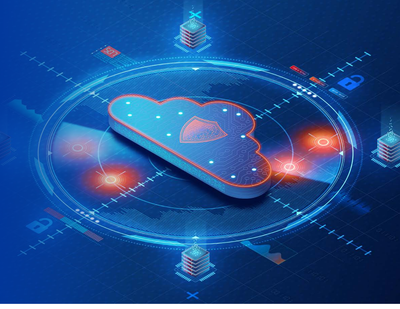
BlackBerry | Cybersecurity

HOW TO EVALUATE A MANAGED XDR SERVICE



Managed XDR services differ, so choosing the best fit for your organization's needs is critical. When evaluating each provider, consider differences in technology, capabilities, operational costs, and vendor reputation. **Look for these features to ensure your organization receives the most benefit from a managed XDR service:**

A COMPANY WITH A PROVEN TRACK RECORD

Expert threat hunters have years of experience to guide their work and properly identify and effectively stop threats for you. Managed XDR offers your organization a way to access seasoned cybersecurity analysts without having to recruit them in a competitive hiring environment.

24x7x365 THREAT MONITORING AND MITIGATION

Managed XDR should provide continuous threat detection and response coverage to enable your organization to reallocate IT security resources to other tasks.

THIRD-PARTY INTEGRATION

Collecting and interpreting threat telemetry from numerous sources is a powerful feature of managed XDR. Integration can reduce your incident response times, alert fatigue, and false positives.

ACCESS TO SECURITY ANALYSTS

Having XDR managed by cybersecurity professionals is good but being able to consult cybersecurity experts and ask questions about environment specifics is better.

ADVANCED TECHNOLOGIES

Some managed XDR providers offer services that include advanced technology, such as AI-driven threat prevention and automated incident response. These technologies are a force multiplier when properly deployed, offering your organization increased protection without the costs of additional headcount.

RELEVANT DATA DELIVERED OVER MULTIPLE CHANNELS

Effective managed XDR systems not only collect threat telemetry from multiple sources, they also deliver relevant data to you through email, SMS, alerts, and other channels.

MITRE ATT&CK MAPPING, CUSTOM PLAYBOOKS

Integrating the MITRE ATT&CK® mapping into technology platforms and creating custom response playbooks offers a lightning-fast layer of threat prevention.

CONTINUOUS AUTHENTICATION

Ensuring only trusted entities gain access to your organization's resources is a key component for moving towards a Zero Trust framework.

When it comes to managed XDR services, no two solutions are alike. CylanceGUARD®, the BlackBerry® managed XDR platform, integrates an award-winning team of threat hunters with predictive AI, best-in-class automation, continuous monitoring and 24x7x365, world-class support to help you defend against sophisticated and coordinated cyberattacks.

Before deciding which managed XDR service best fits your organization, download the BlackBerry Managed XDR Buyer's Guide.

BlackBerry | Cybersecurity

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 195M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear – to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*

19072022