ENDPOINT PROTECTION PLATFORM (EPP)

The scale & sophistication of cyber threats has grown. So has the demand to couple advanced endpoint security solutions with skilled analysts to proactively detect and respond to those risks.

Bytes' Managed EPP service leverages the power of our 24/7 SOC, together with your choice of enterprise EPP tooling, to do just that.

The Challenge

Endpoint security has evolved from traditional antivirus to comprehensive protection, which includes behavioural detection and attack surface reduction tooling, from sophisticated malware and evolving zero-day threats. To maximise protection, expert analyst skills are required to ensure that the endpoint attack surface is secured and that threats are monitored, detected and mitigated.

Many organisations lack the time, skills or resources to operate, maintain and monitor their EPP solution, which is why we support our customers' endpoint security, 24/7.
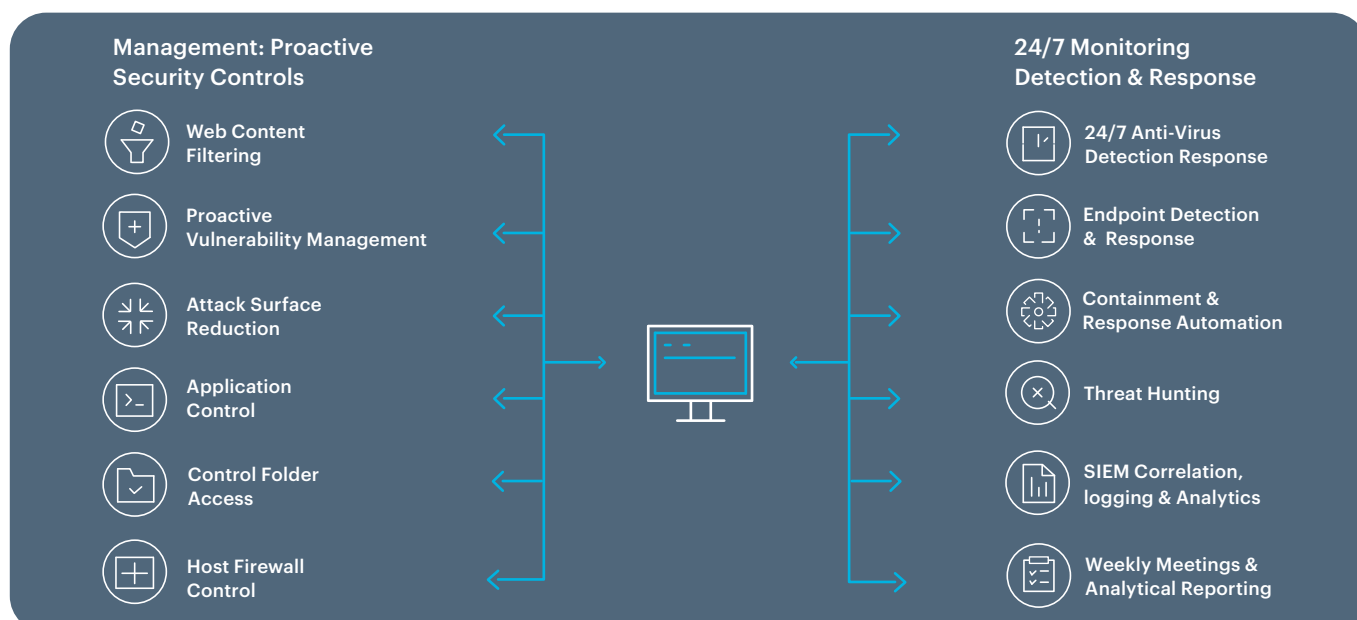
The Solution

Bytes' Managed Endpoint Protection service provides not only the proactive management to reduce vulnerabilities and the attack surface, but also applies needed security policieis with 24/7 monitoring. Ensuring you are always on top - detecting and responding to threats promptly.

Benefits

- **Gain Control.** Endpoints and users are the new perimeter. Take control of the risk.

- **Proactive Management.** Reduce vulnerabilities, close attack surface and reduce endpoint risk.

- **24/7 Detection & Response.** Cyber wars need a cyber army.

- **Powered by your Enterprise,** market leading endpoint security tools.

- **Reduce Cost.** Managed Service means no hiring or staffing headaches.

Our Managed EPP enhances customers' endpoint security by delivering:

Management: Proactive Security Controls

- Web Content Filtering
- Proactive Vulnerability Management
- Attack Surface Reduction
- Application Control
- Control Folder Access
- Host Firewall Control

24/7 Monitoring Detection & Response

- 24/7 Anti-Virus Detection Response
- Endpoint Detection & Response
- Containment & Response Automation
- Threat Hunting
- SIEM Correlation, logging & Analytics
- Weekly Meetings & Analytical Reporting

Contact us at
tellmemore@bytes.co.uk

For more details visit
bytes.co.uk/security

Service Features

Proactive Management

Endpoint devices and end-user devices such as servers, desktops & laptops on any network will be exposed to exploits, misuse and malicious actors. Preventative controls are by far the best strategy. However, this requires configuration and maintenance by Skilled Engineers! Our team provides proactive management of your endpoints to provide the following:

Proactive Vulnerability Management

Our team will Identify & prioritise endpoint vulnerability remediation processes and remediation requests for approval.

Attack Surface Reduction

We shall harden and deliver proactive endpoint policy management and reduce places where the device is vulnerable to attack.

Application Control

Polices will manage and restrict applications that users can run.

Web Content Filtering

We shall manage your corporate web policies to secure your machines against web threats & unregulated content.

Controlled Folder Access

We will maintain policies for controlled folder access to protect valuable data from malicious apps & threats, such as ransomware.

Host Firewall Control

We shall configure & maintain host-based, two-way network traffic to block unauthorised network traffic flow & reduce the attack surface.

24/7 Detection & Response

Malicious actors will evade your security controls. Now the importance is placed on detecting, blocking and responding to malicious actions. Our 24/7 SOC team will provide the following support.

24/7 Anti-Virus Detection Response

Microsoft Defender Antivirus is the next-generation protection component of Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

Anti-Virus detection always requires investigation and response to ensure proper remediation. Our SOC team monitors the behaviour-based, heuristic and real-time antivirus protection to alert and respond to malicious activity 24/7.

Endpoint Detection & Response

Behavioural anomalies are monitored in real time using EDR queries based on telemetry that collects and processes information, network activities, user login activities, registry and file system changes and more.

Containment & Response Automation

Our SOC team responds rapidly to detected attacks by isolating machines or collecting an investigation package. This include the processing and investigation of incidents generated by Microsoft Automated Incident Response module.

Advance Threat Hunting

Our Analysts run standard procedures for offline threat hunting, using our query-based threat hunting tool. Our team of certified incident handlers and forensic analysts will identify risk indicators for further analysis.

SIEM Integration & Correlation

We maintain corporate web policies to secure your machines against web threats and helps you regulate unwanted content.

Bytes Operations Centre Team

Even the best tooling in the world needs skilled analysts to operate an endpoint security ecosystem 24/7. Cyber never sleeps, after all! With Security Operations Centres in London, Dubai, Pune, Doha, Riyadh and Sydney, our team of 200+ SOC analysts look after your endpoints to allow your own IT and Security Teams to focus on other business priorities.

Incident Management Platform

24/7 transparent & auditable collaboration, Incident Management, Dashboarding, SLA Management and Customer ITSM integration API.

Weekly Meetings

Understand the complete picture from our certified analysts who illuminate risks, incidents and recommend security posture enhancements. 15-minute response for critical incidents, with real-time SLA dashboards.

Rapid Response & Smart Automation &

Central support for automation of IR activities, repetitive processes, increased accuracy and shortened recovery time for remediation.

Zero Complexity, Low Maintenance

We supplement your team and maintain systems to keep things simple for you.

Access to Global SOC & SecurityHQ Labs

Enriched threat intelligence with an all-encompassing world view from global SOC and Labs.

Easily Integrated

Our services are simple to deploy and easy to integrate within your systems.

Precise, Action-oriented & Flexible Reporting

Risk based and patch prioritised time, with weekly and monthly reports.

High Scalability & Flexibility

Bespoke services tailored to the needs of the customer or partner.

Expert Analysts

With Industry best certifications - OSCP, GPEN, GWAPT, CEH and more.

Continuous Governance Model

Embed a continuous governance model to ensure improvement.

Incident Response Capability

The Problem

Security incidents do, and will, occur. Post detection, a rapid response is critical to contain and investigate rogue activity 24/7.

The Solution

Bytes provides Incident Response playbooks, supported with our IBM Resilient SOAR Platform & Certified Incident Handlers to contain threats.

Cyber Warfare Needs a Cyber Army

The Problem

Your adversaries are armed with skilled experts. You need the same, and more.

The Solution

We empower our customers by providing skilled resources as an extension of our team. Bytes utilises over 200+ Security Analysts who continuously hunt, detect and respond to security events, 24/7, from our global SOCs.

Risk Reporting & Business Security Intelligence

The Problem

38% of breaches are the result of errors and/or misuse of systems. Risky assets, users and behaviour needs to be presented graphically and within a business context.

The Solution

By visualising risky behaviour and misconfigurations, we target the threat at its source. Our customers receive detailed weekly reports with granular statistical analysis to illuminate uncertain behaviour, security posture issues and security incident metrics.

Complex & Evasive threat Detection

The Problem

Organisations struggle with the rapid identification of malicious behaviour. This identification requires a matured SIEM, with advanced correlation, anomaly and user behaviour analysis, together with continuous monitoring.

The Solution

Bytes applies advanced correlation & machine learning to expose patterns of illicit behaviour. SOC immediately investigates the extent of an event, and its context, to derive a complete analysis with mitigation and risk quantification.

Our expert analysts support and manage:

Bitdefender   Carbon Black.   SOPHOS   CROWDSTRIKE

Have a question? We would love to hear from you.

Reach us

tellmemore@bytes.co.uk | 01372 418 500

bytes.co.uk/security

Follow us

f in 🐦