A complete endpoint security solution with AI-guided policy management

The constant evolution of IT environments means attackers are using more sophisticated methods to infiltrate networks – with the endpoint being your last line of defence. As ransomware attacks rise, organisations are becoming more concerned about cyber damage and disruption. The expanding use of file-less and stealthy infiltration, combined with "living off the land" (using common IT tools for attacks), threatens the confidentiality, integrity, and availability of endpoint assets.

Our managed endpoint security solution addresses the threats posed by cyberattacks. By constantly monitoring activity at the endpoint using a lightweight agent and applying security policies we'll keep your business safe. We've partnered with Symantec and CrowdStrike, the leading providers of end point solutions, to deliver our service.

More effective security

Our solution uses AI techniques (including behaviour analysis) coupled with time-tested prevention technologies. It gives you unparalleled endpoint visibility and protection, with telemetry from the largest civilian threat intelligence network. We protect the endpoints regardless of where attackers strike on the attack chain, using a variety of advanced capabilities. And we'll strengthen your security position through intelligence gathered by deception technology when attackers trigger easy to deploy deceptors.

Simplified management

You can coordinate your entire endpoint security from a single cloud console to reduce management complexity. At the same time, our artificial intelligence (AI) guided security management will help deliver more accurate policy updates and fewer misconfigurations to help improve the overall health of your security system.

Integration with existing investment

Our solution can quickly stop the spread of an attack and provide an orchestrated defence and response at the endpoint. You'll also get better visibility of threats using shared intelligence from across our cyber platforms.

A smarter, simpler way to manage endpoint security.

- drive more accurate, intelligent and faster insights with AI-guided security management from a single cloud-based dashboard
- manage complete endpoint security from a single cloud console to reduce endpoint security management complexity
- get rapid updates through a "single agent" architecture simplified design
- eliminate routine tasks and enhance endpoint security decisions through simplified workflows with context aware recommendations
- our solution uses Autonomous Security Management to learn from admins, organisation, and the security community.

Detect a wider range of threats and snuff out any danger

Our endpoint security solution includes Advanced Machine Language (AML) to detect new and evolving threats before they can execute. It constantly monitors and instantly blocks files that behave suspiciously. And by using Memory Exploit Mitigation, it can block zero-day exploits against vulnerabilities in popular software.

Core capabilities

Antivirus
Scans and eradicates malware that arrives on a system.

Firewall and intrusion prevention
Blocks malware before it spreads to the machine and controls traffic.

Application and device control
Controls file, registry, and device access and behaviour; also offers whitelisting and blacklisting.

Power eraser
An aggressive tool, which can be triggered remotely to address advanced persistent threats and remedy tenacious malware.

Host Integrity
Ensures endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments with the ability to isolate a managed system that does not meet your requirements.

System lockdown
Allows whitelisted applications (known to be good) to run or block blacklisted applications (known to be bad) from running. Our single agent architecture enables IT security teams to add innovative security technology with simplified deployment, meaning no new agents are needed. In addition we support many environments, including IPv6.

Advanced capabilities

Global Intelligence Network (GIN)
The world's largest civilian threat intelligence network informed by 175 million endpoints and 57 million attack sensors across 157 countries. The data collected is analysed by more than a thousand highly skilled threat researchers to provide unique visibility and cutting edge security innovations.

Reputation analysis
Determines the safety of files and websites using artificial intelligence techniques in the cloud and powered by the GIN.

Emulator
Uses a lightweight sandbox to detect polymorphic malware hidden by custom packers.

Intelligent threat cloud
Advanced techniques such as pipelining, trust propagation and batched queries mean you don't have to download all signature definitions to the endpoint to maintain a high level of effectiveness – reducing the size of signature definition files by up to 70%, which in turn reduces bandwidth usage.

Roaming client visibility
Receives critical events from clients that are off the corporate network.

Suspicious file detection
Enables IT security teams to tune the level of detection and blocking separately to optimize protection and gain enhanced visibility into suspicious files for each customer environment.

Hardened endpoints
By isolating suspicious or malicious apps into "jail-mode" it prevents the execution of privileged operations, including downloading executable files, writing to the registry and more.

Fixed function device lock down
Enforce default-deny to applications and restrict updates to defined trusted updaters.

Restricted execution of unauthorized apps
Manage the "allow" list of approved apps for standard endpoints for additional flexibility.

Extended use of unapproved applications
You can allow application deemed safe while alerting administrators to the potential risk of application drift.

Why choose BT?

Breadth and depth of experience

We are one of the world's leading security brands, with decades of experience in the field:

- we have one of the largest security and business continuity practices in the world with over 3,000 security professionals
- we monitor customer devices around the clock from our 16 global Security Operations Centres
- we have analyst recognition for delivering outstanding Managed Security Services globally.

Security Operations Centres (SOCs)

We have a network of 16 SOCs around the world, where customer devices are managed and monitored, and where our security analysts are on hand to provide real-time support and response services to protect your networks. To provide the highest quality of service, the SOCs are accredited and audited variously to industry and government information assurance standards.

What could Managed Endpoint Security do for you?

We look forward to hearing from you.
03333444190 info@hm-network.com hm-network.link/authorised-bt-partner

HM-NETWORK.com

Authorised partner of BT

Offices worldwide

July 2020