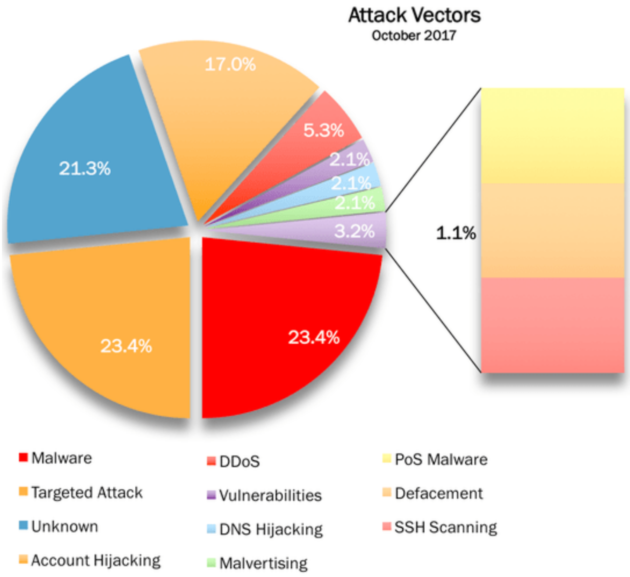
Brace for Cyber Security 24 x 7

B Protected

Managed Security Protection Service

Security threats stem from both external and internal sources, external sources being the most malicious in nature but with the least likelihood of occurring. In today's digital world, neither is more important than the other, organisations need to secure themselves for the potential threat of both. B Protected focuses on an organisations "outside in" security protection securing data in motion in and out of the network. The external threats, come in two main forms, targeted attacks, such as DDoS and exploiting available vulnerabilities, and non-targeted such as script kiddies and random port scans looking for exploits.

Protecting your publicly available systems from external attacks is the foundation of the "B Protected" product suite. Ensuring the confidentiality, integrity and availability is critical if you provide services of any kind via the Internet.



Examples of external threats:

- Internet-borne threats
- Not all known – in the wild threats
- User targeted – i.e. phishing attack
- System targeted – i.e. DDoS

Simple measures like installing additional layers of security and enforcing smart, data security conscious policies – such as a ban on users sending corporate data to external personal accounts – can make a big difference when it comes to safeguarding information.

Protect Against Data Leakage

The Brace168 Managed Visibility Service includes:

Cloud Access Security Broker (CASB)

Our CASB service sits between your on-premises infrastructure and a cloud provider's infrastructure. We act as a gatekeeper, allowing you to extend the reach of your security policies beyond your own infrastructure to that of cloud services.

Intrusion Detection System (IDS)

Having an Intrusion Detection System in place is crucial to stopping data leakage. An IDS is a device or software that monitors systems and networks for security threats, both internally and externally. The IDS system sends alerts when it detects potential malicious activity.

Domain Name System (DNS)

It's important not to just prevent against possible threats, but to detect, using sophisticated means such as algorithmic DNS pattern-matching to detect threats that may or may not be known.

Authentication (SSO)

Single Sign-On mechanisms, while convenient, carry significant risks. A "keys to the castle" approach widens the scope of information that becomes vulnerable should a leak occur. Increased focus should be given to the protection and authentication of user credentials, for example, with smart cards or one-time pins.

How we can help

Having 24 x 7 oversight on your environment for security threats, not only gives you peace of mind, but ensures the uptime and availability of your critical assets. This in turn gives you the confidence that you're complying with the government's new data breach regulations.

Brace168

Call today on (02) 8315 2870 to find out more or visit www.brace168.com.au

Source: OAIC Notifiable Data Breaches Quarterly Statistics Report: January 2018 – March 2018