apex
Computing Services

Apex Zero Trust

Only allow approved software to run on your company devices using application whitelisting, ringfencing, and endpoint control

What is Apex Zero Trust

Apex Zero Trust provides a robust Zero Trust security approach, focusing on application whitelisting, ringfencing, and endpoint control. This ensures that only approved applications can run on your network and prevents unauthorized access to critical data, minimising the risk of malware and ransomware attacks.

How does Apex Zero Trust Work

- **To stop unauthorised applications from running on your machines and servers.**
- **To stop ransomware from being able to run.**
- **To stop shadow IT.**

The need for application whitelisting. Businesses face increasing threats from malware, ransomware, and unauthorised access, putting sensitive data at risk. Traditional antivirus and security solutions often fail to fully protect against sophisticated attacks, especially zero-day exploits, insider threats, and unauthorised application installations.

The Importance of Apex Zero Trust

As cyberattacks become more sophisticated, relying solely on traditional security measures is no longer sufficient. A Zero Trust approach actively blocks any unapproved applications or suspicious activity, protecting sensitive data, reducing the attack surface, and ensuring compliance with industry security standards. It is a proactive defence mechanism rather than reactive, making it essential for modern IT environments.

The Outcome

With Apex Zero Trust in place, businesses will have a stronger, more resilient defence against cyber threats. This results in fewer breaches, reduced downtime, and enhanced protection for critical business data. Customers can focus on growing their business, knowing that their IT infrastructure is secure from unauthorised access and potential ransomware attacks.

What This Product Does: ✓

Application Whitelisting: Ensures only authorised applications are allowed to run.

Ringfencing: Protects and isolates applications to prevent unauthorised data access.

Storage Control: Limits access to sensitive data on USB drives and external storage devices.

Endpoint Security: Enforces strict policies on all endpoints, enhancing overall security.

Real-Time Protection: Monitors and blocks unauthorised applications or actions in real-time.

What This Product Doesn't Do: ✗

Does not replace a full antivirus solution: Apex Zero Trust is an additional layer of security and should work alongside traditional antivirus systems.

No email filtering: Apex Zero Trust does not filter or manage email security.

Does not perform data backup: Backup solutions are still needed to protect against data loss.

Not a replacement for user training: Employee awareness and training remain essential for a full security posture.

Does not provide network monitoring or intrusion detection: It focuses on endpoint and application control, not on network-wide monitoring.

Security

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk