

24/7 MDR/SOC Service

Our expertise.
Your peace of mind.

No matter where cyber threats are hidden, or what they are, Virtual Guardian is here to protect you. Our 24/7 Managed Detection & Response (MDR) and Security Operations Center (SOC) services safeguard your organization from digital assaults so you can focus on what matters – running your business.

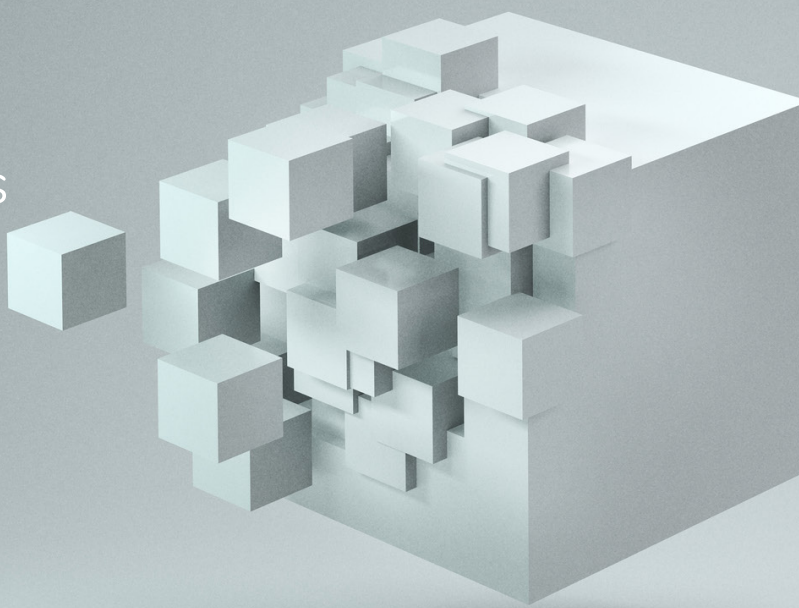
In operation since 2011, Virtual Guardian's SOC meticulously scrutinizes network and user activities to swiftly detect and mitigate attacks, continuously monitoring events, log files, user behaviors and network traffic while also ensuring compliance with legal and cyber-insurance requirements.

Our cybersecurity experts have deep knowledge of the current threat landscape. They will identify advanced attacks and insider risks by devising detection protocols and use cases capable of promptly identifying suspicious activities within moments. Through the implementation of best of breed advanced technologies like SIEM (Qadar), SOAR (Revelstoke)

VMDR (Qualys) and XDR (CrowdStrike and Microsoft), our security specialists swiftly and effectively respond to threats. You can rest assured that our team is working with the highest quality information possible, guaranteeing effective and efficient results for your cybersecurity monitoring and response.

When suspicious events or patterns are discovered, our SOC team conducts fast, thorough investigations to stem the risks to systems and employees. This prompt response and communication to your organization, minimizes the potential impacts of cyber threats to your operations.

The dangers
are real.
The solution is
simple.



Virtual Guardian can
identify risks and offer
end-to-end and on-going
management to help
protect your systems and
data from outside threats.



Virtual Guardian's 24/7 MDR/SOC service offers THE most complete cybersecurity feature set:

WORLD-CLASS COVERAGE SERVICE

- 24/7 Always-on monitoring & cyber analyst support
- 24/7 Threat disruption & containment support
- Named cyber risk advisor (reporting, communication & collaboration every month)
- Detailed escalations w/ analysis & recommendations
- Automated and rapid human-led investigations, threat containment & remediation
- Detections mapped to Mitre Att&ck framework
- Threat intelligence, research & thought

COVERING ALL ANGLES OF ATTACK

- Continuous user & entity behavior analysis (UEBA)
- Ransomware, brute force, phishing, dos attack and mores use cases reaction included
- Multi-source coverage & visibility (on-prem, clouds, O365 account monitoring, etc.)
- Automated detections w/ signatures, behavioral analytics, IOC & IPS security network effects
- Network analysis (i.e. unauthorized lateral movement detection)

ADAPTED TO YOUR REALITY, PERSONALIZED TO YOUR NEEDS

- 24/7 or evening/nights/weekend
- Anti-ransomware protection
- Vulnerability Management & Automated Patching
- Dark web monitoring
- Endpoint detection & response



287 6th Street E,
Suite 500,
St. Paul, MN 55101

1550 Metcalfe Street,
Suite 1100,
Montréal, Québec
H3A 1X6

130 Adelaide St. W.,
Oxford Tower
Suite No. 2202
Toronto, ON M5H 3P5

1255 Lebourgneuf Blvd,
Suite 270
Québec (Québec) G2K 0M6

+1 -800-401-TECH (8324)

www.virtualguardian.com

www.gardienvirtuel.ca

© 2024 VirtualGuardian, Inc. All rights reserved.