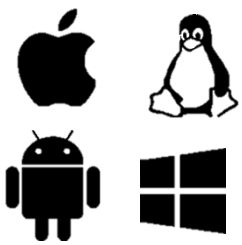
RANSOMWARE

BACKUP: THE LAST LINE OF DEFENSE

Ransomware is a type of malware that targets vulnerable servers, desktops and end point devices including Windows, Mac, Linux and Android. Once infected, the ransomware will systematically encrypt files visible on the hard drive, direct attached storage, and network shares. A notification will offer a key to decrypt the files for a ransom fee. Without the decryption key the user will be unable to unlock the files.

What?

Systems



How?

Unpatched

Vulnerabilities

Why?

Phishing

Malicious Email & Ads

Best Practices Against Ransomware

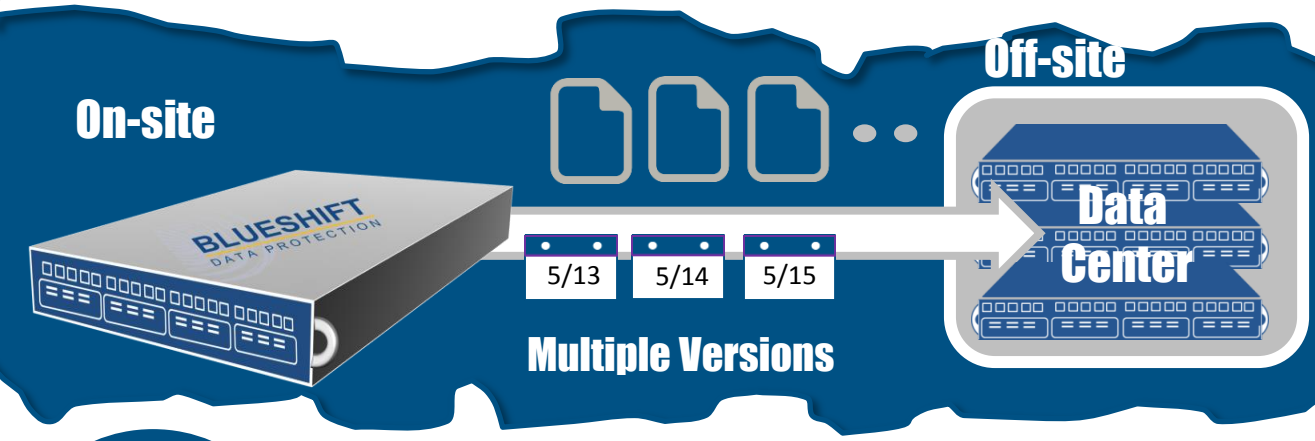
1 BACKUP Your Data

No backup, no protection! In any disaster, as long as you have a backup you can restore to a fresh install.

2 Redundancy

On-site & Off-site Backups

Multiple versions stored on-site & off-site can insure data recovery even if the malware is dormant for some time.



3 Isolate Your Backups

Backups stored on network shares, mapped/unmapped drives, direct attached storage (DAS) and network attached storage (NAS) can all be exposed to Ransomware.

4 Test Backups

Regular testing and disaster recovery drills is essential to insuring data is recoverable.

5 Organize

Know where license keys, passwords and CD-ROMS are for a timely recovery.

Backup → Redundancy → Isolate → Test → Organize

BLUESHIFT
DATA PROTECTION

www.dataprotection.jp