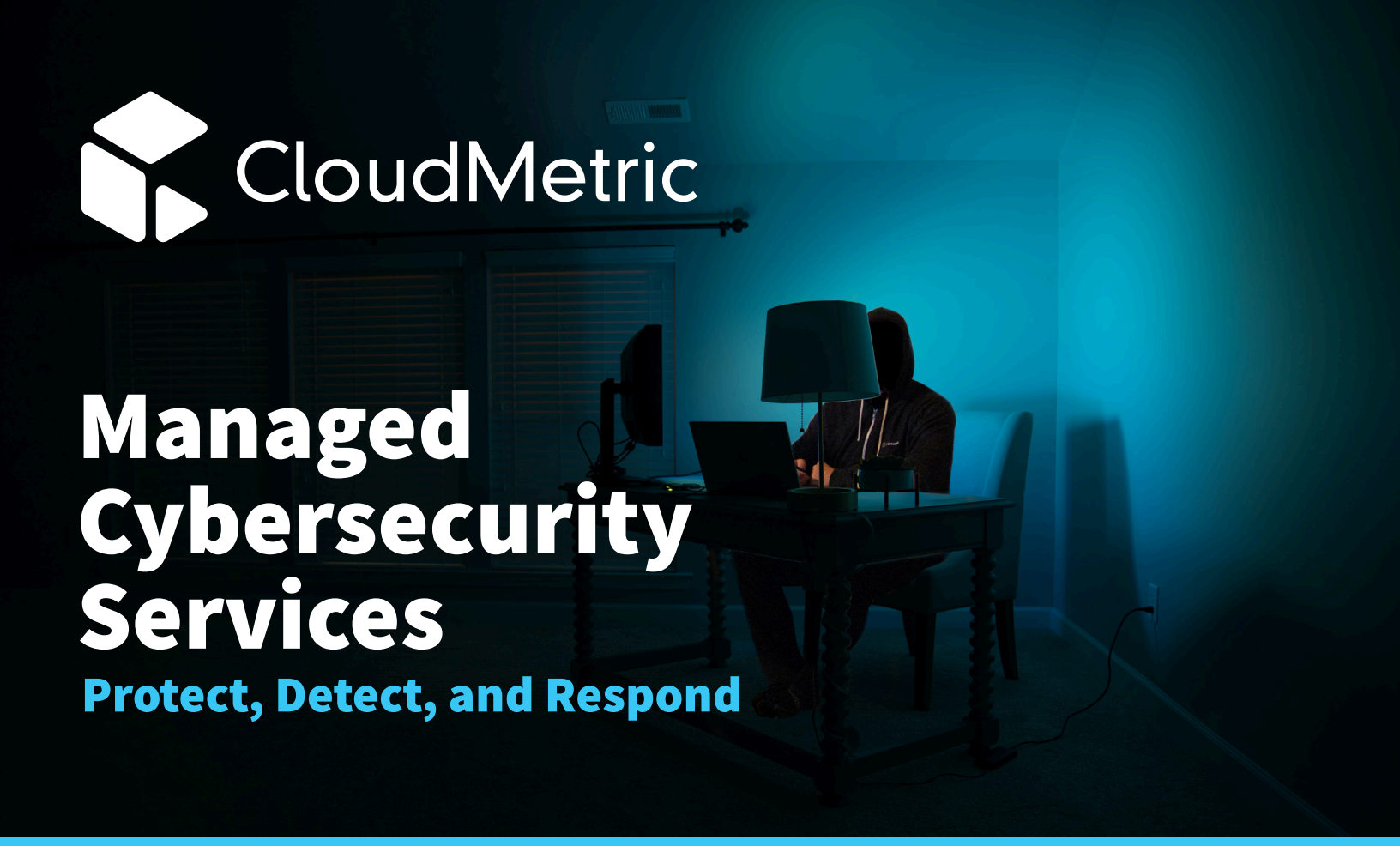
CloudMetric



Managed Cybersecurity Services

Protect, Detect, and Respond

Because Your Business IS AT RISK!

A Wake-Up Call for Businesses

Statistics confirm that businesses of every size need to evaluate their current cybersecurity practices. With a **600% increase** since the pandemic, the cost of cybercrime is estimated to be around **1% of global GDP**. Canada is no exception! Nearly **60 percent** of Canadian organizations were **targeted by ransomware** attacks in 2022, costing Canadian organizations **$5.6 million USD**.

Anti-Virus is Insufficient

In a world where cyberattacks are growing, traditional anti-virus solutions are simply not enough. **Anti-virus vendors can not keep up** with the development of new cybersecurity threats. The number of threats for desktop and mobile devices, social media, and cloud services is ever increasing. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit **$8 trillion worldwide in 2023** and will grow to **$10.5 trillion by 2025.**

Managed Security

What is Endpoint Detection & Response (EDR)?

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware. EDR is defined as a solution that records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems.

What is Managed Detection & Response (MDR)?

Managed Detection and Response (MDR) is a cybersecurity service that combines EDR technology and human expertise to perform threat hunting, monitoring, and response. The main benefit of MDR is that it helps rapidly identify and limit the impact of threats without the need for additional staffing. These experts are on call around the clock, so they can rapidly respond based on their knowledge of every aspect of endpoint security, from detection to restoring the endpoint to a known good status to preventing further compromise.

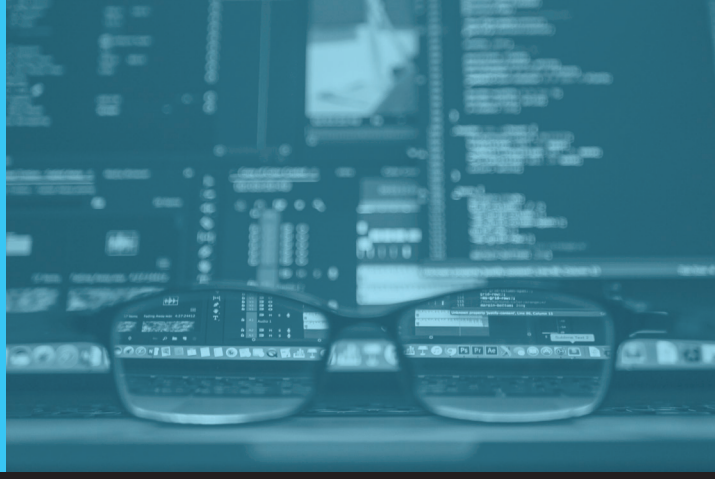
What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack. MFA is based on three elements: Things you know (password / PIN); Things you have (smartphone / badge); and Things you are (fingerprints, retina).

Receive peace of mind with managed endpoint detection and response.

CloudMetric
www.cloudmetric.ca
1.833.323.7905

A Multi-Layer Approach



The Huntress Managed Security Platform

The Huntress Managed Security Platform is recommended as the first layer of protection. Huntress offers advanced threat detection and response and is monitored 24/7/365 for fast detection & response. Features include:

- 1-Click Remediation
- Next Generation Anti-Virus
- Auto Host Isolation
- Process Insights
- Footholds
- Open Port Scanner
- Application Whitelist
- Windows Workstation / Server Protection
- Ransomware Canary
- Detailed Reporting

SentinelOne Singularity Control

For an additional layer of protection, SentinelOne Singularity Control is recommended. While this layer offers much of the same features, it also offers additional protection that include:

- 1-Click Recovery
- Firewall Control
- Linux Server Protection
- Mac Protection
- Cloud Protection
- USB & Bluetooth Device Management
- Application Inventory and CVE's
- Import of Non-Native Data
- Marketplace Apps

Duo Multi-Factor Authentication by Cisco

DUO MFA is recommended to keep your employee logins secure and optimized for productivity. Features include:

- Multi / Two Factor Authentication
- Mobile App with Push Notifications
- WebAuthn and Biometrics Support
- Single Sign-On Support
- Cloud Support
- Device Insight Overview
- Access Controls

Speak to a cybersecurity expert before it's too late!

CloudMetric
www.cloudmetric.ca
1.833.323.7905

Take Proactive Measures

FREE Risk Assessment

Risk assessments help organizations understand, control, and mitigate all forms of cyber risk. Taking our FREE risk assessment is the first step to evaluating your current security controls and vulnerabilities.

In-Depth Cybersecurity Assessment

An in-depth cybersecurity assessment is a critical component of a risk management strategy, data protection efforts, and insurance compliance. More than just a checklist, It analyzes your organization's cybersecurity controls and their ability to remediate threats.

Automated Network Penetration Testing

While assessments capture a point-in-time snapshot. Penetration testing can perform a live, full-scale control test (firewall restrictions, configuration changes, etc.). A penetration test can also measure the effectiveness of these controls through its exploitation techniques.

Cybersecurity Awareness Training for Employees

Cybersecurity awareness training educates employees to understand common types of social engineering attacks like phishing and spear phishing. This can be taken one step further by conducting phishing simulations. Training can be performed in person or online.

CloudMetric

Cybersecurity isn't easy,
but it comes down to three basic principles:
Protect, Detect, and Respond

www.cloudmetric.ca

1.833.323.7905