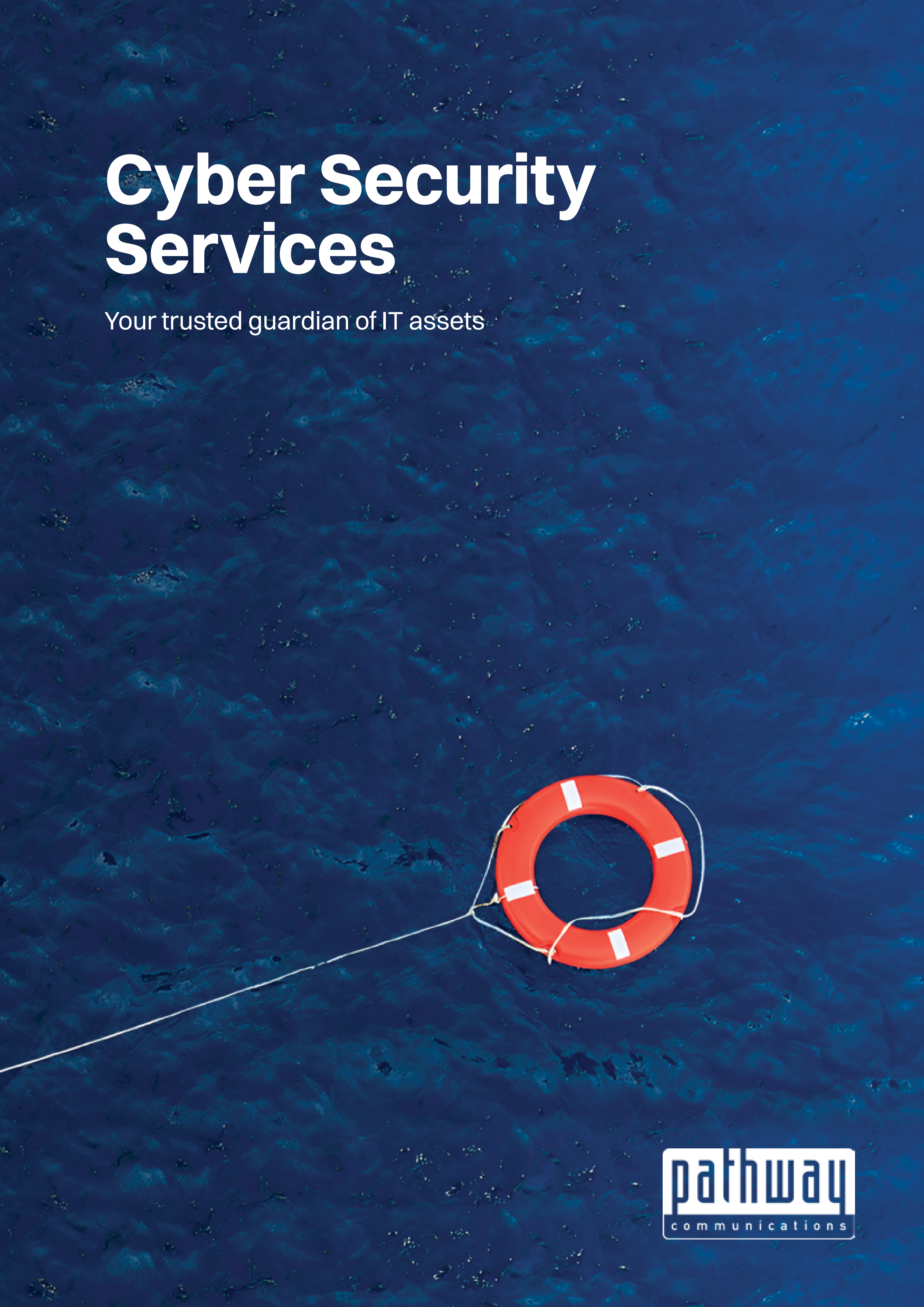
Cyber Security Services

Your trusted guardian of IT assets



pathway
communications

Security is no longer an option. It's a necessity.

Technology keeps evolving. So does the severity and number of cyber attacks.

From exploiting vulnerabilities in software to tricking users into revealing sensitive information, cyber attackers keep coming up with new techniques every hour to gain access to your IT systems. If your confidential data is not protected with top-notch defence mechanisms round-the-clock, it becomes vulnerable to cyber attacks and data breaches, making it easier for hackers and cyber criminals to gain unauthorized access to the data.

Cyber crime has been up **600%** since COVID-19

A ransomware attack succeeded every **40 seconds** in 2022

Over **560,000** new pieces of malware are discovered every day

91% of cyber attacks begin with a spear phishing email

SMB

Over **43%** of attacks are aimed at SMBs

USD 4.35 million
Average total cost of a data breach

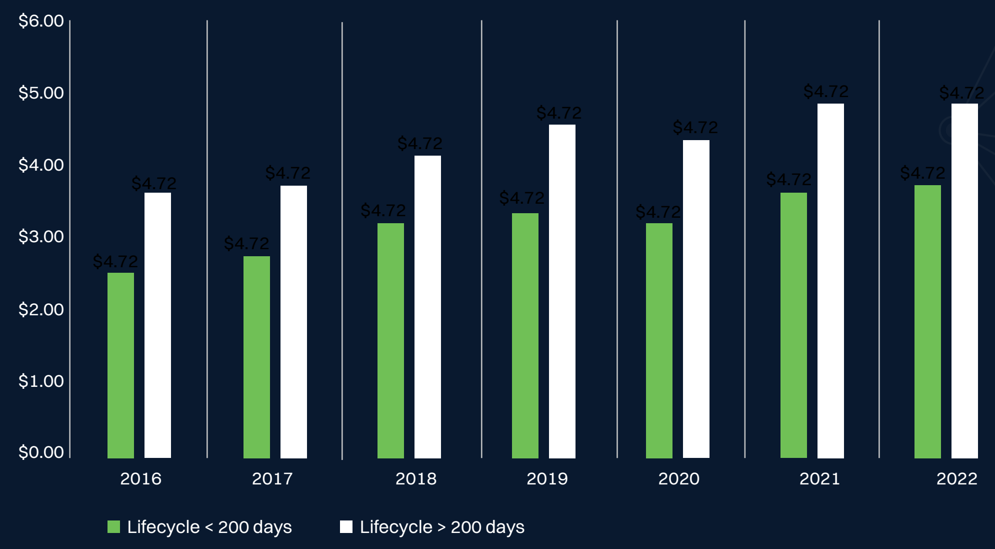
USD 4.82 million
Average cost of a critical infrastructure data breach

USD 4.54 million
Average cost of a ransomware attack, not including the cost of the ransom itself

USD 4.91 million
Average cost of data breach with a phishing initial attack vector

$2.8 billion
The total cost of over 700,000 cyber attacks against SMBs in 2020

Average cost of a data breach based on data breach lifecycle



Source: IBM

Cost of cyber attack

The cost of a cyber attack can vary greatly depending on the size and scope of the attack, as well as the industry and specific organization affected. Costs can include direct expenses such as remediation and recovery, legal fees, and loss of revenue or business. In some cases, cyberattacks can result in significant financial loss due to the theft of money.

Beyond financial loss: The true cost of cyber attacks

In addition to causing financial losses, cyber attacks can have severe and far-reaching consequences for your business. Some of them are:

- Loss of data
- Loss of customers, partners, and investors
- Damage to reputation and trust
- Legal liabilities
- Loss of competitive advantage
- Disruption of business operations (productivity and revenue loss)
- Loss of intellectual property

Stay secured. Stay productive.

Cyber threats constantly evolve, and **businesses of all sizes and industries** are always at risk. So, having comprehensive and proactive security measures, such as regular vulnerability assessments, security awareness training, and implementation of security best practices, in place can help you stay ahead of the threats and reduce the risk of cyber attacks. It enables you to prevent attacks before they occur rather than reacting to them after the damage is already done.

While security tools are necessary, they alone cannot protect organizations. It is the people, who are continuously monitoring, configuring, and tuning the tools and are able to leverage them to respond faster and better to security incidents, that make the difference.

Companies saw a **42% reduction in cyber risks** after implementing an integrated risk management strategy

Organizations experienced a **45% reduction in the cost of cyber attacks** after deploying security information and event management (SIEM)

Organizations saw a **50% reduction in cyber incidents** after investing in cybersecurity measures

Benefits of arming your IT systems with security solutions

- Protection against cyber threats
- Improved compliance
- Increased productivity
- Enhanced customer trust
- Cost savings
- Better decision-making

Pathway Cyber Security Services

Give your IT assets the elite security they deserve

Pathway Communications offers end-to-end security solutions for infrastructure and application monitoring, threat detection, visibility, and response. Our security platforms collect data from several sources and endpoints, analyze and present them for visualization in dashboards. This allows Security Analysts to immediately detect, identify, investigate, and respond to potential threats and adverse events.

We prevent

- Security assessments and audits to identify vulnerabilities and risks in your system
- Penetration testing to simulate real-world attacks and identify weak spots in your defences
- Security training and awareness programs to educate your employees on safe online behaviour and best practices

We protect

- 24/7 security monitoring by our expert SOC team, using state-of-the-art tools and technologies
- Real-time threat detection and response to minimize the impact of any security incidents
- Continuous vulnerability scanning and patch management to ensure your system is always up-to-date and securebehaviour and best practices

We resolve

- Incident response planning and execution to minimize the damage of a security incident
- Forensic investigations to determine the cause of a breach and prevent it from happening again
- Data recovery and restoration services to get your system back up and running as quickly as possible

Our holistic approach to cyber security

Assess

Our Security Analysts conduct a thorough risk assessment to identify and analyze potential risks and vulnerabilities in your organization's IT assets and systems. We will use a combination of IT Security Audits, Vulnerability Assessments, Penetration Tests, and customized assessments (based on the specific threat landscape and regulatory/legal requirements) to analyze current security posture and related gaps.

Develop & Implement

Based on the risk assessment results, our team of experts develops a customized security plan based on your budget and existing security setup to mitigate the identified risks and threats. This plan is designed to remediate critical gaps and easy wins that can immediately help your organization minimize cyber risks.

Monitor

Pathway uses different SIEM (Security Incident and Event Monitoring) technologies that can be customized based on your requirements to detect threats, ensure compliance, and manage security incidents. Through the lightweight agents on your devices and network, SIEM technologies collect, ship, analyze, visualize, and store detailed performance data, such as response time for requests, database queries, calls to caches, failed password attempts, external HTTP requests, and more.

We gather this real-time information from multiple endpoints, whether they are located on-premises, in a data center, or in the cloud. This helps us to quickly detect any anomalies or threats and take action to mitigate them. Our agent policies are continuously updated to incorporate new data sources, patterns, and protection methods to keep your system secure.

Detect

Pathway Security Analysts validate each detected threat to eliminate false positives and ensure that only the real threats are dealt with. Our threat detection relies on multiple protocols:

- End user and device behaviour anomalies (UEBA)
- Network Traffic Analysis (NTA)
- Comparison of signatures and features from threat intelligence feeds
- Proactive threat hunting by SOC Analysts
- Intruder deception methods such as honeypots

All our detection efforts are based on the Indicators of Compromise (IOCs) aligned to the MITRE ATT&CK™ framework. This framework is a global knowledge base that captures attackers' real-world tactics and techniques. With these methods, we can provide top-notch security solutions for your business.

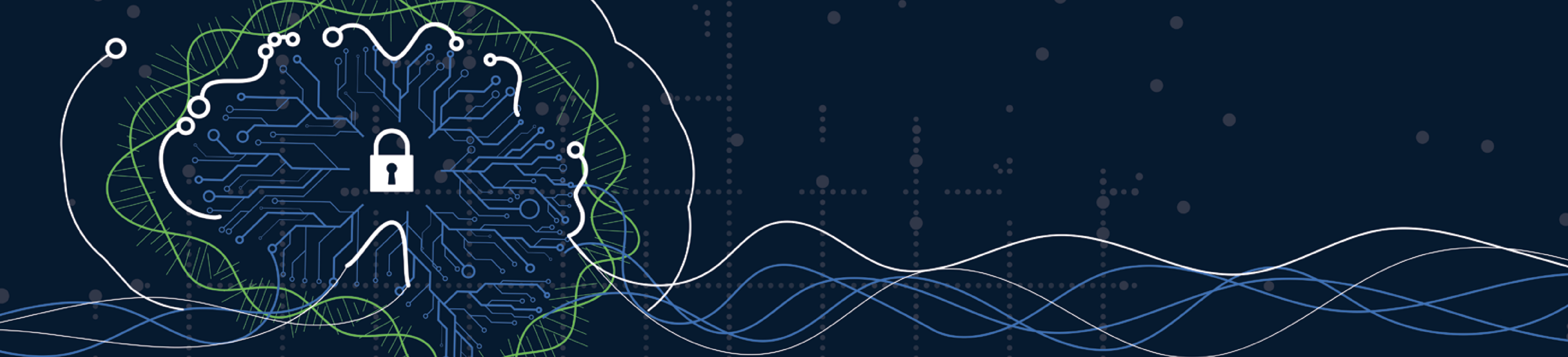
Respond & Remediate

When an alert is confirmed to be a real threat, Pathway's security team quickly investigates and prioritizes the event. Senior security engineers handle such events and take steps such as isolating, confining and stopping the attack. Some remedial measures are automated using software playbooks, while others require careful examination by experts following standard operating procedures.

We work like an extension of your IT teams to remediate cyber incidents in a timely manner. We develop procedures and operational guides that ensure all remediation activities are seamless and timely. After a genuine threat is detected and remediated, Pathway's experts conduct a thorough analysis to identify the source, timeline, and path to the event. This information is used to implement preventive measures promptly. We partner with corporations and professionals who can perform advanced forensic inspections to aid this process.

Improve

Pathway's SIEMs detect anomalies in your systems by comparing real-time data against normal functions. However, as new threats, breaches, and malware emerge every day, we also compare the data against new and evolving threat signatures and patterns to stay ahead of cyber attackers. Our sources for this information come from commercial threat intelligence feeds delivered by multiple providers. In addition, we also perform regular security assessments, penetration testing, and training programs for our staff to continuously improve our service to you.



Our offerings

Managed Security Services (MSS)

Protect	Detect	Respond	
Firewall Keep away the unauthorized traffic and ensures network security			**Managed Detection and Response (MDR)**
Anti-phishing Identify and block the phishing attack in real time	Identify vulnerabilities through Vulnerability Assessment & Penetration Testing **(VAPT)**	Prioritise, mitigate, and remediate identified vulnerabilities through **Patch Management**	**Vulnerability Management**
SD-WAN Improve application performance and agility	Identify threats through **Threat Intelligence**, which provides information on prevailing attacks	Hunt and remediate malware/malicious activities through **Threat Hunting**	**Threat Management**
	Detect threats, ensure compliance, and manage security events/incidents through **SIEM**	Accelerate security operational activities and automate the responses through **SOAR**	**Security Operation Center (SOC)**

IT Advisory /Assessment Services

- Cyber security Assessments
- Cyber Insurance Readiness
- Data Security and Privacy Assessment
- Network/Infrastructure Security Assessment
- Endpoint Security Assessment
- Training/Awareness Exercise
- Virtual CISO/Cyber security Advisories as needed

Professional Services

- Security Tools POCs
- Security Tools Implementation
- Runbooks
- Operational Guides
- Security Tools Operations
- Security Tools Management:
  - Firewalls
  - Web Application Firewalls
  - Email Gateways
  - DLP
  - EDR
  - IPS/IDS

Our capabilities

Managed firewalls, endpoint, and content protection

- Intrusion detection and prevention
- Managed patching and custom rule design
- Email firewalls for data leak prevention
- Endpoint monitoring and scans
- Software security compliance testing

Security Information Event Management and Analysis (SIEM)

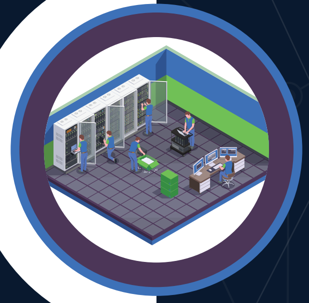
- Logging and sensor deployment and management
- Log analysis
- Visualization and dashboards
- Pattern analysis and deviation alerts

Professional services

- Infrastructure penetration testing and remediation
- Network and systems review and design
- Operational continuity and disaster recovery design, testing, and audit
- Policy design and enforcement
- Vendor and supplier security review

Security Operations Center (SOC)

- Customized services that span policies, technology, and personnel
- Realtime monitoring and response
- 24/7 coverage
- Account management
- Executive reporting



The Pathway advantages

Fully-equipped, world-class Security Operation Center (SOC)

Our Security Analysts conduct a thorough risk assessment to identify and analyze potential risks and vulnerabilities in your organization's IT assets and systems. We will use a combination of IT Security Audits, Vulnerability Assessments, Penetration Tests, and customized assessments (based on the specific threat landscape and regulatory/legal requirements) to analyze current security posture and related gaps.

24/7 access to SOC Cyber Analysts and Elite Threat Hunters

Pathway offers 24/7 access to our team of SOC Cyber Analysts and Elite Threat Hunters so that you can turn to us for help at any time. This helps to reduce the impact of cyber incidents and minimize downtime, ultimately saving you time and money. Additionally, the peace of mind that comes with knowing that expert support is always available can help you to feel more secure and confident in your cyber security posture.

SMB-friendly

Threats can emerge at any time, day or night. That's why Pathway offers around-the-clock Managed Detection and Response (MDR), which combines continuous monitoring of all assets, accurate alerts, detection, and rapid response to cyber security events. This ensures your IT infrastructure and applications are properly configured, hardened, and protected with the help of our world-class Security Operations Centre (SOC), which monitors, detects, and responds 24/7.

Customization

Pathway offers a complete range of security services with budgets of any size. These include packages of bundled services or individual ("a-la-carte") services which cater to the specific needs of our clients.

Certified experts

Pathway's team of experienced professionals has expertise in cybersecurity, including risk management, threat analysis, incident response, and compliance. They have a wide range of skills and technical certifications for proactive monitoring to support your business.

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certified Information Systems Auditor (CISA)
- Cisco Certified Internet Engineer (CCIE) - security and routing
- Unix System Administrators
- Microsoft Certified Solutions Expert (MCSE)
- Microsoft Certified: Azure Solutions Architect (MCASA)

24/7 vigilance against threats

Threats can emerge at any time, day or night. That's why Pathway offers around-the-clock Managed Detection and Response (MDR), which combines continuous monitoring of all assets, accurate alerts, detection, and rapid response to cyber security events. This ensures your IT infrastructure and applications are properly configured, hardened, and protected with the help of our world-class Security Operations Centre (SOC), which monitors, detects, and responds 24/7.

Our technology partners for advanced cyber security

Pathway uses a variety of vetted commercial software platforms and tools to deliver the best security services.

Microsoft

RAPID7

DUO

Google

Kaseya

ZABBIX

tenable

KnowBe4

OPMANTEK

FORTINET

Bitdefender

About Pathway Communications

Pathway Communications specializes in providing innovative and cost-effective IT and communication solutions for businesses of all sizes. Rooted in Canada, we offer a wide range of services, including Managed IT Services, Cybersecurity Solutions, Data Center, Cloud, Colocation, Voice, Data, and Internet, to help our clients stay connectedand operate securely in today's fast-paced world.

ISO 27001 & 27002

ISO 27018:2014

ISO 9001 2015 CERTECH

AICPA SOC

PIPEDA

PHIPA COMPLIANT

SAP® Certified in SAP HANA® Operations Services

HIPAA COMPLIANT

PCI DSS CERTIFIED

The certifications mentioned above represent a selection of our achievements and do not encompass the complete range. Please get in touch with us for a comprehensive list of our certifications.

pathway communications

Follow us for regular updates

Contact us

☎ +416-214-6363

✉ sales@pathcom.com

95 Apple Creek Blvd., Markham

www.pathcom.com

Scan the QR code to visit our website

Disclaimer: The images featured in this brochure are for illustrative purposes only.