

Security Stack

In 2019, you need more than anti-virus to protect your computer. We believe you need a "Stack" of layers.

Our Security Stack moves our customers towards compliance with the "Essential Eight" - a list of the 8 most effective strategies to mitigate cyber security incidents as defined by the Australian Cyber Security Centre.

It is expected that by complying with these 8 things the vast majority of security events will be prevented or significantly mitigated.

The Essential Eight

6 Items Addressed by Security Stack

Application Whitelisting - prevent installation of unapproved software. Prevent execution of unapproved software in user space.

Patch Applications - an automated system is used to confirm and deploy application updates.

Microsoft Office hardening - Microsoft Office macros are secured.

User application hardening - Disable autorun. Disable UPnP. Disable OLE in Office. Enforce User Access Control.

Restrict Administrative privileges - run as a non-admin user wherever possible. Lockdown administrative tools if you can't. Don't use privileged accounts for email and web.

Patch Operating Systems / - an automatic system is used to patch security and other critical patches for supported operating systems.

NOT Covered by Security Stack (but available)

May need a license to protect remote access

Multi-Factor Authentication - protect everything possible.

Requires backup license and setup

Great Backups - at least daily, retained for at least three months.

Additional features of Security Stack

Managed Anti-virus system – infections checked and remediated daily*

Manage DNS security - A cloud based security system sitting between your computers and the Internet. The principle purpose is to prevent your systems from communicating with known "bad" or infected sites on the Internet. This can also be used to manage access to web sites or categories of web sites for example blocking social media.

Disclaimer

* Note that this Security Stack is provided to attempt to prevent any infection of malware / ransomware / virus. In the case of infection, automated tools will attempt to contain and remedy the infection. If these tools cannot solve the issue, manual remediation of infection, due to unpredictable scope and effect, is out of the scope of this agreement. We will take action as deemed necessary and contact you as soon as possible.

Products Used

Anti-Virus - Webroot

DNS Security - Cisco Umbrella

Maintenance System - Manage

Lockdown (Windows only)

Software Update System - Ninite Pro (Windows only)

HIT Code: A201