Cybersecurity Protection Package

FAIRDINKUM
LEVERAGING INNOVATION WITH TECHNOLOGY

No matter your organization's size, protecting your users and devices from potential threats, both internally and externally, is an ever-growing concern.

With the ever-changing landscape of cyber threats, you'll want to be protected from current and future malicious attempts on your network, whether your organization is utilizing on-premise systems or cloud hosted environments.

At Fairdinkum our priority is providing technologies that will combat these threats as well as provide a strong outward facing organizational security profile to your partners, clients or investors.

Our cybersecurity package was created by curating the top-tier tools and services already vetted by our team and thoroughly researched and tested based on sources such as NIST, SOX, Cyber Insurance audits and regulatory agency requirements.

Finally, this package was created to scale easily to meet the security needs of organizations of all sizes and verticals.

Tools & Services

Multi-Factor Authentication	✓
Hard Drive Encryption	✓
Hosted Email Protection	✓
Security Training	✓
Ransomware Protection	✓
Active Directory / Azure Monitoring	✓
Heuristic Monitoring	✓
External Party Data Breach Monitoring	✓
Log Aggregation	✓
Vulnerability Scans	✓
Phishing Test	✓
Password Vulnerability Testing	✓
Firewall Realtime Threat Blocking	✓
Persistent Foothold Protection	✓

Multi-Factor Authentication
A username and password combination alone are no longer secure. Exclusively using simple username and password protection on Internet facing portals, such as Webmail, VPN or Remote Desktop, can allow hackers to gain access via weak or stolen user passwords. Multi-factor authentication (MFA) is a two-step verification process that adds an extra level of protection by requiring authorization via a mobile device or physical key fob. MFA can also be utilized to better secure access to physical workstations and devices.

Hard Drive Encryption
Remote computing has many advantages; however, it puts data at risk if a laptop is lost or stolen. Even with a password protected device, laptop hard drives can have their data read and stolen with little effort. By utilizing hard disk encryption, all data on a laptop hard drive is protected from extraction by an unwanted party.

Hosted Email Protection
Although not always recognized, cloud hosted systems do require attention in order to configure and monitor enhanced protection services. Our cybersecurity package allows for these configurations and monitoring. Typical monitors implemented are Geo-fencing which alerts users or monitors to access gained to accounts from unexpected geographic locations which may indicate a breach of a user's account as well as impossible travel, which combines geo-fencing with logins that originate from different locations within a timeframe that is not possible. There are various similar protections implemented via this service.

Security Training

In order to increase employee awareness against cyber security threats and social engineering attacks, management must provide training to users. Security training via interactive web modules provides the necessary tools to ensure compliance with policies and procedures. Security courses can be customized, and progress can be tracked to ensure all employees have the appropriate knowledge to assess and mitigate cyber threats.

Ransomware Protection

Ransomware is a form of malware that encrypts all local and network files and prohibits access to this data. Recovery can only be performed by a restore of data from backup. In severe cases when a ransom must be paid, recovery is not always guaranteed. Active protection against ransomware will minimize outbreaks and reduce/eliminate damage. Our cybersecurity package utilizes multiple points of protection such as canary file monitoring which monitors specific local files for any modifications. When these files are disturbed, it will trigger a full lockdown of the affected device that will protect other devices on the network. Our engineers will still maintain secure access to the affected device to allow for remediation of the incident. Beyond this, our package utilizes custom monitoring for known ransomware indicators such as file types and behavior.

Active Directory / Azure Monitoring

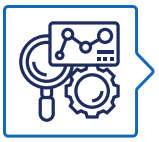
Active Directory and Azure AD administrator accounts should be kept to a bare minimum. With active domain monitoring, alerts will be generated any time an account is added to an administrative group, whether intentional or malicious.

Heuristic Monitoring

Traditional antivirus relies on known malicious code, file names and other known parameters to identify and isolate threats. Heuristic monitoring takes this protection further by performing analysis on application activity to determine if an application is a potential threat and requires remediation. This type of monitoring is essential to protect against zero-day threats.

External Party Data Breach Monitoring

More than 14.7 billion data records have been lost or stolen since 2013 due to data breaches. This data includes account passwords and logon information. Actively monitoring these large data breaches will identify which employee accounts have been.

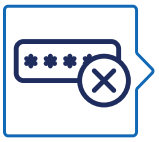


Log Aggregation

All network devices and servers generate diagnostic and informational logs for all events that occur. These logs are generally hard to review because they exist in many locations on several different platform types. With log aggregation, a centralized device captures all logs generated by accepted systems and places them into a single container which can then be used to automate alerts based on specific events. This process allows for greater speed to response when the first signs of trouble begin to appear.

Firewall Realtime Threat Blocking

The first line of defense in protecting your organization's external presence is your firewall. Realtime threat blocking enhances firewall protection capabilities by performing continuous monitoring of all attempted connections to your firewall. These connections are then analyzed via a proprietary algorithm and identified threats are autonomously blocked.



Password Vulnerability Testing

Weak passwords are easily compromised via brute force and dictionary attacks. Periodic hash testing against all accounts will expose weak passwords and output reports on which passwords are in danger of potential decryption and should be immediately changed.

Vulnerability Scans

Exploitations in firmware, configurations and software are a common occurrence in today's technology. These exploits can make any organization a target both from internal and external cyber-attacks. Continuous automated vulnerability scans will verify the security of all servers, network devices, workstations and laptops within the organization for remote or on-premise users. The scans are run on a continuous basis to check devices for any known exploits. From the scans, a report is created identifying potential risks. Once identified, these risks can be addressed.

Phishing Test

91% of successful data breaches start with a spear phishing attack. The best defense for these attacks is to raise employee awareness and improve their security behavior. "Disguised" phishing emails sent to all users on a quarterly basis will output to a report outlining which users are most susceptible to attacks.

Persistent Foothold Protection

To evade detection, attackers are abusing legitimate applications and processes to slip through the network undetected. Once inside, they establish a quiet foothold and plan their next move, often the deployment of malware to cripple systems, or ransomware to encrypt and steal sensitive data. Our service detects these persistence mechanisms to identify and eliminate persistent actors who are dwelling in your environments through unauthorized access.

FAIRDINKUM

LEVERAGING INNOVATION WITH TECHNOLOGY

15 E 32nd Street, 9th Floor, New York, NY, 10016 • 212.624.3200 • fairdinkum.com