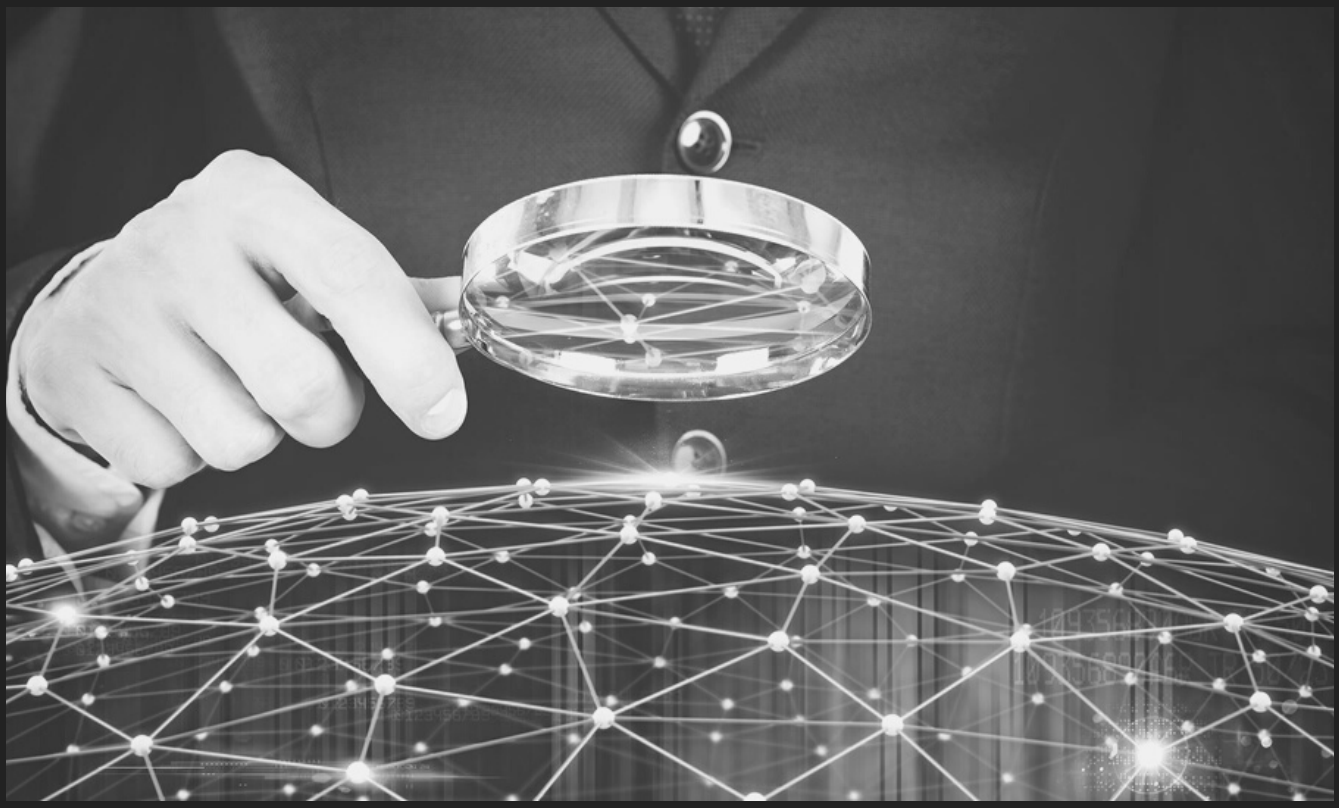
SENTINEL
by WATCHTOWER365

SENTINEL

BE AWARE. BE SECURE

SENTINEL

In a post-perimeter world, organisations must rely on Managed Endpoint Detection and Response (MEDR) as a service from a managed security service provider to provide the first line of defence against a cyberattack. Yet, existing solutions require advanced expertise and time to use effectively. Modern EDR that is built for speed for organisations of all sizes that value simplicity and efficiency.



EXPERIENCE THE ADVANTAGES

Deploy Fast. Manage Simply.
This service was built for speed - Organisations with scarce security resources achieve active response and a strong security posture in minutes.

Suspicious Activity Monitoring
This service monitors endpoints, creating a “haystack“ in the cloud where a combination of behavioural analysis and machine learning pin-points any IoC “needles.”

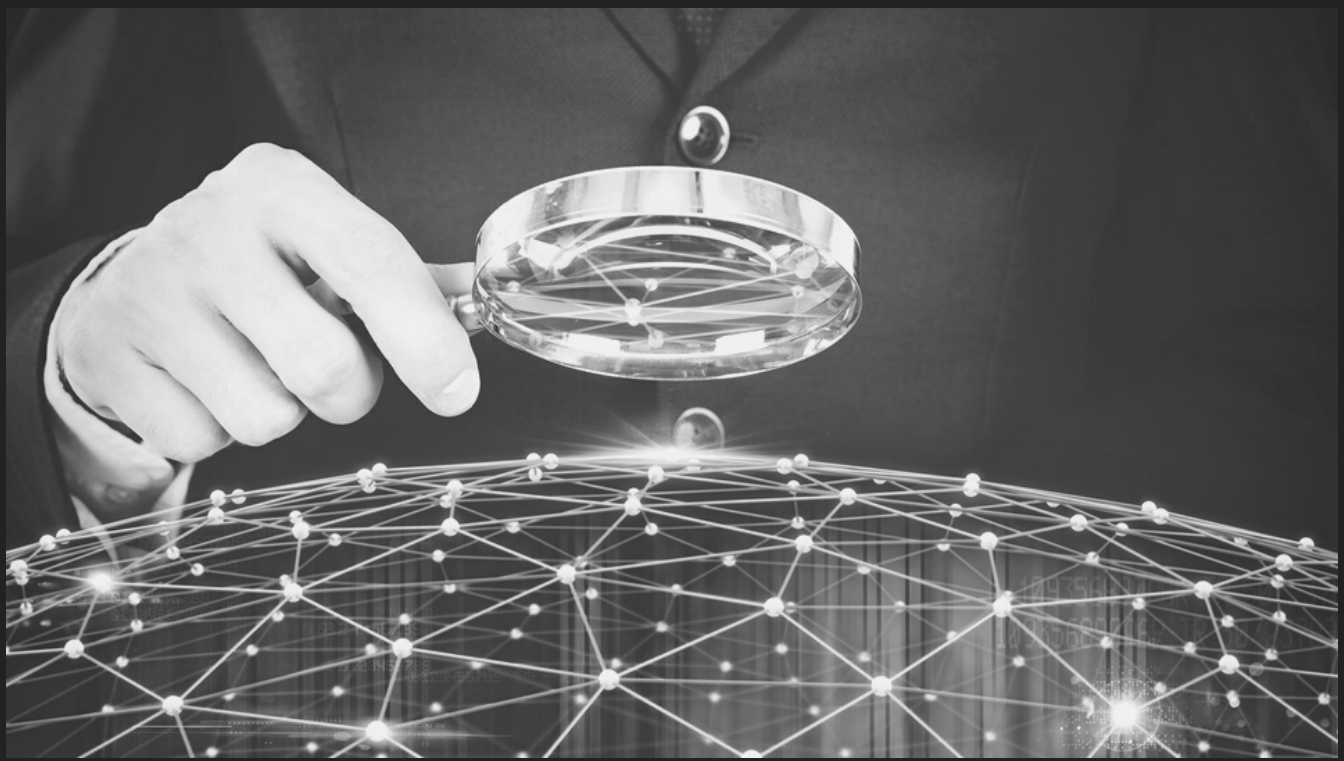
SENTINEL

Managed Endpoint Detection and Remediation comes with a powerful Endpoint Protection platform. Today, even basic malware campaigns are automated - enabling cybercriminals with few resources to launch sophisticated attacks against organizations of all sizes. To fight back, businesses deployed multiple layered, yet siloed, endpoint security solutions, which threat actors soon defeated by exploiting the gaps in between.

These synergistic trends mean there has never been a greater need for a unified, comprehensive approach to endpoint protection that's strong enough to thwart advanced attacks, but agile enough to adapt to the threat landscape.

Key Advantages:

- Precise protection without bloat
- Innovation that outpaces malware
- Complete solution, any size organization



SENTINEL

When suspicious activity occurs, security professionals need to actively respond in mere minutes, immediately stopping potential threats from propagating, while determining if the behavior is indeed malicious.

Endpoint response solutions need to be quick and easy to deploy, rapidly protecting organizational assets and shortening the time to respond. Integrated threat detection allows for progressive enrichment of threat detection insights across an attack chain.

And a cloud-based platform that guides administrators through investigation, response, and recovery give them the tools and intelligence needed to respond.

Key Advantages:

- Active response in minutes
- Linking engine for complete remediation
- Up to 72 hours of Ransomware Rollback
- Progressive Threat Detection
- Flight recorder for suspicious activity monitoring
- Endpoint Isolation
- Guided Threat Response

Sentinel enables the secure use of corporate applications on unmanaged devices - proactively thwarting information-stealing malware and other threats to corporate data. It helps to meet Infosec compliance and provides simple, low-cost deployment and management of endpoint security, wherever and however applications and data are accessed.

The Armored Client provides real time patented protection to applications and data without needing to detect and respond to threats. It does this by using kernel level prevention of data exfiltration, even if threats exist, combined with the secure wrapping of applications and injected security.

The Armored Client takes a layered approach to protecting endpoint devices being used remotely to access your applications and data and to support secure online browsing. Whether your employees are using unmanaged, BYOD or managed endpoint devices, all your corporate apps are targeted on the endpoint and run in a secure session.

Why Armored Client?

- Meets infosec and compliance requirements for data, risk and endpoint management - PCI, FFIEC, HIPAA, GDPR etc.
- Easily enables remote working - simple to centrally configure, distribute, manage and support software (and can be bundled with other apps)
- Works alongside, and crucially plugs key gaps in, all other security software and solutions, including VDI, AV, EDR and VPN.

SENTINEL
by WATCHTOWER365

GET IN TOUCH!

www.watchtower365.com

enquiries@watchtower365.com