

Ransomware

Prevention and Response Checklist





Ransomware prevention checklist

Preventive measures at the user level

- Conduct security awareness training and educate your end users about ransomware attacks.
- Train your end users to spot and report phishing emails containing malicious attachments.

Preventive measures at the software level

- Ensure your firewalls are operational and up-to-date at all times.
- Logically separate your networks.
- Employ a strong email filtering system to block spam and phishing emails.
- Patch vulnerabilities and keep all your software updated.
- Set up rigorous software restriction policies to block unauthorized programs from running.
- Keep your antivirus fully operational and up-to-date.
- Conduct periodic security assessments to identify security vulnerabilities.
- Enforce the principle of least privilege.
- Disable Remote Desktop Protocol (RDP) when not in use.
- Disable macros in your Microsoft Office files.
- Use a strong, real-time intrusion detection system to spot potential ransomware attacks.

Preventive measures at the backup level

- Back up your files using a 3-2-1 backup rule, i.e. retain at least three separate copies of data on two different storage types, with at least one of those stored offline.
- Ensure that you back up critical work data periodically.
- Enforce regular checks for data integrity and recovery on all your backups.



Ransomware response checklist

Time-sensitive reactive measures

- Shut down infected systems immediately.
- Disconnect and isolate infected systems from the network.
- Isolate your backups immediately.
- Disable all shared drives that hold critical information.
- Issue an organization-wide alert about the attack.
- Contact your local law enforcement agency and report the attack.

Analysis-based reactive measures

- Determine the scope and magnitude of an infection by identifying the type and number of devices infected, as well as what kind of data was encrypted.
- Determine the type and version of the ransomware.
- Identify the threat vector used to infiltrate your network.
- Conduct root cause analysis.
- Mitigate any identified vulnerabilities.
- Check if a decryption tool is available online.

Business continuity reactive measures

- Restore your files from a backup.

Additional resources



Step-by-step guide to detect and respond to ransomware attacks.

[Know more >](#)



8 best practices to prevent future ransomware attacks.

[Know more >](#)



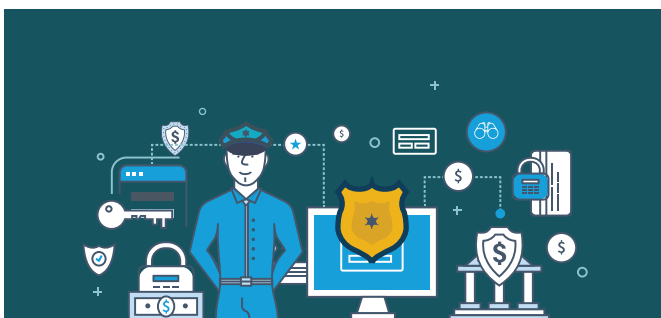
Infographic on HIPPA guidelines on ransomware attacks.

[Know more >](#)



Infographic on how to protect your organization from ransomware attacks.

[Know more >](#)



Ebook FBI recommendations to prevent ransomware attacks

[Know more >](#)

DataSecurity Plus

ManageEngine DataSecurity Plus is a data visibility and security solution. It tracks and alerts on critical file modifications and movement across file servers, failover clusters, workstations, and USBs. Users can locate and analyze files containing PII/ePHI stored in Windows file servers, failover clusters, and OneDrive environments using built-in data discovery rules. Its data leak prevention (DLP) capability helps detect and respond to the exfiltration of sensitive data via USBs, email, printers, and more. It also provides detailed audit reports that help organizations streamline compliance with multiple IT regulations.

To explore these features and see DataSecurity Plus in action, [launch the online demo](#).

To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

↓ Download free trial

\$ Get a quote

Explore DataSecurity Plus' solutions



File server auditing

Audit, monitor, report on, and alert on all file accesses and modifications made in your file server environment in real-time.

[Learn more](#)



Data leak prevention

Detect, disrupt, and respond to sensitive data leaks via USB devices, emails, printers, and more through real time security monitoring.

[Learn more](#)



Data risk assessment

Perform content inspection and contextual analysis to discover sensitive data in files, and classify it based on vulnerability.

[Learn more](#)