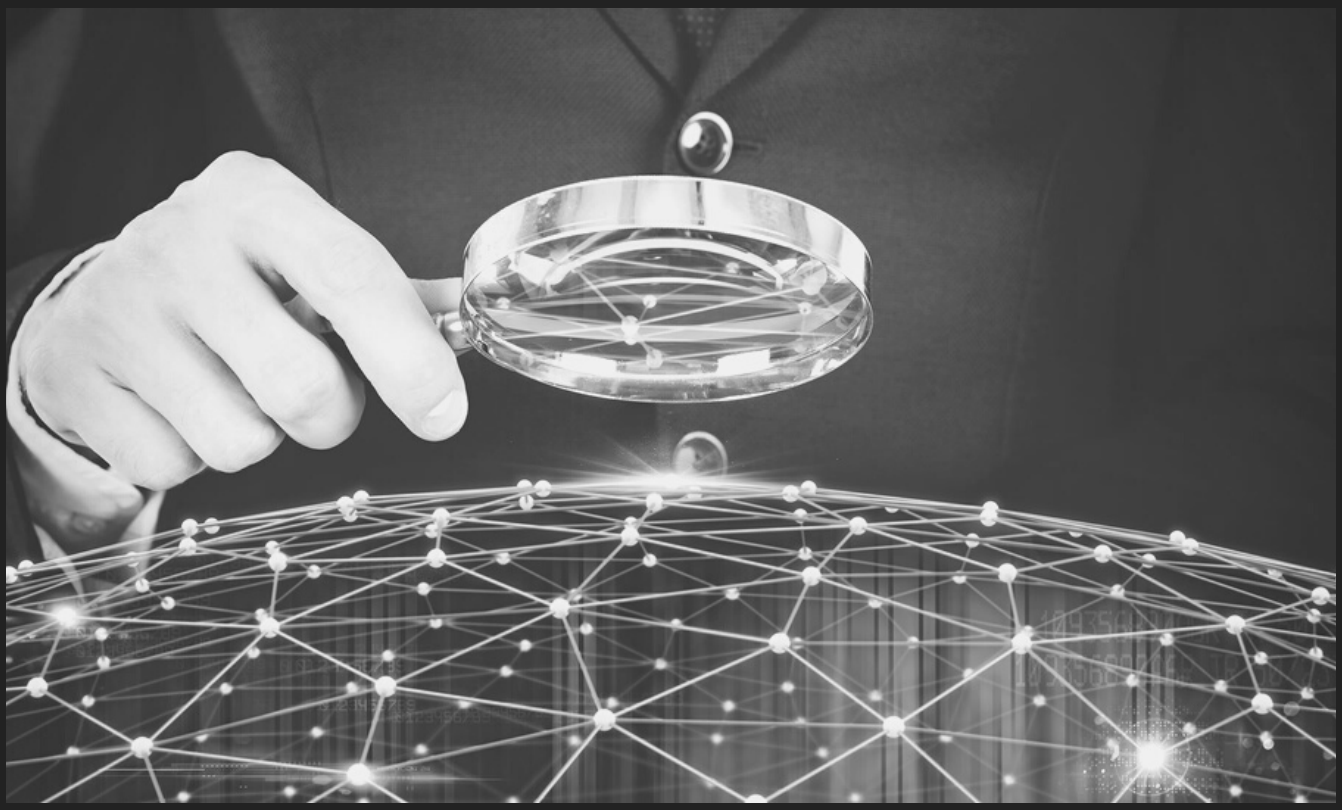
guardian
by WATCHTOWER 365

GUARDIAN

BE AWARE. BE SECURE

GUARDIAN

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.”

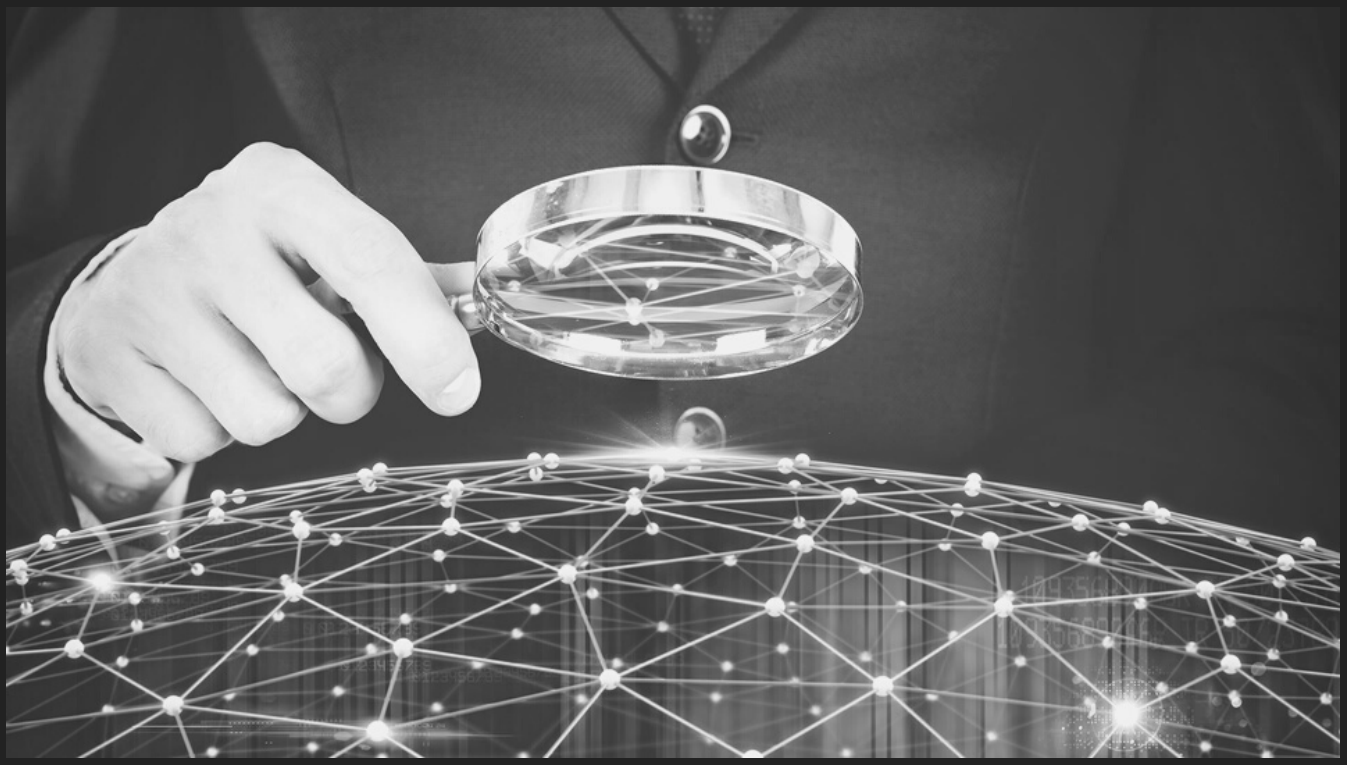
GUARDIAN

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



GUARDIAN

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

GUARDIAN PLUS

WatchTower365 Guardian 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.

It could not be simpler to centrally configure, distribute, manage and support Armored Client, giving you the reassurance of instant protection from cyber attacks across your unmanaged enterprise environment and for your third-party suppliers.

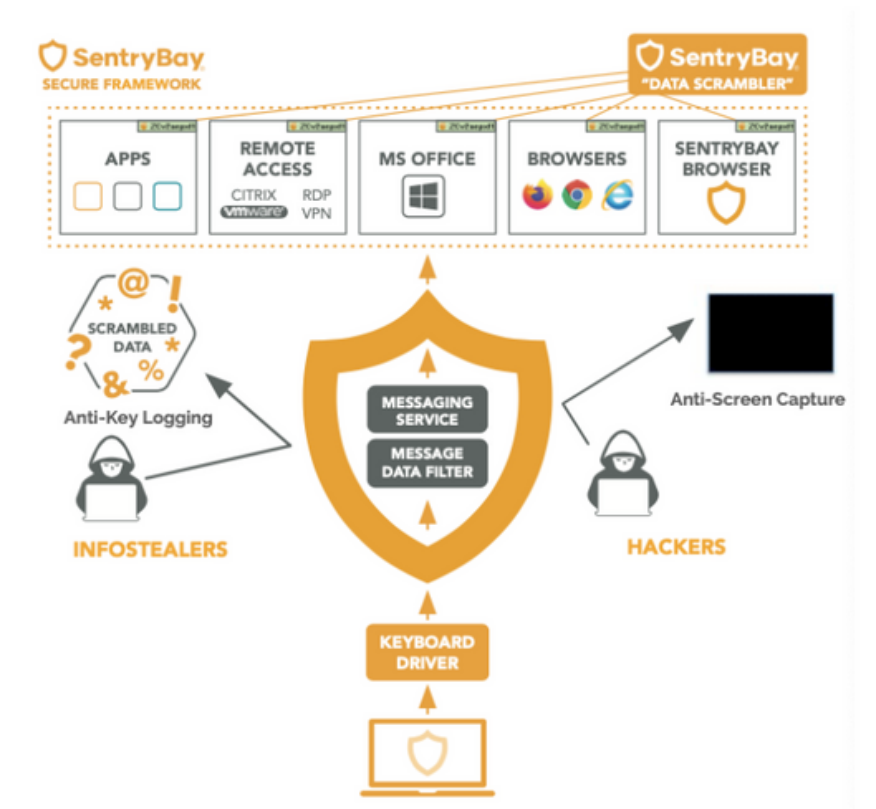
As well as helping you to meet your key compliance requirements, you benefit from a tangible CAPEX saving if you have implemented remote working, BYOD and BYOPC policies or wish to use the Armored Client to enable such policies. And don't worry about compatibility with existing infrastructure and security products, Armored Browser provides complementary protection alongside standard VDI, EDR, VPN and anti-virus solutions.

The Armored Client Portal provides you with web-based administration, configuration and deployment and allows you to create feature groups for easy management. Configurations can be applied in order to wrap and inject SentryBay security into selected applications within each user group and these will be dynamically updated.

PROACTIVE ENDPOINT PROTECTION OF APPLICATIONS AND DATA

WatchTower365 Guardian provides unique patented endpoint protection of data & applications via application containerisation, layered security and kernel-level anti-key logging & anti-screen capture protection irrespective of the undetected threats present.

- **PREVENTS** zero day undetected threats
- **ACTIVE** data protection - kernel-level anti-keylogging / anti-screen capture
- **CONFIGURABLE** pre-select which applications to protect
- **SIMPLE** one-time download - simple & transparent to use
- **COMPLIMENTS** existing AV & EDR
- **SIGNIFICANT** cost savings - NO locked down hardware required
- **SECURE** remote access - home working - secure devices anywhere



WatchTower365 Guardian Armored Client Powered by SentryBay

Key Benefits:

- Real-time protection of ALL data entry into VMware - logon and session activity
- Prevents zero day undetected threats exfiltrating data when using VMware on ANY device
- Simple One Time Download - easy to install - ease of deployment & enforcement
- NO integration required - NO performance impact
- Complements existing AV or EDR security solutions - if present
- NO 'locked down' hardware required - significant costs savings
- Regulatory compliance - GDPR, PCI, PSD2 and more
- Mitigate data breaches and potential financial penalties

Active Protection From:

- Key-Logging (including kernel-level)
- Screen Capture
- RDP Double-Hop
- DLL/Code Hooking Injection
- Code Execution Protection
- Man in the Browser & Man in The Middle
- DNS Attacks
- and many more threats...

ENTERPRISE MOBILITY MANAGEMENT

WatchTower365 Guardian platform is built on the foundation of award-winning and industry-leading unified endpoint management (UEM) capabilities with additional zero trust-enabling technologies, including zero sign-on, multi-factor authentication (MFA), and mobile threat defense (MTD). Together, they enable a seamless, secure user experience by ensuring only authorized users, devices, apps, and services can access business resources.

- Multi-Operating system support for Endpoints
- Complete Endpoint lifecycle management
- Flexible deployment options
- Data compliance and user privacy
- Ecosystem vendor integrations
- Secure access to corporate resources

The WatchTower365 Guardian provides a mobile centric architecture for the hybrid enterprise:

- Unified Endpoint Management
- Zero Sign-On
- Mobile Threat Defense

UNIFIED ENDPOINT MANAGEMENT

WatchTower365 Guardian's Unified Endpoint Management gives you insights to make better decisions that result in faster, more personalized service, while empowering teams to do their best work on the devices and apps they love - without compromising security.

Key Benefits:

- **Support Mobile Users Effectively:** Embrace mobility and enable your users to work on any device with the confidence that security measures are available to protect corporate information across endpoints.
- **Simplify administration:** Make policy delivery consistent and easy. Implement a single user policy just once and apply it across all of your user's devices.
- **Manage BYOD:** It shouldn't matter who owns the hardware. Manage access to corporate information without invading the user's personal data.
- **Secure what matters:** React quickly in case a device is lost or stolen and protect the corporate content users access.
- **Be the IT in "Unity":** Manage and secure all your users' devices through a single, unified system.
- Common Experience: It shouldn't matter who owns the hardware. Manage access to corporate information without invading the user's personal data.
- **EMM style or full agent:** Why choose? Have the best of both worlds and manage your devices via EMM AND have the option to utilize the powerful agent based management style.
- **Operational Security:** Combined with endpoint security, it can easily isolate affected devices in the event of a breach, automatically push software, and put the device back on the network.

ZERO SIGN-ON

Reduce the likelihood of data breaches by eliminating passwords.

- Passwordless authentication - Go beyond SSO and eliminate the need for passwords on any device.
- Smart, risk-based policy enforcement - Easily enforce policies based on the criteria that matter to your organization.
- Single console tracking - Secure any SAML or WD-FED federated cloud or on-premises services using a standards-based approach.

Key Benefits:

- Reduce Risk. Eliminate Passwords.
- User-Friendly, Frictionless Authentication
- Prevent Unauthorized Data Access
- Discover Mobile Cloud Risks
- Intuitive Remediation
- Scalable Cloud Security Framework

MOBILE THREAT DEFENCE

Defend and remediate threats targeting mobile devices.

- Protect Against Mobile Phishing
- Easy Deployment
- Speed Matters
- Continuous App Visibility and Evaluation
- Granular Control
- Flexible Compliance Actions Support User Productivity

guardian
by WATCHTOWER 365

GET IN TOUCH!

www.watchtower365.com

enquiries@watchtower365.com