Legacy vs Next Generation Protection.

Legacy solutions can’t keep up Its as simple as that!

82 % of SMEs that experienced a cyber attack say it completely evaded their existing cyber security solutions and AV and Malware.

For example, existing AV and Malware examine signature files before they run not once it’s been activated.

The latest threats do not match the existing legacy database codes, or a compressed polymorphic malware, file less threats, compressed codes and malicious zero-day documents these have no chance of being detected by your existing solutions without our help!

Existing AV and malware look at code before its executed not whilst its running changing or during an application for malicious behaviour.

Legacy solutions don’t monitor your infrastructure constantly to ensure complete protection. With behavioural AI monitoring, change monitoring and management, built in quarantine and kill features that far surpasses existing solutions deployed today you’re in safe hands.

Our detection and response solutions offer rollback properties that takes your network back to a time before the attack happened, making our solution an essential part of any disaster recovery strategy and a great defence especially against ransom ware.