Corum Cyber Defence Service Overview

Service Goals

Corum Cyber Defence delivers enterprise-level cybersecurity protection at small business price points.

The service has been designed to prevent cybersecurity incidents, and stop viruses, malware and determined hackers from accessing or stealing your business' sensitive and personal information.

Flexible options are available to add additional layers of security as your business grows and the need for sophisticated asset protection increases.

Corum Cyber Defence is a holistic cybersecurity program for your business. Risk reduction technologies at the PC and network layers are combined with user awareness activities, policy and process tools that provide clear rules and best practices for your staff.

If an incident does occur, incident response and recovery options are also offered.

Solution Components

Corum and its partners will provide:

- AI-Based protection for the entire pharmacy
  - This includes all pharmacy connected systems, including point of sale (POS) and dispensing computers.
  - Enterprise proven and cloud-managed from a world-class security vendor
- System Based firewall
  - Provides strong network protection, including IDS/IPS.
  - Removes network-based malware, phishing, and monitors pharmacy devices for threats such as ransomware and crypto-mining vulnerabilities.
- 24/7 monitoring and automated remediation
  - Full-time endpoint detection and response.
  - Support from Corum analysts in reviewing and responding to critical alerts.
  - Viruses, crypto lockers, and other potentially dangerous applications will be automatically removed.
- Device hardening
  - Security policies are applied to all devices to make it difficult for hackers and internet-based criminals to gain access.
  - Ensures that devices are protected from internal and external threats.
- Operating systems updates
  - Windows operating system patches will be applied automatically.
  - Non-compliant systems will be reported monthly.
- Pharmacy-specific policies and cyber incident response procedures
  - Ensure your employees understand security best practices.
  - Know what to do when there is an incident or security alert.

- End-user awareness training
    - After securing your computers and network, you need to create "human firewalls".
    - Security awareness training ensures staff are cyber-aware.
- Cyber incident and compliance reporting
    - Monthly compliance reports will provide insight into the threats detected, prevented and removed within your pharmacy.
    - Includes information on the security policy compliance, patching and out of date applications on your pharmacy systems.
- Incident response services
    - In the unlikely event that the protections fail, Corum Cyber Defence will provide you with direct access to experienced cyber incident response professionals.
    - Assistance with restoring systems and guiding you on how to report the incident.
    - Note: This is a separate service, charged only if an incident occurs.

Commitment

Corum will monitor and manage your Corum Cyber Defence and SafeGuard services (if included) to ensure:

- It is secured and free from malware and other internet-based threats
- The operating system is kept up to date
- The device is hardened and resistant to attack
- Devices are isolated to protect other pharmacy systems
- Critical security events and potential incidents are acted upon automatically, critical incidents are investigated, and you are alerted.
- Monthly reports are provided.
- If a system is compromised, Corum will isolate the impacted system as quickly as possible, and the system will remain isolated until the threat is removed.
- Corum will work with you to restore systems as quickly as possible (system restoration is not included in the Corum Cyber Defence service and will be charged separately at our standard rates).
- Corum will contact you within two business days if there is an issue with the service.
- Corum will advise you of any systematic or technical issues which may contribute to the service not working correctly.

Customer Obligations

- You will ensure your computer meets minimum operating system levels and internet speeds to provide a reliable service.
- You will alert Corum of any potential issues that may affect the Corum Cyber Defence service operating effectively.

- You will allow access to all relevant pharmacy systems (or endpoints, routers, network devices) and the system network required by Corum to configure the service.