Business CYBERSECURITY Menu

RELIABLE

FAST

CERTIFIED

PRIORITY 1
TECHNOLOGY SOLUTIONS

OUR CYBERSECURITY PACKAGES

BASIC

$120 /Site /Month (Up to 10 computers)

- Next Generation Antivirus
- Server 2FA Controls and Security
- 365 2FA Email Monitoring
- 365 Advanced Security - Conditional Access
- Basic patch management and deployment

ESSENTIALS

$250 /Site /Month (Up to 10 computers)

Everything in Basic PLUS

- 24/7 Professional Security Operations Centre Monitoring
- Application Control
- Adanced security event logging
- Dark web credential monitoring
- Automated backup recoverability testing

ADVANCED

$350 /Site /Month (Up to 10 computers)

Everything in Essentials PLUS

- Advanced ransomware monitoring
- Hacker persistence monitoring
- Full systems SIEM collection and analysis
- Monthly vulnerability scanning
- Manual backup recoverability testing

Got more than 10 computers? Our security package licensing comes in packs of 10, you might need two or more packs to cover your business.

GOT CYBER INSURANCE?

If you have not met the minimum requirements for security, your cyber insurance may not cover you after a cybersecurity event or breach. You must take every reasonable measure, even if you're insured.

SOME OF OUR CYBERSECURITY SERVICES

NEXT GEN ANTIVIRUS
Next-gen antivirus solutions use AI (Artificial Intelligence) to detect and neutralise threats. Virus definitions are generated live, without needing to perform constant updates.

365 SECURITY
Microsoft office 365 is inherently a highly secure platform, however people suffer hacking and breaches every day. The 365 platform needs to be configured with appropriate security controls and monitoring.

BACKUPS
Backups are essential for mitigating ransomware risk. A backup solution must be implemented and checked to ensure it is restorable and isolated from any ransomware event.

APPLICATION CONTROL
Restricting administrative access to all systems and controlling what applications are accessed and installed is critical for security.

MULTIFACTOR AUTHENTICATION
All remote or internet-facing websites, servers, computers or devices should have strong multifactor authentication to prevent phishing and brute-force hacking attempts.

VULNERABILITY SCANNING
Vulnerability scanning is a highly effective way of remaining secure. Vulnerability scans test your entire network and provide a security report and list of actions to further secure your systems.

24/7 SECURITY OPERATIONS CENTRE
24/7 monitoring is critical for security. Hackers and other threats do not rest, and neither should your protection. The security operations centre monitors for abnormalities, and when detected, abnormal activities are reviewed by a security engineer.

PERSISTENCE MONITORING
After a security breach, a bad actor or hacker may not take any malicious action. Instead, they may place a back door or method of accessing the systems so they can complete the attack at a later time. Software monitoring for these persistence methods is essential.

DARK WEB CREDENTIAL MONITORING
Breached credentials are often sold on the dark web. Dark web monitoring checks the dark web for your username notifies of a breach so you can change your password.

PATCH MANAGEMENT
New vulnerabilities are discovered in software and operating systems every day. Security patches and updates must be swiftly managed and deployed to prevent a breach.

Got more than 10 computers? Our security package licensing comes in packs of 10, you might need two or more packs to cover your business.

GET IN TOUCH TODAY

helpdesk@p1it.com.au

1800 931 269

19/489-491 South Street, Harristown Queensland 4350

www.p1it.com.au