How businesses can best defend against Ransomware attacks

IP-guard's proactive strategies to protect sensitive information against Ransomware

> "Ransomware damages a corporation's reputation, interrupts operations in a costly manner, and often causes data loss."

- Basic Management
- Application Management
- IT Asset Management
- Device Management
- Email Management
- Bandwidth Management
- Document Management
- IM Management
- Print Management
- Removable Storage Management
- Screen Monitoring
- Website Management
- Network Management
- Remote Maintenance

Please note:
Comprising of 14 modules, IP-guard is able to meet diverse management needs. Modules can be optionally selected (minimum: Basic Management Module + any 2 other modules) and repackaged depending on the specific organisation's management requirements.

Steps To Defend Against Ransomware Attacks

1 Install reputable anti-virus across all corporate devices

As a first line of defense, ensure anti-virus is installed and up-to-date across all endpoints within the corporation to prevent known threats from entering the environment.
Do note, however, that anti-virus software is based on "signatures" (which is like an ID number for a virus), so new virus variants will likely slip through the cracks

2 Establish security awareness organisation-wide

Ransomware can come from emails or links within emails. To reduce the chance of ransomware entering the environment through social engineering attacks, such as email phishing, it is important that users to ask themselves the following questions before clicking on unknown links or opening attachments in emails:

A. Do I know the sender?
B. Am I expecting something from this company?
C. Do I need to open the file or go to this link?

IP-guard's website management module can create a "white list" (safe list) of websites to ensure that end-users do not access unknown, and potentially malicious, websites.

3 Back-up important data frequently

While the first versions of ransomware aimed to simply encrypt the victim's local hard-drive and demand a financial payment to unlock the drive, the latest evolutions are now encrypting network drives as well.

IP-guard's document management module is uniquely designed. Unlike other backup solutions, our system does not require network drive mapping to a back-up document, which means that ransomware attacks on network drives do not affect backup drives.

4 Patch regularly

Many ransomware attacks occur via the vulnerabilities of Windows Software and 3rd party software. It is important to keep software "patches" (software updates) up-to-date in order to minimise the likelihood of ransomware attacks.

IP-guard's asset management provides a comprehensive feature, including Windows updates and software deployment that assists system administrators to distribute software patches in the easiest way and shortest time.

5 Encrypt documents

An excellent way to protect your business from ransomware is by implementing file-level encryption. This is a type of encryption where the default file system itself (such as Windows on Microsoft) encrypts individual files and/or directories on the device.

IP-guard V+'s transparent encryption approach encrypts documents during the save/close phase of a document. It provides a seamless migration for the end-user from their current operations to the encrypted environment.

6 Restrict ransomware, malware from installing

Restrictions on software installation could be one of the easiest and most affordable methods of preventing ransomware and malware from entering the corporate environment.

IP-guard's application management module can restrict new applications being installed on endpoints (such as computers) and also provide granular control over executable files residing on the endpoint computers, such as blocking a file from executing or running from the "AppData" directory.