AvePoint

Ransomware Readiness Checklist

Practical Tips to Prepare Your Organization for Ransomware

Cybersecurity and rising number of ransomware attacks and data breaches have captured headlines around the world. This media attention has led to increasing consumer awareness that "they and their personal data" has become the target of cyber criminals, social hacktivists, and innocent or adversarial insiders.

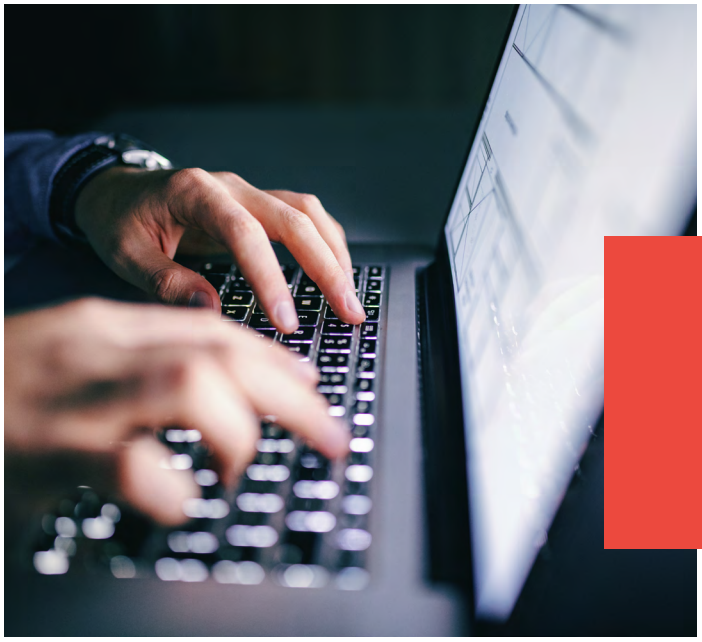
In our new normal work environment, with a remote and hybrid workforce, many businesses have taken a rapid "ready or not" approach into the adoption of cloud technologies, causing a virtual explosion of data. While data is now being accessed and managed in the cloud, the devices and locations from which people are doing their work are often in shared, non-private spaces. These conditions are prime for cyber criminals to swoop in and take advantage of vulnerabilities in our systems.

The most significant cybersecurity threat today is ransomware. On the corporate level, significant breaches may be career-ending for company executives, and as the level of attention on attacks rises, so does potential reputational as well as financial damage to the organizations that fall victim.

"Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." (Ransomware — FBI)

Most ransomware attackers are not evil or insane; they just want something. While most organizations simply do not have the budget to protect against evil people, they can protect against people that will look for weaker targets. This means that if you make it harder for threat actors to attack you and your organization less attractive for them to target, they will likely go somewhere else.

These simple steps will help not only decrease the likelihood of an organization being targeted with ransomware, but also to potentially mitigate the damages if and when you are infected.



01 Make sure that you are running up-to-date end-point security and anti-virus software for all your emails

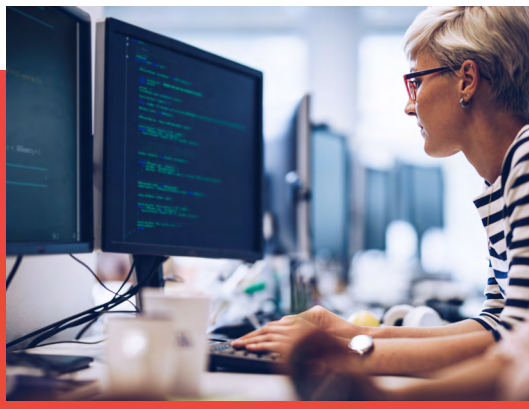
Email phishing and spam are the main way that ransomware attacks are distributed. Secure email gateways with targeted attack protection are crucial for detecting and blocking malicious emails that deliver ransomware. These solutions protect against malicious attachments, documents, and URLs in emails delivered to user computers.

It's also essential to secure your users' inboxes. Regularly patch your systems, conduct vulnerability assessments, and leverage intrusion detection, real-time anti-virus, and end-point protection. Make sure you are not only filtering and blocking malicious emails, but also training your end users to "think before they click."

02 Implement anti-phishing campaigns and block malicious websites

Secure web gateways can scan your users' web surfing traffic to identify malicious web ads that might lead them to ransomware.

While monitoring websites and web applications for potential hacks and exploits can identify threats before they become a problem, don't let these scanning technologies be your only security measure. Remember, most costly breaches are the result of simple failures, not attacker ingenuity.



03 Implement monitoring tools across your systems

Monitoring tools can detect unusual file access activities, viruses, network C&C traffic and CPU loads, possibly in time to block ransomware from activating.

04 Implement Identity Management and Least Privileged Access

Be sure that your organization has implemented policies for strong passwords and multi-factor authentication. A 2-factor authentication or multi-factor authentication is a must to decrease the possibility of compromised credentials.

In case credentials are compromised, limit user access to what is necessary for your employees to do their job; review and reaffirm this access regularly. For example, if an employee is working on a time limited project that requires access or permissions, those permissions should be tied to the length of the project only and should be revoked as soon as appropriate. Products like AvePoint Online Services can help you to appropriately provisions sites and users with limited permissions, access, and control.

05 Make it easier for your employees to do the right thing than the wrong thing

In the absence of security education or experience, people (employees, users, and customers) naturally make poor security decisions with technology. This means that systems need to be easy to use securely and difficult to use insecurely. This is a critical point and probably one of the single largest opportunities for security programs to be revamped.

Make it easier to use your systems properly. Create policies, rules and IT controls that make common sense and help your end users to do their jobs effectively. Be sure to teach them the systems and controls that you want them to use and verify that they are using them.

Don't set up policies that are so cumbersome and restrictive that your employees are pushed to private cloud options (Dropbox, Google Docs, etc) to do their jobs effectively. At the end of the day, your employees will do what they need to do to get their job done. Help them and yourself by making it simple to use the systems you can control.

Consider a policy (that is enforced) that requires all company data to be scanned, tagged, and classified, so that it is appropriately handled and backed up. By tagging and classifying corporate data, organizations can then effectively layer in other security and data protection controls that direct and contain that data within appropriate systems and with appropriate identity management and access controls. Products from AvePoint like Compliance Guardian can help not only tag and protect information, but also can scan for redundant, obsolete, and trivial information that may be removed.

06 Train, train, train your end users

Attackers don't usually infiltrate your systems by cracking some impenetrable control; they look for weak points like trusting employees. Every company has at least one person who will click on anything. Offer security awareness trainings to help employees identify signs of an attack.

Phishing is a primary starting point for ransomware infection. With more people working from home, threat actors increased their use of phishing. Email is inexpensive and easy to use, so it makes a convenient way for attackers to spread ransomware.

At the enterprise level, phishing scams are often designed to appear as though they're coming from a trusted source. For example, DocuSign issued an alert in late 2021 regarding an aggressive phishing attempt, stating, "Malicious URLs are being hidden in legitimate DocuSign envelopes. The emails are being sent from a variety of senders and associated email addresses."

The phishing email targets employees, both low-privileged users and high-privileged users. Documents are normally passed in email, so users think nothing of opening a file in an email attachment. The malicious macro runs, downloads ransomware to the local device, and then delivers its payload.

The ease of spreading ransomware in email is why it's a common malware attack. Be sure that you are proactive with your training and education. Run internal phishing campaigns and educate your employees to stop, think, and then click!

07 Establish a plan for business continuity

Perform a Business Impact Assessment on your systems to determine not only criticality of systems, but also recovery time and recovery point objectives. Keeping a full image copy of crucial systems can reduce the risk of a crashed or encrypted machine causing a crucial operational bottleneck. Don't forget to test your disaster recovery plans, so you can learn any gaps before a real-life crisis.

08 Back up your data early and often

Even with the best security training, you need to be prepared for the "one person who clicked." Prepare by backing up your data early and often. Consider primary and secondary backup locations, and ensure you are incrementally testing your backups from restore.

Products like AvePoint Cloud Backup can provide early warning signals through detection of anomaly and encryption. Cloud Backup also provides reporting that allows administrators to determine impacted scopes, which could greatly help to shorten investigation and restore time.

After an investigation has been performed, you can move into a remediation phase to restore from your last good backup. Cloud Backup provides easy-to-follow guidance with suggestions about the best time range from which to restore, which helps with faster and precise recovery from backup data.

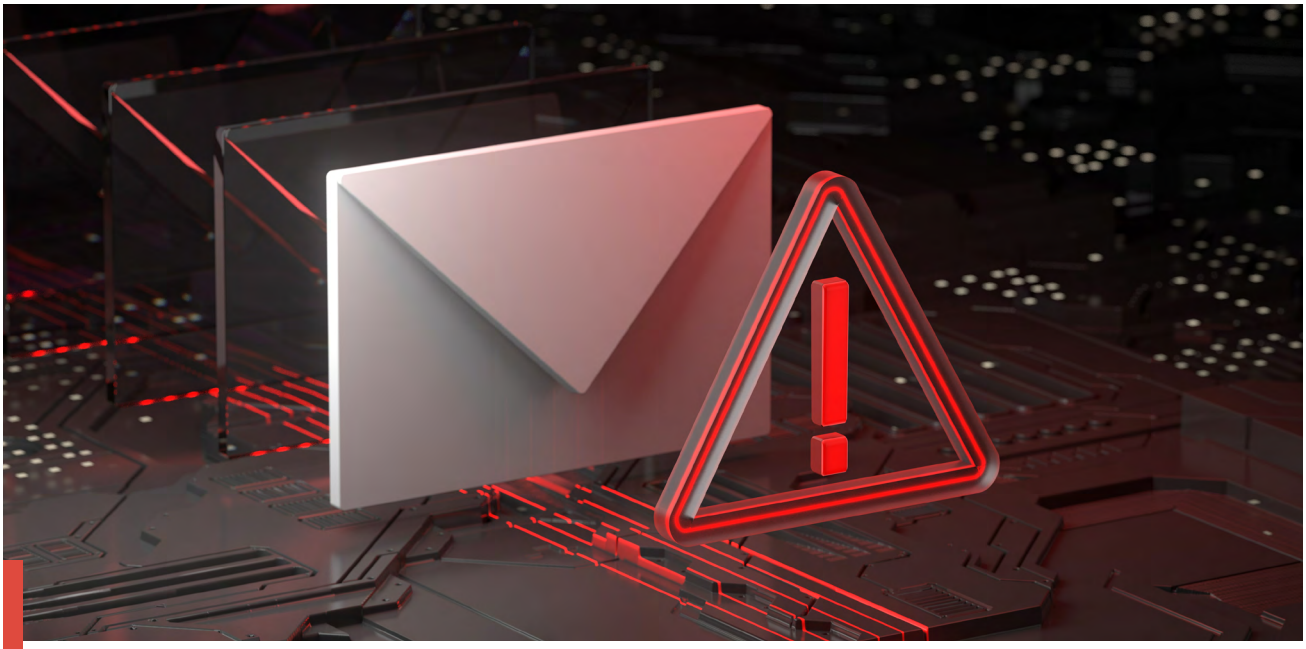
In the absence of metrics, we tend to focus on risks that are familiar or recent. Unfortunately, that means that we are often reactive rather than proactive.

Most costly breaches come from simple failures, not from attacker ingenuity. To better protect your team, you need to understand how data, people, and location weave together to create patterns - good and bad - across and within your organization. Only by understanding your employees, typical activity on your network, and the data you hold, can you effectively protect your company.

The bottom line: security is about mitigating risk. Even with all the strict security measures put in place, the risk of getting hit by ransomware attacks are never zero, and it is always better to be prepared than be complacent. When it comes to data recovery, AvePoint offers powerful data recovery options that are superior to other backup solutions.

Are YOU Ransomware Ready?

- ☐ **01** Make sure that you are running up-to-date end-point security and anti-virus software for all your emails
- ☐ **02** Implement anti-phishing campaigns and block malicious websites
- ☐ **03** Implement monitoring tools across your systems
- ☐ **04** Implement Identity Management and Least Privileged Access
- ☐ **05** Make it easier for your employees to do the right thing than the wrong thing
- ☐ **06** Train, train, train your end users
- ☐ **07** Establish a plan for business continuity
- ☐ **08** Back up your data early and often



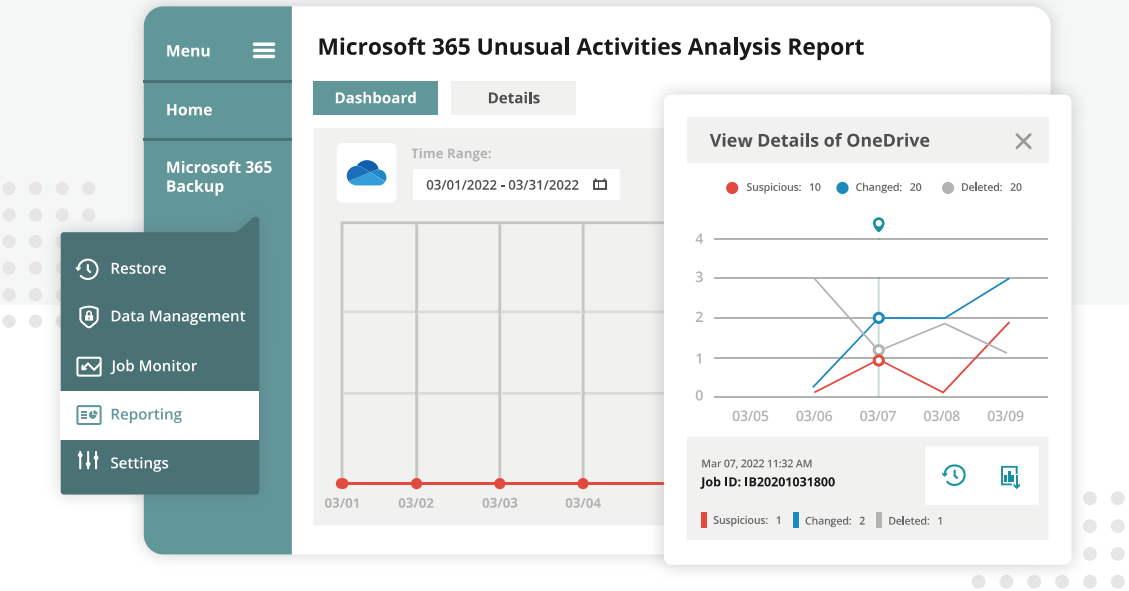
Building Ransomware Resiliency within AvePoint Cloud Backup for Microsoft 365

> “
>
> AvePoint is the **only vender** of 10 to offer strong capabilities in all three criteria of **Microsoft 365, Google & Salesforce backup**, according to Forrester.

Your line of defense

In 2021, every 11 seconds a company was hit by Ransomware - on average, it cost businesses $1.85 million to recover from an attack.

See why AvePoint was recognized as a Leader in The Forrester New WaveTM: SaaS Application Data Protection, Q4 2021. More than 8 million cloud users rely on our full suite of solutions to make them more productive, compliant and secure. Whether you've got 10 or tens of thousands of users, we've got your backup.



Early Event Detection

A function that uses machine learning algorithms to detect unusual activities as well as potential ransomware attack events. Admins can also be notified when such events are detected.

Quick Investigation

Ransomware attacks are serious security incidents. The IT and security teams need to perform incident investigation as soon as possible to have a better understanding of the impact to formulate a plan to remediate the risk.

Cloud Backup provides top-down charts/reports to help admins quickly drill into the areas of question to nail down the impacted scopes, which could greatly help shorten the investigation and restore times.

Faster Restore

After incident investigation is performed, users can then move to the remediation phase to restore data from a good backup.

Cloud Backup provides easy-to-follow guidance with hints about the time range to restore from, which helps with faster and more precise recovery from backup data.

AvePoint EMEA Headquarters
3rd Floor, Watchmaker Court
33 St John's Lane
London, EC1M 4BJ
P: +44 (0) 207 421 5199 | E: sales_uk@avepoint.com | www.avepoint.com/uk