cabco

END-POINT PROTECTION SOLUTIONS

End-Point Protection (EPP)
End-Point Detection and Response (EDR)

cabco

What is an **End-Point Protection Platform (EPP)?**

An endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Cabco's advanced endpoint protection solutions employ a comprehensive strategy that incorporates multiple technologies. These technologies work in tandem, constantly optimizing performance, detection rates, and minimizing false positives. By adopting a multilayered approach, Cabco ensures a robust defence system that efficiently safeguards endpoint devices.

What is an **End-Point Detection and Response Solution (EDR)?**

The EDR-enabling component of Cabco's end-point solutions is a tool for the identification of anomalous behaviour and breaches, risk assessment, incident response, investigations and remediation.

It empowers incident responders to actively observe and assess all network activities and connected device operations. Additionally, it offers automated capabilities for promptly implementing remedial measures, if required.

More on **EPP** and **EDR**

Endpoint Detection and Response (EDR) isn't new. It is an evolution, merging the prevention inherent in Endpoint Protection (EPP) products, with the response and remediation to eradicate infections that successfully penetrate those defenses. EDR solutions enable organizations to align with popular attack response frameworks from organizations like NIST in the USA and ENISA in Europe. With EDR, organizations can identify threats outside of their ecosystem, detect when something suspicious penetrates their defenses, investigate, and appropriately remediate confirmed infections.

EDR platforms are rated by a number of independent testing organizations, as well as industry analysts. While industry analysts such as Gartner and Forrester require vendors to hold customers of a certain size and/or seat count to be considered for their Magic Quadrant and Wave reports, respectively, independent testing organizations such as MITRE Engenuity focus on pure product performance in their analysis.

EDR continues to expand in definition (terms such as XDR) and method of implementation, with MDR (Managed Detection & Response) as an alternative to in-house management of endpoint security. Still, EDR remains the common market term for this solution, which is typically associated with the detection and remediation side of cybersecurity. Cabco helps prevent the evildoers from getting into your environment, and that is backed by our proven remediation when something gets past those preventative measures.

Importance of End-Point Solutions - **EPP and EDR**

RANSOMWARE

Since the emergence of Cryptolocker in 2013, ransomware has become a persistent concern for industries worldwide. Although ransomware had been around for a while, it was not previously recognized as a significant threat to businesses. However, a single instance of ransomware today can easily cripple a business by encrypting vital files, rendering its operations inoperable. In such situations, businesses may realize that their backups are not up to date, tempting them to consider paying the ransom.

Cabco's endpoint protection solutions offer a robust defense against ransomware, employing multiple layers of security. They not only aim to prevent ransomware attacks but also possess the capability to detect and respond to any potential occurrence within an organization. It is crucial to prevent and detect ransomware as every instance of paying a ransom encourages criminals to perpetuate this mode of attack.

68%+

of firms suffered recent attacks and 80% were new “zero-day” threats.

TARGETTED ATTACKS AND DATA BREACHES

In addition to detecting a data breach, companies must effectively contain and remedy it without causing disruptions to their business operations. Conducting a thorough investigation of such incidents requires precision and expertise, which many businesses may lack. Consequently, they often rely on external vendors to provide the necessary assistance. Nowadays, organizations require enhanced visibility into their computer systems to safeguard against emerging threats, mitigate risky employee behaviors, and prevent the presence of unwanted applications that could jeopardize their profitability and reputation.

Traditionally, industries handling valuable data such as financial, retail, healthcare, and the public sector have been prime targets for data breaches. However, this does not imply that other industries are immune to such threats. Hackers typically assess the effort required versus the potential payoff, making it crucial for all industries to remain vigilant and prioritize cybersecurity measures.

FILELESS ATACKS

Fileless malware, a newer type of threat, operates exclusively in computer memory, making it challenging for file scanning-based security measures to identify them. Additionally, some fileless attacks exploit pre-existing applications embedded within the operating system, further complicating the detection of malicious payloads. A notable example is the frequent use of PowerShell in such attacks.

To combat these fileless threats, Cabco's endpoint protection platforms incorporate specific mitigations to detect and protect against malformed or compromised applications. Additionally, Cabco has developed dedicated scanners that continually monitor computer memory for any suspicious activities. By adopting this multilayered approach, Cabco ensures proactive defense, staying ahead of the latest malware trends.

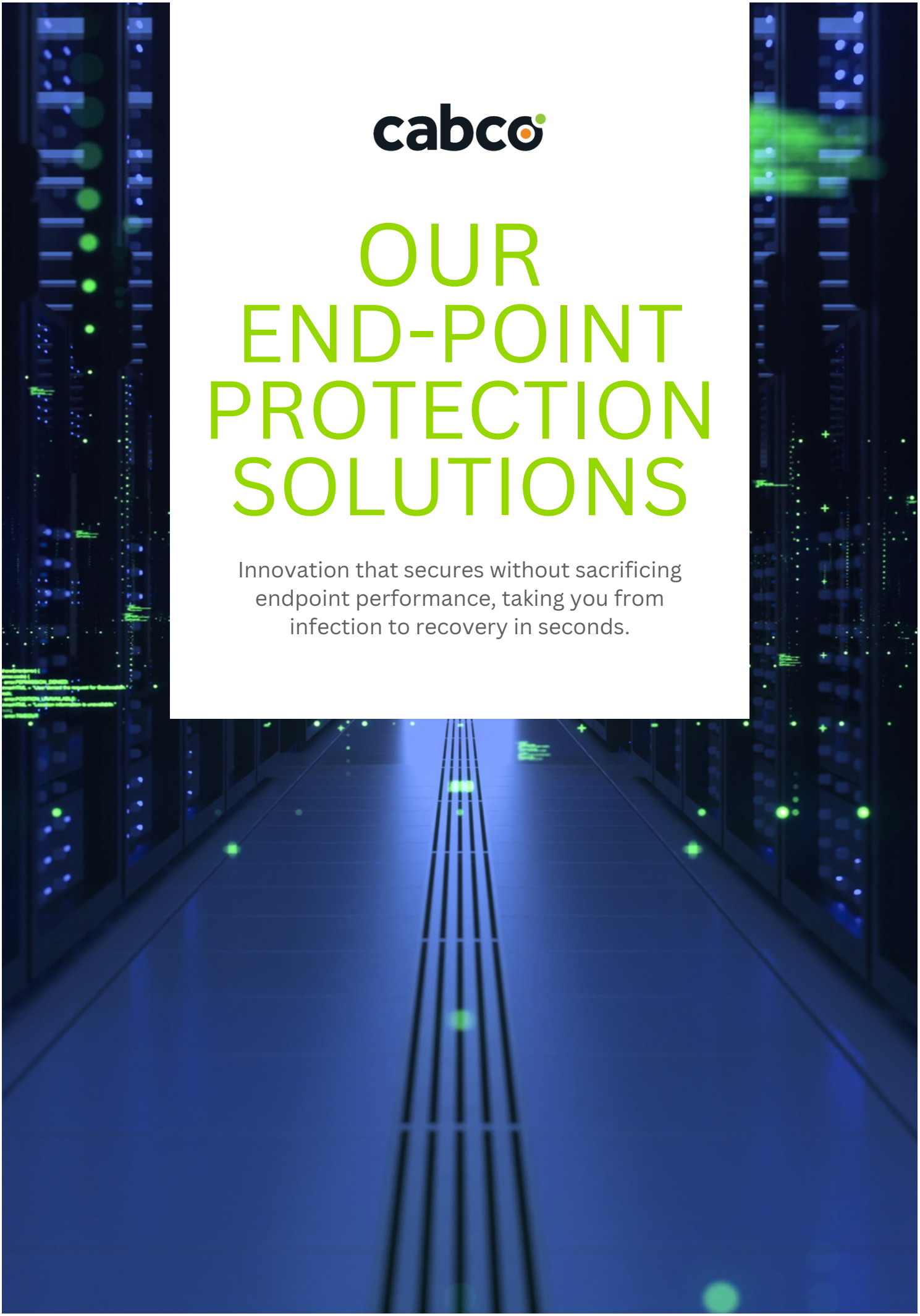
INSIDER THREATS AND PHISHING ATTACKS

Enterprise businesses face significant challenges from insider threats and phishing attacks. Phishing attacks are particularly pervasive in enterprise environments due to the large number of employees available as potential targets. The likelihood of a single employee falling victim to a phishing attempt increases, thereby compromising the entire organization. Similarly, insider attacks pose a threat to enterprises as the sheer volume of employees raises the possibility of an individual acting against the best interests of the company.

To address these concerns, EDR systems offer organizations the essential visibility required to detect, understand, prevent, and remediate issues across all their devices. By leveraging such technology, organizations can enhance their security posture and mitigate the risks associated with insider threats and phishing attacks.

$240k

that’s the average cost of a ransomware attack.



cabco

OUR END-POINT PROTECTION SOLUTIONS

Innovation that secures without sacrificing endpoint performance, taking you from infection to recovery in seconds.

Cabco **Managed EDR** - Lite

In partnership with Malwarebytes

Cabco Managed EDR - Lite is an Endpoint Security solution which addresses advanced threats that leverage different attacks vectors and techniques.

FEATURES

EASY
• Non-disruptive, deploy within minutes.
• One endpoint agent, simple integration.
• Intuitive cloud-native management console.

EFFECTIVE
• Detects “zero-day” threats with low false positives.
• Granular isolation for processes, networks, and Windows desktops.
• Removes executables, artifacts, and changes.

EFFICIENT
• Single lightweight agent, no performance impact.
• 72-hour ransomware rollback for Windows.
• Low total cost of ownership (TCO).

INTEGRATED PROACTIVE ENDPOINT PROTECTION
• Includes automated adaptive detection techniques that learn along each stage of the threat detection funnel.
• Finds and blocks threats before devices are infected.
• Proactively and accurately recognizes and prevents both hostile code and suspicious behaviour.

OPERATING SYSTEM-SPECIFIC ISOLATION MODES
• provides multiple combined modes of endpoint isolation.
• *Network isolation* limits device communications to ensure that attackers are locked out and malware can’t “phone home.”
• *Process isolation* restricts which operations can run, halting malware while still allowing users to remain productive.
• *Desktop isolation* for Windows workstations alerts users to threats and temporarily blocks access while keeping the device online for analysis.

BUSINESS HOURS CABCO SERVICE DESK
Endpoint security monitoring, management, and support include active threat hunting, forensic mapping, continuous investigation, triage, and response to threats.

cabco

Cabco **Managed EDR** - Premium

In partnership with SentinelOne

Cabco Managed EDR - Premium delivers autonomous security for the endpoint, datacentre and cloud envrionments, helping organizations to secure their assets with speed and simplicity.

FEATURES

BUILT-IN STATIC AI AND BEHAVIORAL AI ANALYSIS

Prevent and detect a wide range of attacks in real time before they cause damage. Core protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.

SENTINELS ARE AUTONOMOUS

which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real time.

RECOVERY IS FAST

and gets users back and working in minutes without re-imaging and without writing scripts. Any unauthorized changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.

SECURE SAAS MANAGEMENT ACCESS.

Choose from US, EU, APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.

24X7 DEDICATED CABCO SOC TEAM

Endpoint security monitoring, management, and support include active threat hunting, forensic mapping, continuous investigation, triage, and response to threats.

INVESTIGATE HISTORICAL DATA WITH AFFORDABLE EXTENDED DATA RETENTION

The ability to look back into any point in time allows analysts to see if the threat has targeted your organization in the past and view the full stream of information on how that attack occurred, including the entire process tree, timeline, and related activities. SentinelOne provides visibility into your environment with 365 days and beyond of EDR data to let the Cabco SOC team analyze incident activities and conduct historical analysis within the same UI.

cabco

cabco

Plans

Products and Services to **fit your unique business needs**

	Lite	Premium
Audience	Organizations of all sizes that need standard Endpoint protection	Organizations and businesses that want an all-in-one endpoint protection platform
Support	Self-Managed	• 24/7 monitoring and management by Security Operations Center • Online Support
Training		• Documentation • Webinars • Live Online • In Person
Features	• Web Protection: Prevents access to malicious websites, ad networks, scammer networks, and bad neighbourhoods • Application Hardening: Reduces vulnerability exploit surface and proactively detects fingerprinting attempts used by advanced attacks • Exploit Mitigation: Proactively detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint • Application Behavior Protection: Prevents applications from being leveraged to infect the endpoint • Anomaly Detection: Proactively identifies viruses and malware through machinng learning techniques • Payload Analysis: Identifies entire families of known and relevant malware with heuristic and behavioral rules • Ransomware Mitigation: Detects and blocks ransomware via behavioral monitoring technology	• ActiveEDR allows users to track threats in real time, as they happen • Respond & Recover at machine speed. Maintain context for easy threat hunting • OS and Deployment Diversity - The broadest platform coverage across Windows, Mac, and Linux natively cloud-based or available on-prem • Offers more than 300 APIs for seamless and thorough integrations • SentinelOne's patented technology links all behaviours and indexes all activities into a storyline on the agent, in real-time • Empowers security analysts- Analysts can hunt faster, focusing on what matters, instead of wasting time looking for the needle in the stack • Alert reduction- Malicious attempts are prevented in real-time, reducing overall risk and alert fatigue all too common with other EDR products

CONTACT US FOR PRICING

Interested in learning more? Give us a call! We're happy to help you choose the perfect EDR Solution for your business.

1-800-675-4025

Sales@cabco.ca

https://www.cabco.ca/

200 - 2 Ralston Avenue,
Dartmouth, NS B3B 1H7

65 King St,
Moncton, NB E1C 0A3

711 Woodstock Rd,
Fredericton, NB E3B 5N8