How to protect your organization from

# RANSOMWARE

Ransomware is a sophisticated class of malware that holds your data hostage until a ransom is paid.

## Prevention

- Back up your files
- Patch vulnerabilities
- Employ email filtering
- Provide the least amount of privilege possible
- Educate end users
- Whitelist applications

## Detection

- Use a robust, real-time ransomware alert tool to flag malware invasions.
- Learn the telltale signs of a malware attack, such as files being accessed, renamed, deleted, or encrypted in mass.

## Sequestration

- Use a preconfigured, automated ransomware detection tool to instantaneously detect and kill threats.
- Shut down infected systems and isolate them from the network to protect your other file servers.

## Restoration

- Before recovering your files from a backup, ensure that the malware has been cleared from your organization completely.
- View forensic details on the ransomware attack—such as who did what and from where—to identify the source of the threat and prevent future breaches.

## To pay or not to pay?

- If your organization experiences a ransomware attack, never pay the ransom; there is no such thing as honor among thieves.
- According to **Kaspersky's Security Bulletin 2016**, one in five companies who pay the ransom never get their data back
- Visit nomoreransom.org to report cyber crimes and check out the ransomware decryption tools available.