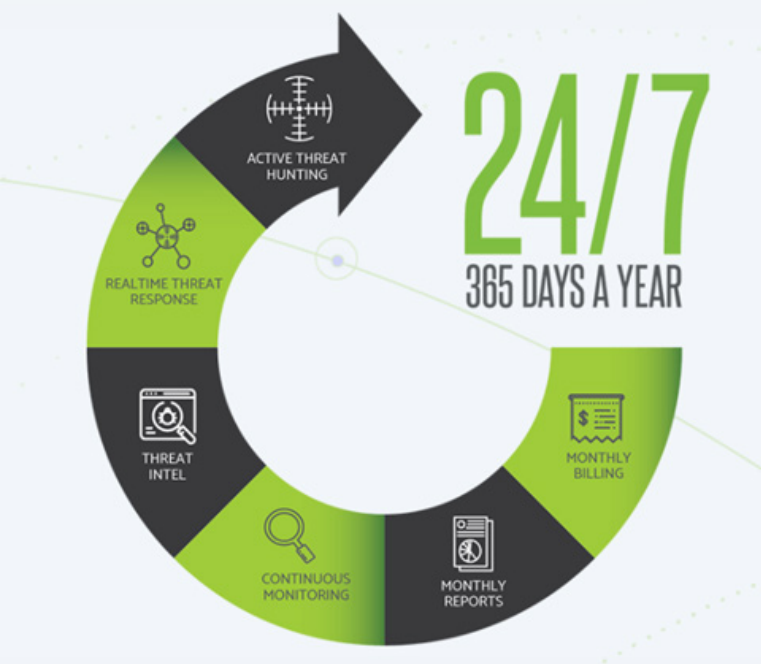
CARBONITE an opentext company | WEBROOT an opentext company

State-of-the-art MDR, Cyber Liability Insurance and Incident Response for MSPs

blackpoint

Today's threat landscape means that, if you have vital services to deliver, hold valuable intellectual property, or have commercially sensitive data, and if disrupting your organization will severely affect others – then you are a prime target for cyberattacks. Whether the criminals are targeting you, your clients, or both as a means to get from one to the other, the stakes are high.



Attacks are increasingly sophisticated, and older IT security models simply aren't strong enough. Especially for MSPs, having supplemental assistance to proactively stop attacks is now crucial for maximizing security and mitigating client breaches.

That's why the Webroot + Blackpoint Cyber integration is ideal for MSPs and their clients. By combining unique, real-time telemetry from Webroot® Business Endpoint Protection and Webroot® DNS Protection with Blackpoint's managed detection and response (MDR) services, this integration provides the reliable, holistic attack prevention and mitigation MSPs need to keep clients secure.

Instant context and high accuracy

This integration incorporates live data from Webroot to provide instant context, while accurately highlighting the threat situation the Blackpoint Cyber console. Webroot provides key risk information such as threat status, threat path, engine version, communications status, shields status and environment settings for detailed inputs into the Blackpoint Cyber system.

Actionable threat telemetry

Unique layers of additional, actionable threat information are only available through Webroot's propriety endpoint protection delivery. If Webroot DNS Protection is also deployed within a given environment, then DNS Protection log data is also available in the Blackpoint Cyber console to contextualize and enrich the MDR's understanding of communications between your clients' network and devices and the internet.

Protection and recovery for Microsoft® 365

Alongside the Blackpoint MDR service, you can take advantage of a separate Microsoft 365 defense service. This option provides round-the-clock security monitoring and policy enforcement through Blackpoint's cyber analysts, who monitor and harden your clients' Microsoft 365 environment and Microsoft 365 client accounts.

Blackpoint cyber liability insurance for MSPs

By partnering with Blackpoint Cyber, you also get breach cost recovery through their cyber liability insurance, giving you additional peace of mind and resilience in the unlikely event that an attack is successful.

Stellar service approach

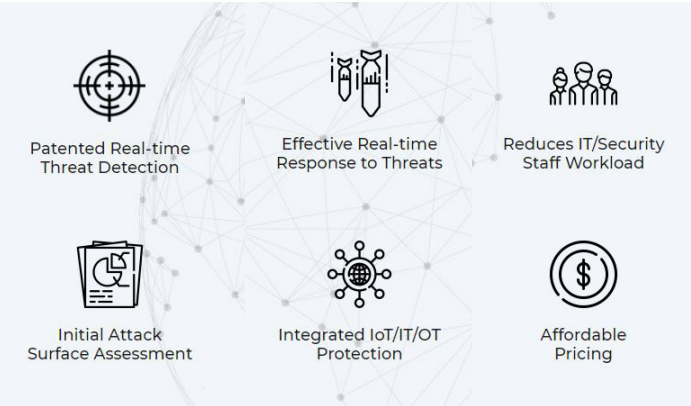
The Blackpoint MDR service offers a continuous and proactive approach to defending your clients' networks. It starts with a trial to ensure attackers have not already infiltrated the network, and to identify any vulnerabilities in your infrastructure.

During a trial, you can expect the following review:

- Asset Visibility – Discovers what is connected and what each asset is doing in real time.
- Privileged Account Activity – In most breaches, privileged credential theft is present. Preventing this abuse is key.
- Port Hardening – Attackers scan for open ports. By monitoring and closing unneeded ports and hardening those you do need, you effectively reduce attacks.
- Software Visibility – There are numerous services and applications that communicate with a single device. Blackpoint SNAP-Defense software uncovers the different scripting languages communicating with each endpoint and helps determine the information exposure risk.
- General User Behavior – Normal user behavior, particularly privileged behavior, blends into the background noise of a typical network. Attackers rely on this noise to avoid raising alarm. Blackpoint brings user behavior to the fore for continuous review to help identify malicious or suspicious activity.

For More Information

To learn more about the benefits of the Webroot + Blackpoint Cyber integration or start an MDR trial, email info@blackpointcyber.com or call +1 410 203 1604. You can also contact your Webroot Account Manager directly



Blackpiont at a glance

"The integration of Blackpoint Cyber and Webroot makes our lives much easier and provides enhanced protection for our customers... Overall, this integration is a win-win for MSPs."

– Platte River Networks, Webroot partner

For more information:

Contact your Webroot account manager.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.

About Blackpoint Cyber

Blackpoint Cyber is a technology-focused cyber security company headquartered in Maryland, USA. The company was established by former US Department of Defense and Intelligence cyber security and technology experts. Leveraging its real-world cyber experience and knowledge of malicious cyber behavior and tradecraft, Blackpoint provides cyber security products and services to help organizations protect their infrastructure and operations. The company's proprietary security operations and incident response platform, SNAP-Defense, is available as a product or as a 24×7 Managed Detection and Response (MDR) service. Blackpoint's mission is to provide effective, affordable real-time threat detection and response to organizations of all sizes around the world.