C&W Business

Cybersecurity
Local presence, Global expertise

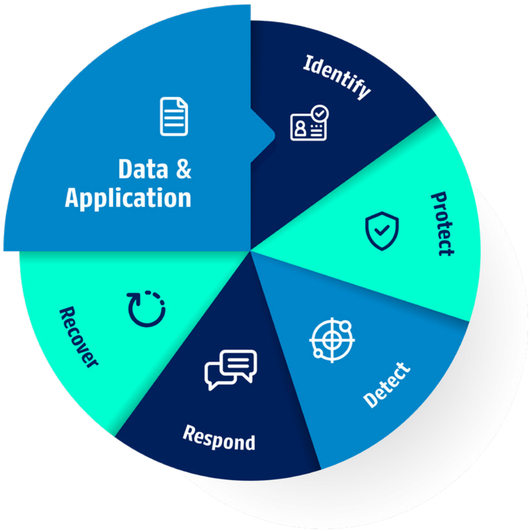
Protecting your network and data

A comprehensive cybersecurity solutions overview

Fortifying your digital landscape defences

Protecting your technology infrastructure is our priority. Your business data will be safe with our real-time monitoring, comprehensive application protection, robust infrastructure defences, and expert security advice.

Our portfolio of 24/7 security solutions provides reliability, flexibility, and effectiveness. The solutions align with the NIST Cybersecurity Framework and are built on state-of-the-art technology. They function under the support of a Security Operations Centre (SOC) that operates at all times, every day of the year, monitoring threats and evaluating the measures to be taken. With our solutions, your information is secure, your revenue is protected and your reputation is safeguarded.



Securing all your devices and endpoints

Every device that connects to your network poses a threat and has the potential to become the most vulnerable point in your IT infrastructure.

Risk	How we can help
An employee clicks a link in a phishing email.	**Protective** features help block malicious code, viruses, and other intrusions.
An unauthorised user connects to the company's network with their device.	**Preventive** measures include authentication, access control, data encryption, and security policies.
A contractor uses an unsecured personal device to access the company's network.	**Defensive** actions ensure secure passage to your network for remote workers.
Hackers don't work from 9 to 5–you must protect your platform every minute.	**Proactive** monitoring continuously surveils the network for threats.

Endpoint protection

Our Security Engineers continuously monitor your devices to discover and remove cyberthreats such as malware. We maintain real-time visibility of any threats with an automated troubleshooting process that provides quick and effective resolution, including the restoration of your compromised files and systems. We do it all from an easy-to-access platform that provides you with detailed information about each event.

Protecting your apps and data

To effectively safeguard applications and data, such as emails and websites, organisations must go beyond traditional firewalls and adopt a holistic security strategy. This strategy should include implementing layered security measures like encryption and advanced threat detection and ensuring continuous monitoring. Specific attention must be given to preventing business email compromise and protecting against website defacement. These approaches help detect, prevent, and mitigate attacks, thereby protecting user data and privacy while maintaining operational resilience.

Risk	How we can help
Varied web application and email attacks that cause data loss or service interruptions.	Real-time monitoring that prevents network intrusions while detecting and identifying threats.
DDoS attacks overwhelm servers, creating downtime that could harm your reputation and affect your revenue.	Bandwidth protection against attacks that identifies and mitigates traffic overload attempts via cloud-based services.

Web Application Firewall

With our Web Application Firewall solution, you gain an additional layer of protection to safeguard your applications. We detect and block threats like cross-site scripting, SQL injection, and defacement attacks while issuing alerts to keep you informed. We also identify secure connection locations, allowing you to operate with peace of mind.

Email Security

We provide advanced email security services to protect against phishing, malware, viruses, spyware, and spam. To do this, we combine multiple tools, including content filters, phishing detectors, authentication systems, and behavioural analysis applications. We also offer Data Loss Prevention (DLP) services to safeguard sensitive information.

DDoS Protection

Our DDoS Protection service uses scrubbing centres to filter malicious traffic, ensuring that only legitimate data reaches your servers. We also protect against protocol and application layer attacks through a combination of on-premises hardware and software solutions.

Strengthening your network security

With the increase in the number of network-connected devices—including IoT devices ranging from lightbulbs to more sophisticated technology, which often lack strong security—companies face a heightened risk of vulnerabilities. For instance, employees working from home may not employ the same robust security measures as in the office, creating potential weak points. These potential entry points create more opportunities for attackers to penetrate the network. We can help you improve your defence.

Risk		How we can help
Professional hackers engaging in espionage.	→	Comprehensive **protection** against network threats that detects and blocks malicious or unwanted traffic.
Remote workers downloading unsafe apps.	→	Advanced **security monitoring** analyses network traffic and identifies threats and suspicious activity with information from different sources.
Inconsistent security policies to ensure secure access for remote workers.	→	Comprehensive **systems management** enables simple, pervasive configuration that improves and accelerates protection.
Lack of tools to detect, identify, or respond to a breach timely due to a lack of visibility.	→	**Event management** analyses hazards comprehensively and with several sources to establish the most appropriate immediate response and determine prevention measures.

Next-generation SIEM

The Security Information and Event Management (SIEM) represents a superior level of defence against security risks, enabling a comprehensive visualisation of malicious activity on the network. The system centralises the information about all suspicious activity, allows the analysis of the data, and gives your company the ability to generate more sophisticated alerts and more appropriate responses. These alerts can be translated into much faster responses or even preventive measures, always based on a detailed analysis of the attackers and their behaviour. With this tool, you will generate the best defence strategies for each attack, and you can block many of those events before they occur. It is an ideal security system for companies that handle sensitive, critical, or confidential data, or believe they are at high risk of being the target of cyberattacks.

Threat Management

This is a robust Managed Firewall solution that detects and blocks unwanted or malicious traffic at the perimeter. It offers deep visibility and security in any location, from the branch to the Data Centre. As a managed firewall, you can define specific, comprehensive security automated rules that are enforced on each access point to your network, rather than having different security guidelines for different devices. This enables faster and more efficient end-to-end configuration, as well as better monitoring and response to security threats. In addition, it combines several security features that protect against the widest range of threats. These include real-time intrusion prevention (IPS) and port blocking, which prevent unauthorised access.

Protect Your Business

Despite the growing threat of cyberattacks internationally, many Caribbean businesses believe themselves too small to be targeted. Unfortunately, the increasing number of breaches across the region proves otherwise. Cyber incidents can strike at any moment, disrupting operations and threatening your reputation. As your digital emergency response team, we're here to ensure your business remains secure and resilient, providing swift Incident Response and recovery to keep you operational, even in the face of a crisis.

Risk	How we can help
Scarcity of experienced cybersecurity talent	Our experience and certified security personnel put their expertise to work for your business, supporting your full security cycle.
Delayed threat detection and response.	AI-driven endpoint detection and response tools identify and contain threats early, minimising damage and preventing lateral movement across your network.
Difficulty coordinating cross-departmental teams during incidents.	Our expert team collaborates with your IT, legal, and executive teams to ensure clear, timely communication throughout the incident, helping you avoid confusion and delays.
Lack of automated response processes.	Automated Incident Response reduces errors and speeds up containment efforts, enabling a more effective response to sophisticated cyber threats.
Challenges balancing containment with maintaining business continuity.	We take a balanced approach to managing threats without disrupting your operations, ensuring that systems are restored quickly while preserving essential forensic evidence.
Regulatory and legal complexities in managing breaches.	We help you navigate the legal and regulatory complexities of breach reporting, ensuring compliance with data protection laws and reducing the risk of penalties.

Comprehensive Incident Remediation

Our Incident Response & Remediation Service offers around-the-clock support from a team of experienced security engineers. We perform forensic investigations, contain threats using advanced endpoint protection, and ensure that security patches are applied across all systems. Our solution reconfigures existing security tools to enhance your network's defences and minimise future risks. We also provide a final report with actionable insights and recommendations to improve your security posture, empowering your business to emerge stronger than ever from any incident.

Forensic Analysis and Recovery

Our forensic capabilities include log reviews and deep threat investigations to trace points of infiltration and gather evidence for legal or regulatory purposes. We guide your team through the entire recovery process, rebuilding compromised IT environments, deploying servers, and reinstalling critical systems.

C&W Business

True end-to-end solutions

C&W Business is an industry leader that delivers global enterprise solutions with an exceptional local team that knows the Caribbean threat surface. We are ready and able to promptly respond to any issues and recover your operations.

With our consultative approach, we can help you design, build, or reinforce your security posture to keep your data, applications, and networks safe.

We incorporate industry frameworks and standards, leveraging resilient AI-driven technology and the expertise gained from delivering thousands of services throughout the region, to help you through every step of the process, providing strong defences to keep attackers away and agile recovery in case of a breach.

At C&W Business, we're your catalyst for transformative success. From Cybersecurity to Cloud, Datacentres, Unified Communications, and Connectivity, our streamlined solutions ensure scalability and security. With the Pan-Caribbean region's largest and most reliable network.

Design

The first stage is the design phase. We conduct a thorough analysis of your business requirements and goals, which helps us design **an IT solution that's tailored to your needs and perfectly fits your operational environment.**

Implementation

Then, we move towards the implementation of the solution. **We strive for efficiency, aiming for deployments without disrupting your existing operations.** We also follow best practices and standards to simplify and enhance the response to changes.

Management

Once the implementation is complete, we seamlessly transition to the management of the solution. Here, we leverage the **experts of our SOC team** to assure quality and availability. Our team also offers continuous support, ensuring that your solutions evolve with your changing business needs.

To learn more about how we can help you secure your business, contact us at cwcbusiness.com

C&W Business in the Caribbean