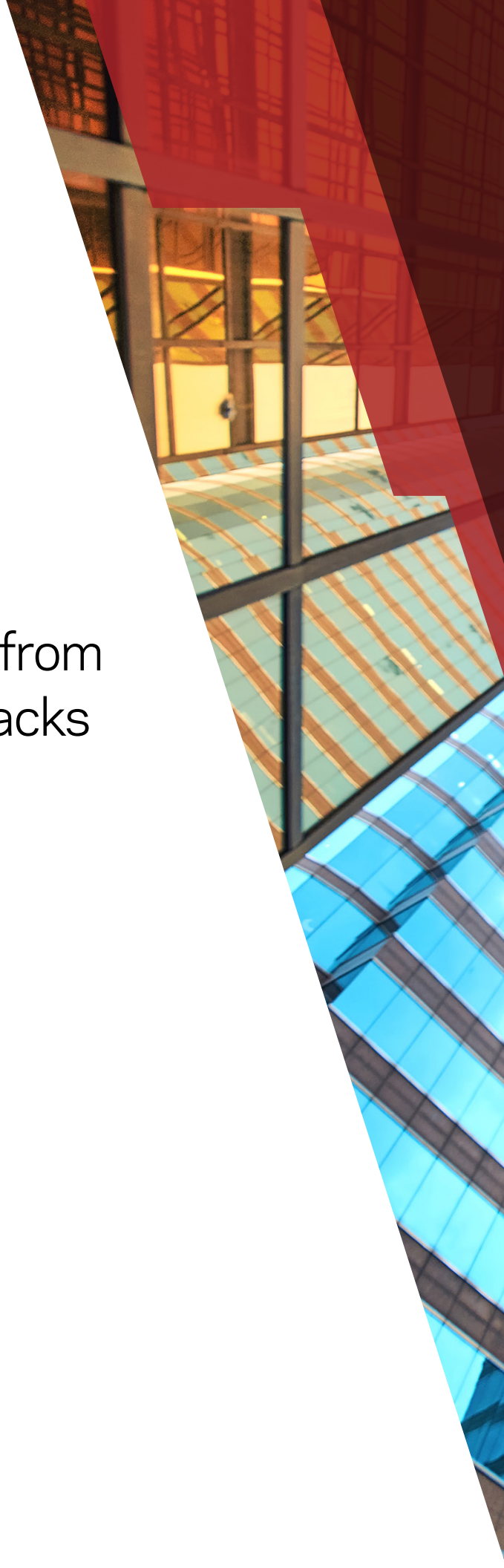


VERITAS

Defend Your Organization from Evolving Ransomware Attacks

Learn what it takes to reduce risk and strengthen operational resiliency.

Cyberattacks on the enterprise are evolving and changing, and ransomware is no exception.

Just a few years ago, cybercriminals focused primarily on encrypting data in exchange for a ransom that could range from several hundred to hundreds of thousands of dollars. Today, everything from factory machinery to lifesaving medical equipment is at risk. What's more, thieves increasingly seek control of backup systems that are used to restore encrypted files and systems. This tactic makes it more difficult to recover, even with backups in place.

Today's environment is challenging and frightening—even for the most well-prepared companies. A single incident can lead to data loss, downtime, regulatory infractions and barriers to productivity. For consumer-facing businesses, there's also the risk of brand damage and a downturn in revenues.

Yet there are steps your organization can take to greatly reduce risk and aid in recovery when a malicious attack occurs and ransomware breaches your organization's frontline security defenses. A robust framework that eliminates a single point of failure and creates operational resiliency is now essential.

Today's environment is challenging and frightening—even for the most well-prepared companies.

How does ransomware typically spread?

Phishing
An email, often with an executive's name, includes a malicious link spoofing a legitimate website or address.

Drive-by downloads
A visit to a compromised site can result in ransomware installations like those that infected the BBC, the NFL, The New York Times and other major sites in the past.

Removable media
Infected USB sticks and other devices, sometimes appearing to be sent as part of a promotion, infect a system.

Remote desktop protocol
IT administrators occasionally require remote access to machines. Sometimes, hackers may be able to enter a system through an open port.

What Ransomware Costs

$7.5 billion

The total cost of ransomware attacks in 2019[1]

$84,116

The average ransomware payment, which has increased 104% since 2019[2]

16.2 days

The average downtime from a ransomware attack[3]

97%

of descriptors worked, but **3%** of companies report that they permanently lost data[4]

How Ransomware Is Evolving

Approximately every 14 seconds, an organization is hit with a ransomware attack.[5] Yet it isn't only the frequency of attacks that's a concern—it's also the growing level of sophistication used to infect systems and lock data.

Today's ransomware is sophisticated. It's safe to assume that any system and data repository that can potentially be accessed—including those residing in the cloud—will be accessed. In many cases, an initial payload infects a system and then downloads other files that worm their way through address books and various applications, data repositories and systems. The malware may seek out specific targets or continue propagating to carry out a future attack. It may also look for backup files and block access to them.

Once ransomware is inside an organization, chaos can ensue. Recent ransomware incidents have shut down hospitals, interrupted 911 service and prevented jail doors from operating.

Approximately every 14 seconds, an organization is hit with a ransomware attack.

In June 2020, an automobile manufacturing giant was hit with a ransomware infection that suspended operations at car and motorcycle factories in the United States, Turkey, India and South America.[6] In April 2020, an IT services giant was targeted and reported that crooks stole unencrypted data from the company's IT systems and then tried to extort money from the firm.[7]

Although the goal is nearly always to extract money from a targeted organization, attackers may threaten a range of outcomes. These could include halting manufacturing or retailing operations by pulling key systems and applications offline, auctioning off sensitive data—including personally identifiable information (PII) about employees—and financial records or trading secrets through the dark web. They may also make it impossible for individuals to access medical records and crucial services. For instance, a 2018 attack against a healthcare provider prevented 1,500 customers from accessing key services.[8]

Four Key Tools to Battle Ransomware

User access and data management permissions tools

These include audit logs, file types, access permissions and reads and writes—all in customizable, intuitive user interfaces.

Recovery systems

Recovery requires robust automation and orchestration, including fast, simple recovery systems that can scale with the enterprise and use automation to handle routine tasks.

Cross-system data and infrastructure visibility

These tools automatically detect and report changes in data access and baseline data activity, such as when a backup's size significantly grows. It also includes analytics and specialized software to spot and act on known ransomware file extensions and tools to detect and report on anomalous behavior and usage patterns.

Robust backup systems

These include tools for reliable backup management, immutable storage, secure long-term retention, built-in replication and native cloud integration across solutions. Resiliency requires hardening, immutability and air gapping.

How to Adopt a Defensive Strategy

In an ideal world, an organization's frontline cybersecurity solution would provide an impenetrable layer of protection for its IT systems. But given the evolving state of malware—coupled with increasing IT complexity—a single layer, no matter how robust, could be breached.

What's more, as bad actors get smarter, organizations must decisively respond. It's not enough to merely focus on stringent cybersecurity and regulatory standards. The problem is broader, and today's borderless networks and highly interconnected systems within the Internet of Things introduce additional challenges. Consequently, it's crucial to have a multi-layered approach.

Organizations that tackle data classification and map their data with appropriate backup systems and protections can begin to build a framework that boosts protection and minimizes overhead. Doing so means automated, scalable protection against ransomware is finally possible.

5 Reasons Organizations Get Hit by Ransomware

1. No coherent strategy or plan to battle ransomware
2. A lack of collective awareness among teams
3. The absence of a robust backup technology framework
4. A poor or nonexistent recovery plan
5. A lack of attention to a broader framework of controls, tools and visibility

Automating

At the heart of a best practice strategy is eliminating a single point of failure and automating processes. These considerations require a good deal of thinking, planning and strategizing to ensure the backup and recovery framework is robust, automated and flexible enough to grow with expanding data volumes—while maximizing the cost-benefit equation.

Testing

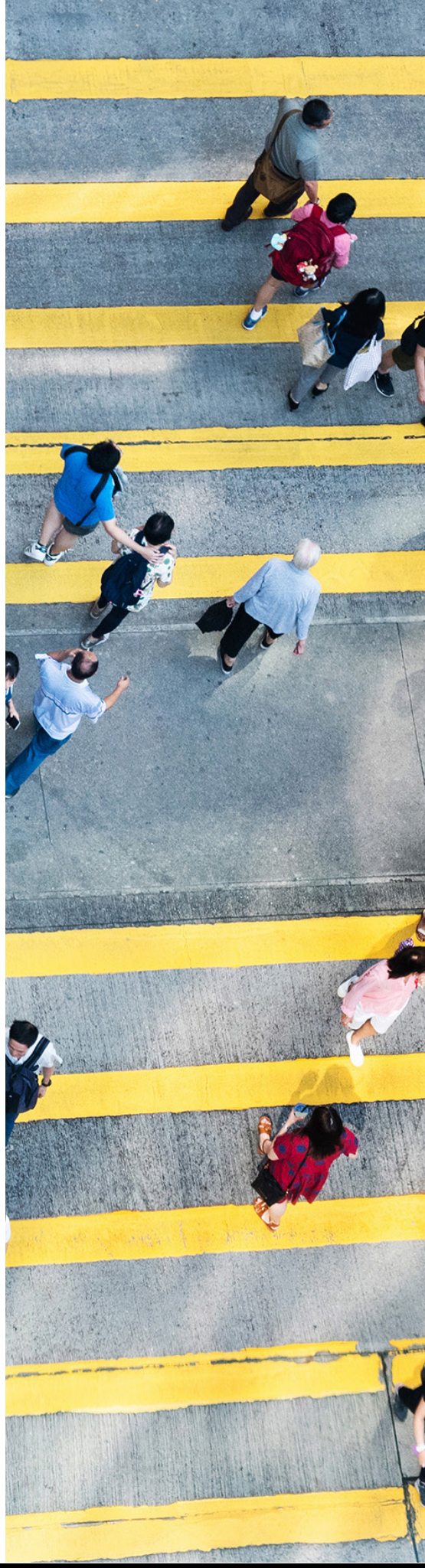
Designing dependable and secure backups is only part of the task. You also need to regularly test recovery systems to ensure all aspects of the plan work in the real world, including the ability to access and use secondary copies, if needed.

Building

It's critical to build out a protective framework for all your data. One problem many enterprises face is so-called "dark data" that hasn't been properly classified. In some instances, organizations may lack the tools to handle this task. In other cases, organizations just haven't devoted the time and resources needed to build the necessary defenses.

RPOs and RTOs

Part of the challenge revolves around identifying recovery point objectives (RPOs) and recovery time objectives (RTOs). It's crucial to understand these two metrics in terms of the value of data, systems and potential damage to the enterprise. One application can potentially be down for days without serious consequences, while another may wreak havoc within minutes. Both metrics play an important role in developing a baseline from which an organization can build a ransomware recovery plan that addresses business needs while remaining attentive to IT realities.



Multi-Layered Protection Is Paramount

An effective multi-layered defense addresses the risk today's malware represents, and it's the defense strategy an organization must use to fully protect its systems and data.

This framework must start with acknowledging that any data system can potentially be compromised and encrypted with ransomware, including network-accessible backup files. In fact, recent attacks have focused on infecting backup files to cripple organizations and challenge their ability to recover quickly. This type of attack can make the price of the ransom lower than the cost of lost business.

Typically, a backup strategy includes keeping at least three copies of your data in two distinct locations and one of them off-site. To maximize protection, these systems must include at least two different types of media—and the data should be encrypted and out of reach of

Any data system can potentially be compromised and encrypted with ransomware, including network-accessible backup files.

cybercriminals. One of the best ways to help ensure secure data is to place it on immutable write-once media such as Write Once Read Many (WORM) DVDs or optical discs. Of course, these media must be protected with physical security as well.

The task doesn't stop there, however. Organizations need broader protection to defend all their data and systems: tools like multi-factor authentication, risk-aware password management and role-based access control (RBAC) plus tools capable of automatically detecting and reporting changes in data access and baseline data activity. These controls and this standard of awareness make it tougher for cybercriminals to enter systems while ensuring a rapid, purposeful response—including blocking access to suspicious users and targeting and deleting known ransomware files.

A comprehensive data management and protection solution provides the tools required to reinforce an organization's data and infrastructure and protect against modern malicious threats like ransomware. With this framework in place, your organization can effectively fortify its IT system, mitigate risk with improved data and infrastructure visibility and ensure automated, orchestrated recovery in the face of an attack. Along with effective employee training about how to avoid risky behavior like not clicking on bad links or using unauthorized devices and services, this approach will take protection to a higher level.

Take Control of Your Ransomware Prevention

In the battle against ransomware, end-to-end visibility isn't just a good idea—it's crucial. When an enterprise knows where its data resides, the value of the data and what processes and tools can best protect it, the risk of ransomware is ratcheted down. In today's anxiety-provoking cybersecurity environment, a sound strategy and systems that reduce attack surfaces and harden infrastructure will give you peace of mind—and take your enterprise to a safer, more secure level.

Learn more at veritas.com/ransomware

1. EMSISOFT, "The State of Ransomware in the U.S.: Report and Statistics 2019," Dec. 12, 2019.
2., 3., 4. Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," 2019.
5. The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Dept. of Homeland Security, "Ransomware."
6. Ars Technica, "Honda halts production at some plants after being hit by a cyberattack," June 9, 2020.
7. BleepingComputer, "IT giant Cognizant confirms data breach after ransomware attack," June 17, 2020.
8. HealthITSecurity, "Allscripts Ransomware Attack Impacts Limited Number of Applications," Jan. 19, 2018.

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

1077 10/26