Velocity Managed Cybersecurity Services

Velocity Technology provides the following Cybersecurity solutions as managed services to help protect your business from hacker attacks. If you don't protect your business you will eventually get hacked.

Contact us today to find out how you can increase your level of cybersecurity!

Security Awareness Training
Training your users on how to spot malicious emails or websites can save your company from ransomware or malware that will steal your intellectual property. This training consists of an in-person 1-hour briefing, online video training, two test emails per staff member per month, and reporting on your staff's progress.

Fully Managed Firewalls
Our fully managed firewall systems are monitored and maintained 24x7 by our support team. This managed security service is continually updated and provides a complete Unified Threat Management (UTM) solution that includes content filtering, bandwidth control, intrusion prevention, advanced malware protection, application management, and identity-based security policies.

Managed Detection & Response
Today's state of the art malware detection services use a combination of AI, Machine Learning, and human analyst intelligence to root out even the sneakiest bad guy. We offer two such systems that target different aspects of cyber-threat actors to provide a comprehensive End Point Detection and Response protection platform.

Continuous Vulnerability Scanning
Our internal vulnerability scanning service can provide regular daily scanning of the internal IP addresses of your company network. We can also provide a service for external vulnerability scanning of your network's Public IP addresses such as your Internet connections

Penetration Testing Services
Velocity Technology can provide penetration testing services for your computer network on an annual or one-time basis to determine the current vulnerabilities.

Breach Detection
This service monitors your network 24x7 and we will alert you if an attacker has penetrated your network.

Dark Web Monitoring
This service will let you know if your business' data (email addresses, usernames, passwords) is being sold on the dark web and how to immediately remediate the situation.

Application Whitelisting
Application whitelisting is designed to provide endpoint control over what software can run on your network, and what resources these applications can access.

Ringfencing
Ringfencing adds a second line of defense for which applications are permitted on your network. First, it defines how applications can interact with each other, and then controls what resources applications can access, such as network, files, and registry.