

Extended Expertise. Yes there is more.

# Add-on Managed Services

Supplementary Offerings Designed to Enhance  
Core Capabilities

# Welcome to our library: feel free to make some noise

Sitting adjacent to our core service offerings, Decisive has many capabilities which we offer to our clients. These services are complementary, however they can also stand on their own, as high value security controls for your environment.

## Gotta cover your bases

It is imperative for businesses of all sizes to deploy security controls to protect their data. These controls begin with a foundational layer which is not a recommendation but a necessity, as the loss or compromise of data can lead to significant financial losses, damage to reputation, and legal repercussions. Navigating the many products on offer to make an informed decision can be a daunting task. Determining how to invest a limited budget to provide adequate coverage can also be a challenge. Decisive Group has done the research and testing for you, partnering with industry leading vendors to offering competitive services which are designed to combat today's modern threats.

## Advanced Endpoint Security

Endpoint detection and response (EDR) is a critical security control that extends beyond traditional signature-based detection methods. Endpoints, such as computers, laptops, and mobile devices, serve as the entry points to an organization's network and are often the targets of cyber adversaries. Signature-based detection relies on known patterns of malicious code, making it effective against known threats but inherently limited in addressing new and evolving forms of malware. Modern cybersecurity demands a more proactive and adaptive approach, which is where advanced endpoint security comes into play.

### Service Features:

- Licensed per agent
- Endpoint security that goes beyond signature-based detection
- Detect known and zero-day exploits and malware variants through behavior analytics
- Block infections in real-time regardless of network connectivity/physical location
- Run domain wide search to find and remove malicious files
- Ability to quarantine hosts

- Threat Intelligence feeds used for threat assessment
- Reduce employee downtime due to infected equipment
- Integrates well with SIEM and SOAR for comprehensive security protection
- Advanced customizable automation rules
- Minimal demand on memory/bandwidth/cpu
- No reboots required for agent updates/install
- 24/7/365 Monitoring of Security Events (Requires SIEM subscription)
- Monthly Reporting



## Vulnerability Management

Vulnerability management, within the broader framework of cybersecurity, stands out as a linchpin in the pursuit of data resiliency. It involves a systematic and proactive approach to identifying, assessing, prioritizing, and mitigating vulnerabilities within an organization's IT infrastructure. As technology evolves, so do the tactics of malicious actors seeking to exploit weaknesses in software, networks, and systems. Vulnerability management serves as a dynamic defense mechanism, continuously scanning and assessing the enterprise landscape to detect and address potential points of vulnerability before they can be exploited.

## Service Features:

- Options for scheduled and continuous vulnerability scanning
- Scheduled scans are performed at a regular cadence
- Customized scan results and prioritization
- On demand scans against new critical vulnerabilities are performed
- Customized remediation plans
- Track vulnerabilities scan over scan to measure effectiveness
- Network and Asset Modeling results are fed into the Decisive SIEM (if subscribed) to enrich and add context to data/events being processed. This significantly increases fidelity of notable events and security investigations



## Security Awareness and Phishing

No data resiliency plan is complete without attention paid toward the human element of security, which is where awareness training plays a pivotal role. Employees, being the frontline defenders against cyber threats, need to be equipped with the knowledge and skills to recognize, prevent, and respond to security incidents. Security awareness training goes beyond mere theoretical knowledge, actively engaging employees to understand the importance of cybersecurity in their daily tasks and fostering a culture of vigilance.

Phishing, a prevalent and ever-evolving cyber threat, often exploits human vulnerabilities to gain unauthorized access to sensitive data. Hence, phishing simulation exercises are a fundamental requirement within security awareness training programs. These simulations replicate real-world phishing scenarios, enabling employees to experience and learn how to identify and thwart phishing attempts. By exposing individuals to simulated phishing attacks, organizations can assess the effectiveness of their training programs, identify areas for improvement, and empower employees to make informed, security-conscious decisions.

## Service Features

- Licensed by number of employees in scope
- Ability to “port over” existing licensing or provide
- Regular assignment of security training to employees based on topical themes
- Tracking and reporting of training completion across teams
- Periodic testing of organization and/or specific teams via phishing campaigns
- Remedial training to those who fail testing
- Monitored mailbox for phishing reporting
- 24/7/365 Analyst team investigating reported messages and updating internal security leadership

**KnowBe4**  
Human error. **Conquered.**

## Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Purus in massa tempor nec. Sed egestas egestas fringilla phasellus faucibus scelerisque. Nisi scelerisque eu ultrices vitae auctor eu augue ut. Cras sed felis eget velit. Ut diam quam nulla porttitor massa id. Scelerisque varius morbi enim nunc faucibus. Vulputate enim nulla aliquet porttitor. Lorem ipsum dolor sit amet consectetur. Nunc sed velit dignissim sodales. Tincidunt augue interdum velit euismod in pellentesque massa placerat duis. Leo urna molestie at elementum eu.

Venenatis cras sed felis eget velit aliquet sagittis. Ullamcorper morbi tincidunt ornare massa eget. Nunc mi ipsum faucibus vitae aliquet nec ullamcorper. Morbi enim nunc faucibus a pellentesque. Pharetra vel turpis nunc eget. Ipsum dolor sit amet consectetur adipiscing elit. Amet tellus cras adipiscing enim eu turpis.



## How to contact us



1 (855) 336-3700



[inquiry@decisivegroup.com](mailto:inquiry@decisivegroup.com)



118 Iber Road, Suite 105,  
Ottawa, ON K2S 1E9

## Enterprise IT. Customized for you.

**Decisive Group designs, builds, and maintains enterprise IT infrastructure and hybrid cloud, as well as managing and protecting data.**

We engage with customers through our hands-on approach, providing guidance and highly personalized service. Solutions-driven, we partner with the world's leading providers of standards-based hardware, software, networking, security, and cloud products with one aim: to optimize processes and improve outcomes for medium and large enterprises.

In 2001, Decisive Technologies was founded as a professional services company in Canada's National Capital Region, and we began offering data centre solutions in 2010. We expanded our offerings in 2013 with the addition of BriteSky Technologies, which originally focused on cloud storage, and in 2021, the companies amalgamated their products and services under the Decisive Group banner.