

# BLUESHIFT XDR

## Blueshift XDR brings affordable, comprehensive managed security operations to companies of any size.

Blueshift XDR™ (Extended Detection and Response) is an affordable, highly automated SOC-as-a-Service platform that simplifies compliance initiatives and extends security visibility and management across your entire organization. Blueshift XDR seamlessly engages with all devices, data, and systems across the network—cloud, IoT, endpoint, server, remote workers, ICS, OT, and more. When it comes to incident response, XDR allows our SOC teams to identify and respond to sophisticated cyberattacks quickly.



### Surprisingly affordable

Your IT staff is busy. Your MSP is busy. With Blueshift XDR, there's no need to hire expensive cybersecurity experts. All services are securely managed by our certified SOC while keeping your data on premises at all times.



### Highly flexible

Featuring a build as you go, 100% cloud-monitored cybersecurity platform, Blueshift XDR makes it easy to structure your cybersecurity operations for your organization's size and budget.



### Immediately effective

Blueshift XDR is easy to install and reduces cybersecurity risk right away. XDR also ensures your organization is ready to meet compliance challenges from CMMC, PCI-DSS, SOC II, GDPR, HIPAA/HITECH, MITRE ATTACK, and more.



Rely on Blueshift's zero-trust approach to defeating ransomware and data theft by ensuring that only trusted processes and authorized users have access to your organization's critical data.

# BLUESHIFT XDR

## Explore Blueshift XDR Managed Security Operations.

Move beyond siloed cybersecurity solutions, and outsource security operations to a team of highly trained cybersecurity professionals.



### Managed Network Detection and Response

Blueshift XDR inspects every packet moving into and out of your network. When threats are discovered, Blueshift traps and blocks them, preventing any infection from turning into an attack.



### Managed Vulnerability Detection

Blueshift XDR provides network vulnerability scanning and agent-based vulnerability detection for all assets—wherever they reside—on premises, at home, or in the cloud.



### Managed SIEM

Blueshift XDR Managed SIEM supports monitored security analytics and compliance across the entire enterprise, including network(s), cloud, containers, endpoints, servers, and remote workers. Support for Windows, Linux, and MacOS ensures compatibility across your entire organization.



### Managed Data Defense

Protect data at rest and in transit with Cigent D<sup>3</sup>E<sup>®</sup> for Windows. Deployed, configured, and managed by Blueshift XDR, D<sup>3</sup>E features zero-trust, file-level multifactor authentication and encryption that protects any file stored in any location, and limits access to only authorized users.



### Managed Self-Defending Storage

With Blueshift XDR, Cigent Secure SSDs are deployed, configured, monitored, and managed centrally. Every Cigent Secure SSD™ features firmware-based cybersecurity protections that make data invisible to would-be attackers. Cyberthreats, including ransomware attacks, are detected and repelled automatically.

[Requires XDR Managed Data Defense](#)



### Managed Application Whitelisting

Surpass typical whitelist features and employ highly effective default-deny defense with PC Matic whitelist management. The optional antivirus solution scans for endpoint malware, rootkits, and viruses.

844-256-1825 [www.blueshiftcyber.com](http://www.blueshiftcyber.com)