WORLD CLASS CYBERSECURITY

Built for small and mid-market companies, and provided as part of Velo IT Group's security-first Managed Services program - the Velo Method

INTRODUCTION TO DEFENSE-IN-DEPTH

At Velo IT Group, we use a multi-layered defense-in-depth approach to IT security in order to combat threats from every angle.

Our Managed Security Services program, part of our comprehensive Velo Method, tackles security from the core components of your company's IT system all the way to the farthest endpoint in your network. This guide outlines the Velo Method's included services which work together to create layers of effective defense for your IT systems, protecting your business from ransomware, data breaches, viruses, malware, phishing, data corruption, and more.

TABLE OF CONTENTS

MANAGED DETECTION AND RESPONSE (MDR)

Even with many layers of defense, threat actors (the bad guys) are constantly trying to evolve and stay ahead of even the best cyber defenses.

So, how do we protect our clients from this? The answer is simple: if a threat gets through, we need to know about it immediately, so we can respond with containment and remediation as fast as possible. This is why Managed Detection and Response (known as MDR) services are so critical.

Every day, thousands of security related logs are generated by your IT systems (every login, file access, open, close, save – all of these actions generate security related events). The job of our MDR program is to collect these events, understand them, and **detect when these events are anomalous, contain known threats, or threat-like behavior.** These anomalies and detected threats are analyzed 24x7x365 by our Houston, TX based Security Operations Center (SOC). If confirmed to be a threat, these events will be escalated for incident response in order to **contain and remediate** the threat as quickly as possible.

INCIDENT RESPONSE

"It's not if, but when."
This is a frightening statement often expressed in the cybersecurity industry.

While deploying a comprehensive defense-in-depth posture can dramatically and effectively reduce your risk of attack, the fact remains threat actors are working day and night to get around these defenses. As a result, you must be prepared for the potential impact of a cyber attack.

Incident Response efforts can include many variables, and as such, many third parties can potentially be involved in an incident response effort. These parties include cyber insurance carriers, the carrier's Incident Response (IR) team, their legal consul, public relations teams, and more. Velo prepares for these potential incidents **by creating an IR Plan document,** having **regular risk-based discussions,** and ensuring we have the right resources in place to respond to an incident from a technical perspective. While your cyber insurance carrier will likely bring in their own IR team in the event of any significant breach, Velo will be there to support them by providing any logs and data needed to complete the investigation and swiftly begin the recovery process.

VULNERABILITY MANAGEMENT

In order to understand the potential cybersecurity risks your organization might be facing, it is critical to understand where certain known vulnerabilities might live within your IT systems.

After all, it is hard to fix what you don't know is broken! This is where our vulnerability management and scanning programs come into the picture. Velo will deploy ongoing vulnerability scanning to detect known vulnerabilities so our security team can devise a plan and remediate these vulnerable areas. These scans will run both internally and externally on your network to hunt out and find any known vulnerabilities.

COMMON VULNERABILITIES

Unpatched operating systems

Vulnerable network devices (printers, cameras, IoT)

Out-of-date software

Unsecured public-facing ports

Default passwords in use

Unsecured transfer protocols

CYBER-SECURITY AWARENESS TRAINING

You can have all the proper infrastructure in place, but without understanding and buy-in from all employees, there will always be a hole in your company's cybersecurity program.

34% OF UNTRAINED USERS FAIL SIMULATED PHISHING TESTS

A recent study found that over one third of untrained users fail simulated phishing tests.[1] Everyone at the organization must be aware of threats that can affect them and how to avoid them. This is why education and training are an important part of Velo's Managed Security Services program. We provide your organization with training materials as well as simulated phishing tests and reporting in order to ensure your employees become a strong line of defense against any potential attacks.

(1) https://info.knowbe4.com/phishing-by-industry-benchmarking-report

DATA ENCRYPTION

Data encryption services can help protect the valuable data living inside your organization.

Data encryption services make your data inaccessible to those who are not authorized to view it. Velo's data encryption services, as part of the Velo Method, identify data - both at rest and in transit - needing to be encrypted in order to maintain security. By implementing encryption policies across the organization, Velo will centrally maintain control and compliance over all encrypted data.

"THE WORLD'S MOST VALUABLE RESOURCE IS NO LONGER OIL, BUT DATA."

-The Economist, May 2017

MULTI-FACTOR AUTHENTICATION (MFA)

MFA is a cybersecurity mechanism coupling what you know with what you have and is one of the single most effective ways to combat account takeover.

As part of Velo's Managed Services program, we will identify where MFA should be applied, and work with you and your end users to implement the new security protocol. Velo's advanced approach to MFA can significantly reduce the perceived burden of MFA by integrating Single Sign-On (SSO) where possible to reduce the number of MFA prompts each user experiences on a daily basis, all while still improving their security posture.

MFA PASSWORD + ADDITIONAL AUTHENTICATION

51% OF USERS RECYCLE PERSONAL AND WORK PASSWORDS[2]

49% OF USERS WRITE THEIR PASSWORDS ON PAPER[3]

(2) https://dataprot.net/statistics/password-statistics/
(3) https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/

FIREWALL MANAGEMENT

Nearly all networks have a firewall, but few companies will experience true protection due to pedestrian expertise when it comes to configuration.

The term “firewall” comes from a construction technique of setting up physical walls to prevent fire from spreading. In theory, the use of a firewall in IT systems is not too different. It is a barrier preventing bad actors from infiltrating your computer systems. Velo’s managed security services will ensure your firewall is configured correctly, optimized for your workflows, and monitored persistently. By collecting logs and working to harden the firewall, we will help you to maximize the capabilities of your firewall infrastructure. Often, firewalls are undersized and therefore are a performance bottleneck. In these cases, Velo will recommend and source the most appropriate and right-sized option.

"THROUGH 2023, 99% OF FIREWALL BREACHES WILL BE CAUSED BY FIREWALL MISCONFGURATIONS, NOT FIREWALL FLAWS."

Kaur, Rajpreet, Hils, Adam, and Watts, John. “Technology Insight for Network Security Policy Management.” Gartner, Inc. 21 February 2019.

SOFTWARE UPDATES

Keeping your software up-to-date is an important step in securing your IT environment.

When software developers release updates to their programs, it is essential those updates are installed to minimize vulnerabilities in your IT systems. In our regularly scheduled strategy sessions, we will identify your key software vendors, and devise a strategy for conducting updates in non-disruptive maintenance windows.

PATCH MANAGEMENT

Patch management is an essential process in resolving operating system vulnerabilities that could leave your company open to attack.

Patch management is an ongoing process that requires a diligent approach in order to be effective. Our security team first tests, then deploys patches as required by your IT environment on a regular schedule. Additionally, we deploy critical patches that address urgent zero-day vulnerabilities as soon as they become available and are tested. Automated patches are done overnight during a maintenance window so as not to interrupt your workday.

WE DEPLOY PATCHES ON A SCHEDULED BASIS

AND ASAP IN RESPONSE TO ZERO-DAY THREATS

ZERO DAY

ZERO-DAY IS A NEWLY DISCOVERED VULNERABILITY

EMAIL FILTERING

Over 3 billion fraudulent emails are sent every day,[4] many of which are phishing emails meant to trick the recipient into giving money, sharing personal information, or opening malware-laden attachments.

3Billion FRAUDULENT EMAILS ARE SENT EVERY DAY

To reduce the chance that an employee falls victim to an email scam, Velo sets up industry-leading email filtering systems for all clients. Known malicious emails and attachments are blocked to prevent accidental user intervention. Emails that are flagged as suspicious are sent to a quarantine server where users can carefully view them and release them if deemed legitimate.

(4) https://www.valimail.com/press/more-than-3-billion-fake-emails-are-sent-worldwide-every-day-valimail-report-finds/

WEB FILTERING

Web filtering is intended to prevent users from accessing internet content identified as malicious in nature.

At the network level, Velo blocks traffic from domains that are known bad actors or have previously exhibited behavior that may be malicious. We also provide customizable web filtering services with content and category options to meet the productivity and compliance needs of each individual client.

60K

MALICIOUS DESTINATIONS DISCOVERED DAILY BY WEB FILTERING LEADER CISCO UMBRELLA[5]

(5) https://umbrella.cisco.com/blog/cisco-umbrella-discovers-evolving-cyber-threats-in-2020

ENDPOINT PROTECTION

Endpoints, such as desktops, laptops, and servers, are often a gateway for attackers to gain entry into a company's network.

With many users on many different devices, it can be difficult for an organization to monitor and keep track of all endpoints. This is especially true as workforces become more remote. As part of our security services, Velo equips all endpoints with best-in-class anti-virus and anti-malware protection, coupled with advanced endpoint detection response (EDR) software which automatically sends alerts to our security team for analysis. This ensures that all managed endpoints are protected, monitored, and receive immediate attention if a problem arises.

BEST-IN-CLASS ANTI-VIRUS PROTECTION

BEST-IN-CLASS ANTI-MALWARE PROTECTION

ENDPOINT DETECTION RESPONSE

REMOTE MAINTENANCE

Common procedures such as disk cleanup, temp file cleanup, and disk defragmentation are performed through automated and regularly scheduled remote maintenance tasks.

SCHEDULED MAINTENANCE WINDOWS

This remote maintenance keeps the IT environment running at peak efficiency, and occurs at a time that is not disruptive to your business (typically overnight). By regularly performing these system maintenance tasks, you not only gain performance improvements, but you are also assured a more effectively secured IT system. This is due to the fact that our cybersecurity toolset and patching programs are better supported in running error-free on a well-maintaned system.

AUTOMATED REMEDIATION

Velo's advanced detection and auto-healing remediation platform allow for an automated approach to compliance with your organization's baseline security standards and policies.

When a harmful or potentially harmful event is detected in your IT environment, it could lead to downtime, performance degradation, and even security issues if left unchecked. For example, something as simple as a new, yet unmanaged device inadvertently joining your network could be a **major security hole** as this new system may not meet your **baseline security requirements**. In order to quickly solve problems like this as efficiently as possible, Velo has developed **detection and auto-healing processes** which are triggered to automatically start bringing unmanaged and out-of-compliance devices into compliance with your organization's security standards. Items such as managed endpoint protection products and security policies are automatically applied to these out-of-complaince devices as quickly as possible. These processes reduce or eliminate potential interruptions to your business and can close a variety of security gaps using finely tuned automations.

TREND ANALYSIS

Trend analysis involves collecting data to find patterns that can help drive IT decisions and improvements.

Velo's monitoring systems record events that happen in your technology environment, and if there are repeat issues, we can analyze them to determine the root cause. This allows us to solve problems, increasing your IT efficiency, rather than using the temporary “band-aid” approach which is far too common in our industry.

TREND DATA BRINGS TO LIGHT ROOT CAUSES

STRATEGIC ANALYSIS SOLVES SYSTEMIC ISSUES

REDUCTION IN IT ISSUES DRIVES EFFICIENCY

DATA BACKUP

Even with the most advanced and sophisticated redundancies, it is still critical to have backups at the ready in the event of disaster.

Cybersecurity attacks often necessitate the need to recover encrypted or ransomed data from backups. Attackers know this and often target less sophisticated backup technologies during their attack so recovery without ransom payment is not an option.

Velo includes backup and disaster recovery services as part of our Velo Method program. We provide an advanced onsite appliance for backups as necessary, as well as an offsite staged environment for disaster recovery. These backups are secured separately from your main network, providing isolation from attack and resiliency when recovery is needed most. Ongoing testing of these backups by your dedicated strength engineer validate this resiliency.

56%

OF ORGANIZATIONS RELY ON BACKUPS TO RECOVER FROM RANSOMWARE[6]

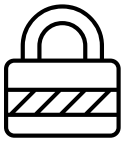
(6) https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

WHAT IS INCLUDED IN THE VELO METHOD?

The Velo Method is a scientifically proven approach to delivering a secure and predictable IT environment. It allows us to provide our clients with IT support, security, strength, and strategy.

SUPPORT

Our support team is a world-class group of metrics-driven IT professionals who deliver outstanding customer service.



SECURITY

An advanced managed security services program which delivers a defense-in-depth strategy protecting clients from a wide variety of threats.

STRENGTH

Through a strategic, ongoing process, our strength team works to regularly align our clients' IT environments with our list of 200+ best practices.

STRATEGY

Our strategy engineers compile a Velo Method alignment report to create a forward-looking roadmap of where improvements should be made to make your IT systems as efficient as possible.

INTERESTED IN THE VELO METHOD?

We hope this guide has been helpful to you as you consider security measures to put in place at your organization.

We would love to talk with you about your company and how a defense-in-depth strategy can make it more efficient and secure than ever before. Give us a call at 214-214-VELO, or click the link below: