If it's not in the whitelist, it can't run!

Delta AWaaS

Managed Application Whitelisting as a Service.

DELTA APPLICATION WHITELISTING AS A SERVICE STOPS MALICIOUS EXECUTABLES IN THEIR TRACKS.

Application whitelisting is designed to prevent malicious software or unauthorised applications from executing on a system. Put simply, it isn’ t authorised to run—it won’ t run. Period! Application whitelisting is NOT signature or heuristic based anti-virus. It is the opposite.

Delta Managed Application Whitelisting as a Service removes the complexity from traditional implementations of whitelisting, whilst offering industry leading protection from targeted cyber intrusions.

Managed end to end with 24/7 x 365 days a year coverage, Delta AWaaS offers the best protection from Ransomware and other malicious software on the market.

PROTECTION FROM TARGETED CYBER THREATS

Ransomware is one of the fastest growing and most effective money making criminal activities in cybercrime today. If infected, you have three choices – pay a ransom for your data, restore from backups or lose it all. Either way, it costs you both considerable time and money, if not total destruction of your business.

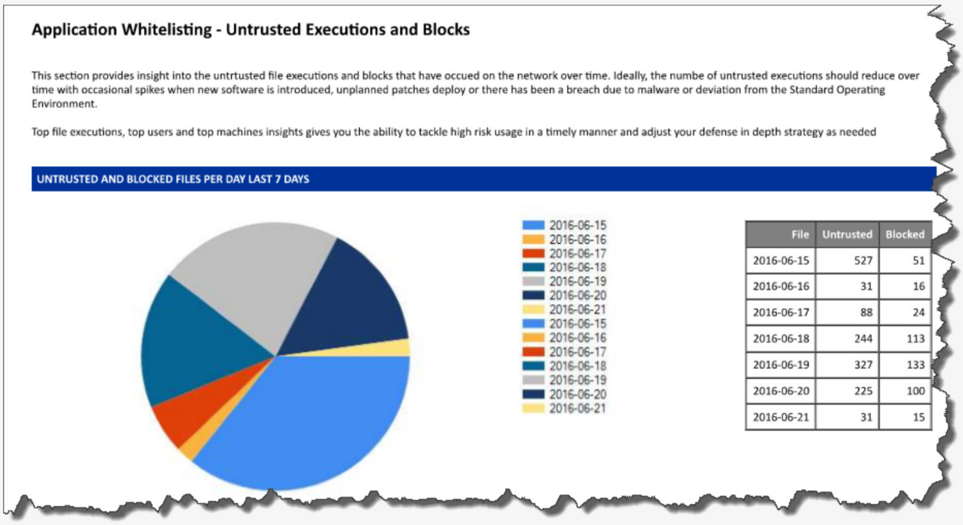
Application whitelisting is designed to prevent malicious software or unauthorized applications from executing. If it isn’ t authorized to run – it won’ t run – period!’

APPLICATION WHITELISTING:

is **NOT** signature or heuristic based anti-virus (block listing). In fact, it is quite the opposite. Only files you allow to run, run. Anything else, good, bad or indifferent will not be able to execute on machines protected by Application Whitelisting.

MANAGED APPLICATION WHITELISTING:

gives you all the benefits of the most effective strategy to mitigate targeted cyber intrusions, while removing the burden of configuration, management and maintenance.



Application Whitelisting - Untrusted Executions and Blocks

This section provides insight into the untrtusted file executions and blocks that have occued on the network over time. Ideally, the numbe of untrusted executions should reduce over time with occasional spikes when new software is introduced, unplanned patches deploy or there has been a breach due to malware or deviation from the Standard Operating Environment.

Top file executions, top users and top machines insights gives you the ability to tackle high risk usage in a timely manner and adjust your defense in depth strategy as needed

UNTRUSTED AND BLOCKED FILES PER DAY LAST 7 DAYS

File	Untrusted	Blocked
2016-06-15	527	51
2016-06-16	31	16
2016-06-17	88	24
2016-06-18	244	113
2016-06-19	327	133
2016-06-20	225	100
2016-06-21	31	15

Application Whitelisting is:

The number one Mitigation Strategy for Targeted Cyber Threats according to the Australian Signals Directorate.

Included on the New Zealand Information Security Manual as one of the mitigation strategies for targeted cyber threats.

Is number 10 on the Canadian Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information rankings.

Is CSC2 in the Critical Security Controls for Effective Cyber Defense SANS Top 20.

The Delta Impact:

Reduces cost for upfront investment, by lowering price, and removing administrative overheads and ongoing system configuration and maintenance.

SYSTEM REQUIREMENTS FOR ENDPOINTS

Item	Specification
Operating System	Windows XP SP3, Vista, 7, 8, 8.1 and 10; Windows Server 2003, 2008, 2008R2, 2012, 2012R2, 2016; (all platforms include 32bit and 64bit support).
Network	Network connectivity to server on port 443 (TCP)

Delta AWaaS is fully hosted in secure Delta data centres. 24/7 monitoring of Delta systems provides you maximum uptime and peace of mind.

FEATURES AT A GLANCE

Baseline building to capture your normal operating environment.	**Application Captures** to enable new applications to be added to your solutions set.	**One time PADs,** allow ad hoc installation of one off Applications.	**Audit mode** to capture what' s normal and identify what' s not.
Enforcement mode to enforce whitelist policies and block everything else.	**Management Reports** for high level view of the state of application usage.	**Detailed Reporting** showing all untrusted executions on a network.	View **Network connections** being made by applications.
Hash based . Each individual executable is trusted, not entire applications.	**Publisher Trusts** allow you to trust all files from known and verified publishers.	**Granular Path Exclusions** allows path exclusions from whitelist enforcement.	**Bulk Adds** to Application captures making whitelist maintenance a breeze.
Uses a **5MB agent,** with next to zero impact on endpoint resources.	**Monitored 24/7 x 365 days per year**	**Check files** against known malicious hashes to aid decision making	Enhancements available though **Delta imanager**

tel: +64 7 5740997

www.deltatsl.com

DELTA
TECHNOLOGY SOLUTIONS