5 STEPS TO HELP DEFEND AGAINST INSIDER THREATS

1. EDUCATE YOUR USERS

- Don't give out your username or password
- Don't leave your laptop unattended in public places
- Don't leave your computer or terminal unlocked when you step away - even in the office
- Don't click on links in external emails - in fact, be wary of any emails from outside your organisation
- Be careful what and from which sites you download from the internet

2. SET PERMISSIONS & POLICIES

IT Departments must define structured access permissions based on job roles or seniority. This relates to both applications and data - especially customer details and financial records

3. FIX ENDPOINT PROTECTION

Install endpoint protection including anti-virus software packages that defend against phishing, malware and ransomware. Make sure your Firewall is up and running

4. MAINTAIN APPS AND OS

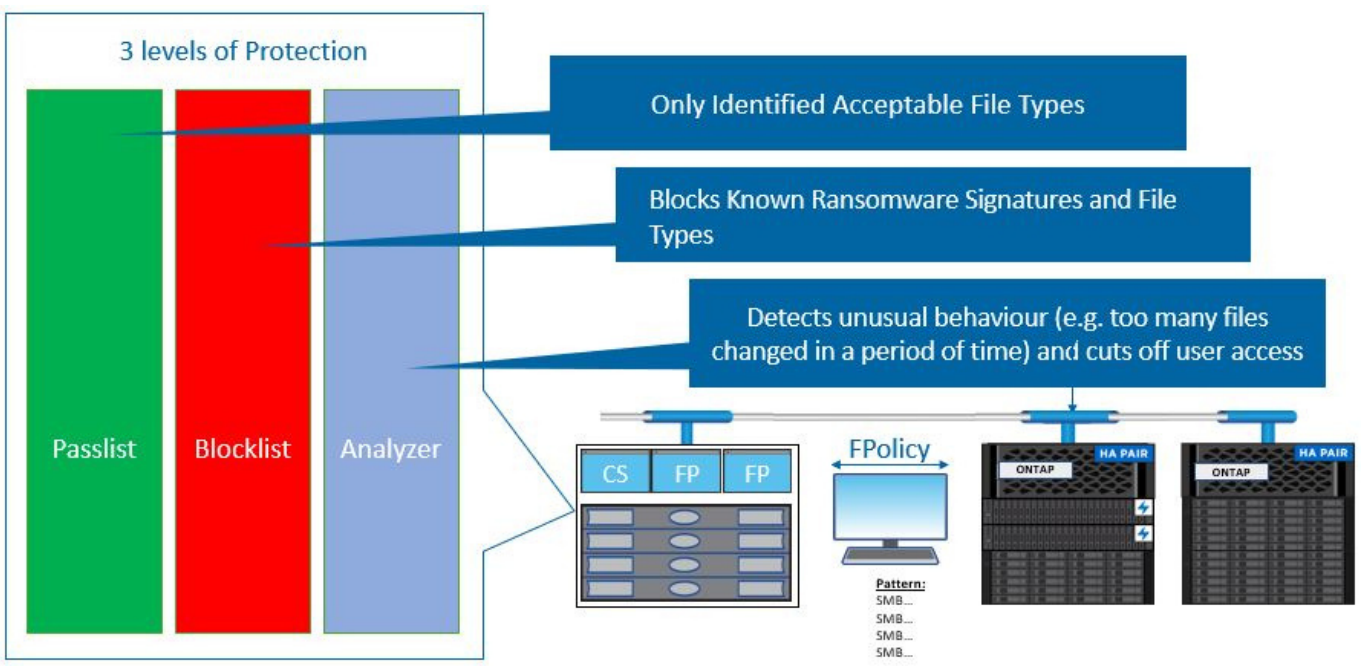
Make sure your Operating Systems and 3rd party applications are up-to-date. Many of these apps have updates that defend against known threats and correct vulnerabilities from earlier versions

5. ENABLE DATA TRANSPARENCY

Install software that monitors and logs all user file access (reads, writes, opens) and can identify when changes were made and from which IP address. Should an infection or abnormal behaviour be suspected, the user's access is blocked, and no further damage can be done.

PROLION CRYPTOSPIKE

ProLion CryptoSpike incorporates a passlist, a blocklist and an analyzer that monitors your file system alongside the other defences



ProLion www.prolion.com