Countering ransomware

A 3-step approach towards threat detection, **backup, and recovery**

ManageEngine
AD360

Introduction

The rise of ransomware has become a crisis that has affected organizations worldwide. As hackers develop more sophisticated strains of ransomware, there is an urgent need for organizations to revisit their anti-ransomware strategies to curb its spread. With more employees transitioning to working remotely, the threat of ransomware is greater than ever.

With ransomware attacks disrupting business operations and leading to loss of data, revenue, and reputation, IT leaders know the consequences of suffering one of these attacks are severe. In today's diverse and distributed IT environment, getting the organization up and running in the event of a ransomware attack can be a significant challenge.

Understanding the seriousness

According to a Gartner analysis on ransomware preparedness, over 90 percent of ransomware attacks were found to be preventable with well-rounded security fundamentals that help identify, detect, and respond to threats. However, it's a mistake to assume that threat detection alone will mitigate ransomware threats.

Having a secure backup of critical business data and applications allows companies to recover data as it was before the ransomware infection. The ideal backup and recovery approach should enable organizations to protect critical data and applications securely and reliably, and help recover the required data in just a few clicks so IT managers can successfully recover from a ransomware recovery without paying any ransoms.

With ransomware attacks on the rise, organizations of all sizes have found themselves vulnerable and are struggling to reduce their risk surface and respond quickly to attacks. There is an increasing need for a comprehensive solution to protect critical data and rapidly recover from attacks.

Ransomware protection and mitigation

As the monetary gains from ransomware attacks continue to rise, security leaders must revisit their enterprise security and threat response strategy. To help with getting started, here are three steps that will help organizations improve their business resiliency and reduce the impact of ransomware attacks.

- Detect early signs of threats and potential risks.
- Respond proactively to prevent contamination and threat propagation.
- Recover data rapidly with flexible recovery options.

Detect early signs and potential risks

Preventing a ransomware attack is possible when equipped with the right tools. ManageEngine's AD360, a real-time ransomware alert tool, swiftly detects and responds to ransomware attacks using mass access alerts coupled with an automated threat response system. AD360's advanced user behavior analytics (UBA) feature helps in identifying accidental or out-of-character changes made to files and folders.

Configure ransomware alerts and responses

Multiple file modifications in a short period and evidence of encryption are two tell-tale signs of a ransomware attack. With AD360's machine learning-powered threat intelligence, organizations can detect these signs of ransomware early on and identify attacks right as they happen.

AD360 is also equipped with an automated threat response mechanism, which lets administrators shut down any ransomware attack right at its inception. Administrators can also choose to be notified via email when there is an unusual process (such as mssecsvc2.0) running on a machine.

Comprehensive activity monitoring and reporting

AD360's user behavior analytics (UBA) engine creates a baseline of normal activities that are tailor-made for each user and notifies administrators when there is a deviation from this norm. This comes in handy when malicious snippets of code are executed from a user's workstation. The UBA engine can quickly recognize that something suspicious is taking place and raises an alert.

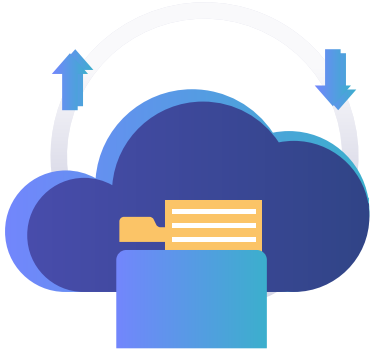
Respond proactively to prevent contamination and threat propagation

When a malicious activity such as bulk file modifications and lateral movement takes place, the administrator is working against the clock. Automation comes handy when IT admins are hard-pressed for time.

AD360 enables administrators to automate threat responses in the unfortunate case that they are subjected to a ransomware attack. Batch files and custom scripts can be invoked when the UBA engine recognizes a threat. Administrators can configure AD360 to do the following when their network is under attack:

- Shut down infected systems immediately.
- Disable all shared drives that hold critical information.
- Disconnect and isolate infected systems from the network.

Recover data rapidly with flexible recovery options



If any systems are compromised despite these safety measures, organizations can recover all the lost data from backups. The backup and the recovery module of AD360 lets administrators back up Active Directory, Exchange, and Microsoft 365 data periodically.

AD360 is built with automation in mind. Administrators can schedule their backups periodically based on their risk appetite. This way, admins won't have to second-guess if all critical data has been backed up.

Enterprise storage devices such as tapes and network-attached storage (NAS) servers are expensive. With a few organization-wide backup cycles, storage costs can quickly go over the roof.

To save storage space, AD360 lets users define the number of full backups to be retained and automatically discards all older and subsequent incremental backups.

With incremental backups, administrators can also back up just the changes made to their AD environment since the last backup cycle and store them as separate versions. User-configurable backup retention can also help businesses meet compliance regulations and other litigation holds.

Active Directory backup and recovery

The native Active Directory backup and recovery features from Microsoft are not suitable for object-level backups and attribute-level restorations. With AD360, administrators can back up and restore not only all AD objects but also other essential AD elements such as schema attributes, group membership information, and Exchange attributes. Administrators can also leverage:

- **Object-level restoration:** Restore entire AD objects to any of their previous versions instantly.
- **Attribute-level restoration:** Restore individual attributes of AD objects to any of their previous values.
- **Rollback:** Roll back your entire AD, OUs, or even individual objects to a previous backup point, and undo all changes made to objects after that point in time.
- **Version management:** Maintain each backup of an object as a separate version, and restore objects to any earlier version.

Microsoft 365 and Exchange Online backup and recovery

Microsoft 365 is a cloud solution that boasts an exceptional 99.9 percent uptime across all its services. However, that is where it draws the line. Microsoft's responsibility ends with merely hosting the infrastructure. The onus of providing data protection, disaster management, compliance requirements, and holistic backups falls on the end user.

AD360, on the other hand, eliminates the risk of losing your Microsoft 365 data, including Exchange Online, SharePoint Online, and OneDrive for Business. With AD360, administrators can:

- **Back up Exchange Online:** Back up all items in your Microsoft 365 mailboxes, Exchange, and SharePoint Teams, including emails, calendar entries, contacts, journals, notes, posts, and tasks. Export an entire mailbox or just a part of it to PST format.

- **Restore Exchange Online mailboxes:** Back up all items in your Microsoft 365 mailboxes such as emails, calendar entries, contacts, journals, notes, posts, and tasks.
- **Restore to different mailboxes:** Schedule periodic backups and incrementally back up just the changes made to mailboxes and sites since the last backup cycle.
- **Restoration preview:** Define a retention period for your Microsoft 365 backups, and automatically discard older backups.

Conclusion

The impact that ransomware attacks have on organizations is expansive. However, with the right threat detection and recovery solutions, the risks can be mitigated. ManageEngine AD360 helps organizations detect, respond to, and recover from ransomware effectively. AD360 enables IT leaders to ensure that their organization has a multi-layer defense plan in place to reduce the impact of ransomware.