ManageEngine
DataSecurity Plus

Ransomware
Prevention and Response Checklist

www.datasecurityplus.com

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 unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore **DataSecurity Plus' capabilities**

File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more