VERITAS

10 CYBERSECURITY BEST PRACTICES THAT RANSOMWARE FEARS MOST

If you're like most IT professionals, the threat of ransomware strikes fear deep into your heart. And you have a valid reason to worry—ransomware now targets every industry, which means it's only a matter of time before your organization will be attacked.

Although ransomware can cause serious damage to your business and reputation, it's not invincible. In fact, it's only as strong as your organization's weakest link. So why not turn the tables? Let's look at the most impactful best practices you can implement right now to create the multi-layered, flexible, unified defense strategy that will ensure business resilience—and make ransomware attackers afraid instead.[1]

1

Prompt systems updates.

Using end-of-life software can allow attackers to exploit unmitigated security vulnerabilities. To reduce your attack surface, ensure you patch and upgrade all infrastructure, operating systems and software applications frequently.

2

Frequent backups.

If you back up your data, system images and configurations frequently, you'll always have an up-to-date place to resume operations if ransomware does strike. Better yet, go one step further by implementing the "3-2-1" recommended backup practice outlined below and test recovery often.

3

Zero Trust model and policies.

The Zero Trust concept focuses on not trusting any devices—or users—even if they're inside the corporate network. Instead, put multi-factor authentication and role-based access control (RBAC) in place, monitor for and mitigate malicious activity and encrypt data both in-flight and at-rest to prevent data exfiltration. If you limit access to backups, you'll also shut down the most common entry method for ransomware.

4

Network segmentation and the 3-2-1 backup rule.

Dispersing your data—keeping three or more copies in different locations, using two distinct storage mediums and storing one copy off-site—will reduce the chances of an attacker gaining access to everything. The 3-2-1 approach ensures a vulnerability in one doesn't compromise all your copies and provides options if an attack takes out an entire data center.

5

Endpoint visibility.

If you implement tools that provide complete visibility across your environment, detect anomalies and hunt for and alert you to malicious activity on your network, ransomware will have no place to hide.

6

Immutable and indelible storage.

One of the best ways to safeguard your data against ransomware is to implement immutable (can't be changed) and indelible (can't be deleted) storage with an internally managed compliance clock. Even the strongest ransomware attack won't be able to break down these walls.

7

Rapid recovery.

Most ransomware attackers hope for two things: time for the attack to spread and money (from you) to make it stop. Implementing an automated recovery process that provides flexibility and having an alternative option—rapidly standing up a data center on a public cloud provider, for example—can shorten downtime and provide alternatives to paying a ransom.

8

Regular tests and validation.

Creating a comprehensive data protection plan doesn't mean your job is finished. Testing ensures your plan will work when you need it. And although initial testing can confirm all aspects of the plan actually work, it's critical to test regularly because IT environments are constantly in flux. It's also a great idea to hire a third party for validation.

9

Cyberattack playbooks.

Imagine if everyone in your organization knew exactly what to do and when in the face of a ransomware attack. It's not impossible if you create a standard playbook that clarifies roles and aligns and empowers cross-functional teams with clear communication paths and response protocols in the event of emergencies.

10

Educated employees.

Don't blame your employees if they're the gateway to an attack. Mistakes happen. Instead, focus on training them to identify phishing and social engineering tactics, build strong passwords, browse safely and always use secure VPNs, never public Wi-Fi.

1. U.S. Federal Government Executive Order, May 2021

You have the power to make ransomware fear you rather than the other way around. By putting together a multi-layered ransomware resiliency strategy along with impeccable cybersecurity hygiene, you can stop attackers before they gain a foothold. Learn more about how Veritas solutions can help you take control and reduce business risk.

Download the white paper ›

Renew your Veritas maintenance and services to continue to get access to free support and upgrades, so you can make the most of your Veritas products. Renewing allows you to capitalize on the innovations in the latest releases as soon as they are available to keep your products up-to-date and operating as they should. It also allows you to leverage Veritas services to get the always on technical support you need to handle and quickly resolve issues. As a result, you can extract more value from your Veritas investment, reduce your risks, and focus on your business. Learn more about Veritas maintenance and support at veritas.com/renewals.

VERITAS

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

For global contact information visit:
veritas.com/company/contact