velo

The Velo Method: Cybersecurity

In this guide, learn how Velo empowers clients with turnkey managed security services providing the resources and protections needed to defend their operations in today's threat laden landscape.

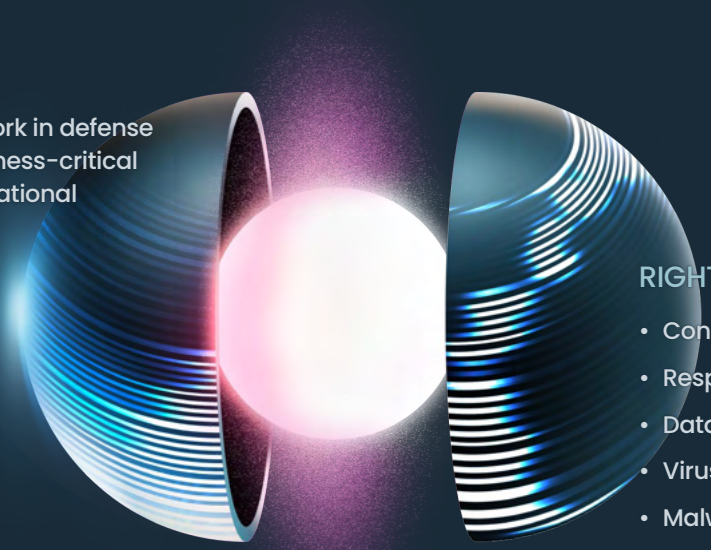
What side of Boom are you on?

At Velo IT Group, we use a multi-layered defense-in-depth approach to IT security to combat threats from every angle **left of boom** as proactively as possible, and we have the resources and tools to help navigate the world **right of boom** when you need to recover and rebound as quickly as possible.

This guide outlines our Managed Security Services which are built into the Velo Method and protect every layer of your IT environment—from core systems to the most remote endpoint, on or off the network. With the Velo Method, you get a partner standing shoulder to shoulder with you providing overwatch on the technical detail and fiercely protecting your operational resiliency.

LEFT OF BOOM:

- Prevention
- Preparation
- Training
- Proactive work in defense of your business-critical data & operational resiliency

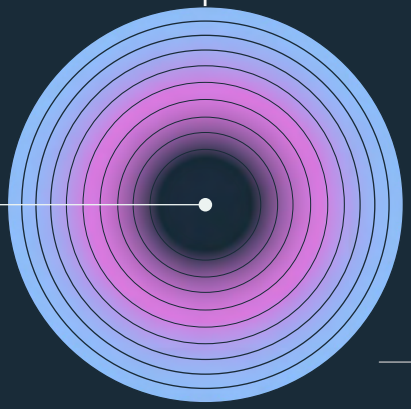


RIGHT OF BOOM:

- Containment
- Response
- Data breaches
- Viruses
- Malware
- Phishing deceptions
- Recovering from ransomware

In the world of cybersecurity, there are two hemispheres: left of Boom and right of Boom—with 'Boom' being the moment of breach.

It's Not If, But When.



Vulnerability Management

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.

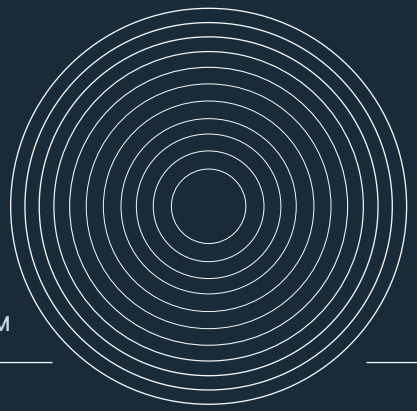
After all, it is hard to fix what you don't know is broken. This is where our vulnerability management and scanning programs come into the picture. Velo will deploy ongoing vulnerability scanning to detect known vulnerabilities so our security team can devise a plan and remediate these vulnerable areas.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

For businesses that benefit from an aggressive, strong cybersecurity posture, it's about more than avoiding data leaks or checking compliance boxes. It's about uptime. We partner with business leaders to prevent the kind of disruption ransomware causes, where businesses are cut off from critical data and brought to their knees.

Common Vulnerabilities:

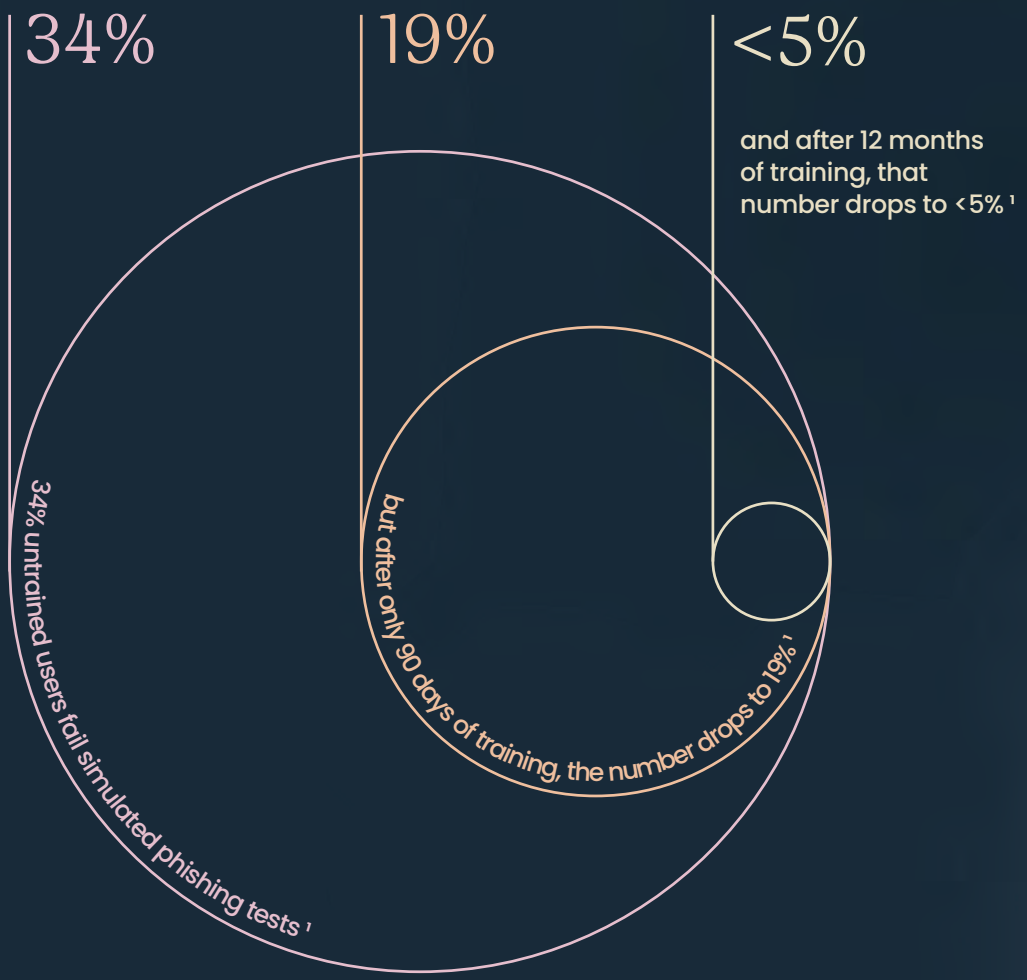
- Unpatched operating systems
- Vulnerable network devices (printers, cameras, IoT)
- Out-of-date software
- Unsecured public-facing ports
- Default passwords in use
- Unsecured transfer protocols

Today's network lives everywhere: in the cloud, on devices, and across countless apps. The security perimeter is now boundless—and vulnerability management is more critical than ever.

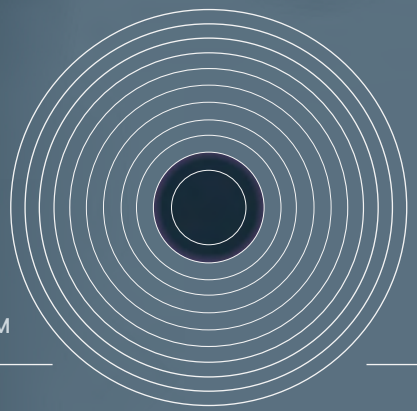


Cybersecurity Awareness & Training

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.



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 to ensure your employees become a strong line of defense against any potential attacks.



LEFT OF BOOM

[1] Source: https://blog.knowbe4.com/knowbe4-2024-phishing-by-industry-benchmarking-report

Data Encryption

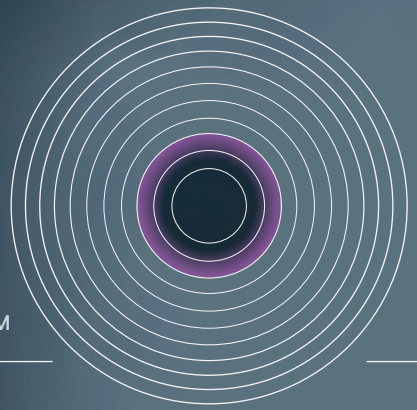
Lock down your most valuable asset: your data.

Your business runs on data. It lives in emails, file shares, applications, and cloud platforms. One of the most effective ways to protect that data is with a well-formulated encryption policy. Ransomware attackers thrive on access to unprotected or poorly secured information. With strong encryption and disciplined key management, we reduce the risk of data exposure—even if a breach occurs.

> "The world's most valuable resource is no longer oil, but data."
>
> – *The Economist*, May 2017

Velo's data encryption policies cover both data at rest (think: a laptop left in the backseat of an employee's car) and data in transit (crossing the internet between systems).

- For devices on the move: Full-disk encryption is critical. A stolen laptop without it could trigger a reportable breach, legal liability, and reputational fallout.
- For network traffic: Encryption in transit safeguards communication channels—especially when sensitive data like passwords, Social Security numbers, banking details, or credit card info is involved.



MultiFactor Authentication (MFA)

Make stolen passwords useless.

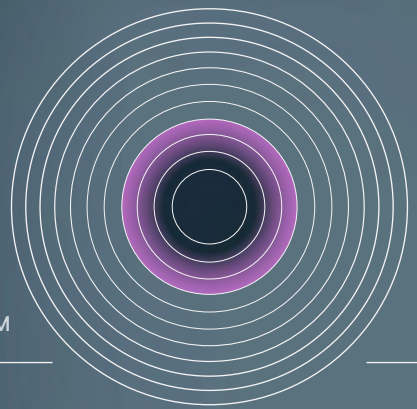
MFA is a cybersecurity mechanism coupling what you know (your password) with what you have (a one-time use code, a token, etc.) and is one of the single most effective ways to combat account takeover. With the prevalence of data leaks involving usernames and passwords, adopting a secondary security measure is a simple way to make sure it's the real you attempting a login with your credentials.

As simple as the prompt approval is, it does get tiring, and that is why we work to integrate 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. We focus first on the "Crown Jewels" - systems that matter most—remote access (VPNs, RDP), admin portals, and cloud platforms like Microsoft 365 or Google Workspace. These are high-value targets and the most common attack vector.

As simplicity increases for your team, complexity increases under the hood. With the crown jewels secured, we work to broaden the reach of the MFA deployment. In some cases we have to upgrade legacy systems where the authentication protocols are not compatible with modern MFA technology. Additionally, we deepen the MFA effectiveness by prioritizing phishing-resistant methods. Not all MFA is created equal. We configure our tools to use secure options like Duo Push with number-matching, FIDO2 security keys, or biometrics—reducing the risk of push-bombing and social engineering.

As part of Velo's Managed Services program, we will identify where and how MFA should be applied, make sure it is integrated smoothly, and you are supported with user education and visibility. That's where Velo comes in: to humanize the rollout, reduce friction, and close the gaps that most teams overlook.

More than half (56%) of all compromises in Q1 2025 resulted from the theft of valid account credentials with no multi-factor authentication (MFA) in place, according to research by Rapid7.[2]



[2] Source: https://www.infosecurity-magazine.com/news/majority-compromises-stolen/

Firewall Management

Most networks have a firewall. Few are protected by it.

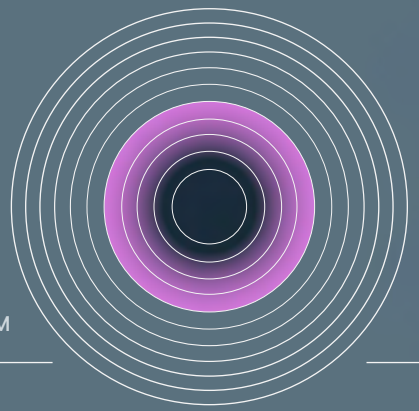
That's because firewalls don't protect by default—they protect when configured, monitored, and maintained by people who know what they're doing. Too often, firewalls are deployed with default settings, poorly sized for the environment, or left unmonitored until something goes wrong.

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 that controls all the traffic across your corporate network letting in approved traffic and 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 misconfigurations, not firewall flaws."

– Gartner, 2023



Software Updates

Staying current keeps you secure - and your systems running smoothly.

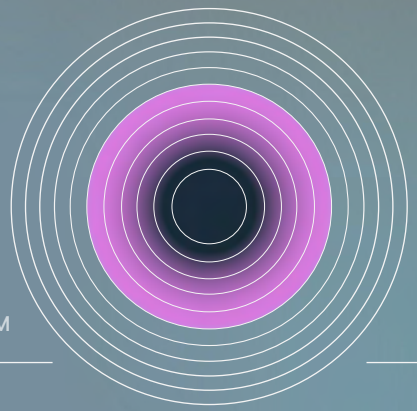
Most cyberattacks don't rely on sophisticated, never-before-seen tactics. They exploit outdated software—tools that are widely used but not regularly updated.

Software vendors issue updates for a reason: to fix bugs, improve stability, enhance performance, and, yes, close security gaps. But unlike patches that address core system vulnerabilities, these updates often apply to your day-to-day tools—line-of-business applications, productivity suites, collaboration tools, and more.

At Velo, we help you stay ahead of these updates. During regular strategy sessions, we identify your critical software vendors, assess your environment's readiness, and plan non-disruptive maintenance windows. For major updates, we'll also help you prepare your hardware—some updates now require more RAM, additional storage, or new system configurations. That means less downtime, fewer surprises, and a dramatically smaller attack surface.

Attackers frequently exploit vulnerabilities within 2 years of public disclosure—often targeting organizations slow to apply patches.

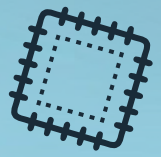
— CISA's 2023 Vulnerability Report



Patch Management

Close the gaps before attackers find them.

Known vulnerabilities remain a top entry point for attackers



Patches close security gaps before they become breaches

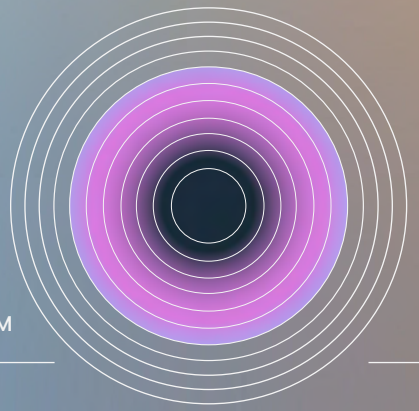
Zero-day

Zero-day exploits require a fast, expert response—and that's what we deliver

Patching is a different layer of defense. It focuses specifically on addressing vulnerabilities in operating systems, firmware, and widely used frameworks—the kinds of flaws that attackers look for first.

At Velo, patching isn't just automation—it's an active, structured process. We test, schedule, and deploy patches that your environment requires on a consistent cadence. Routine patches address known vulnerabilities. Urgent patches for zero-day threats (newly discovered flaws being exploited in the wild) are deployed immediately once validated.

All of this happens during designated maintenance windows to avoid unnecessary disruption.



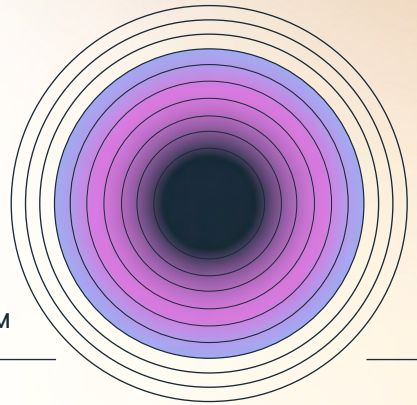
Email Filtering

Stop attacks before they hit the inbox.

Over 3.4 billion fraudulent emails are sent every day, accounting for about 1.2% of all global email traffic. Many of these are phishing emails meant to trick the recipient into giving money, sharing personal information, or opening malware-laden attachments.

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.

3.4 billion fraudulent emails are sent every day [3]



LEFT OF BOOM

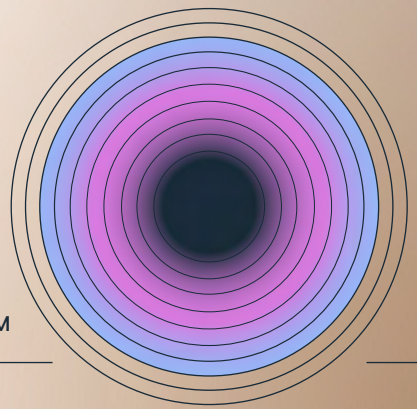
[3] Source: https://controld.com/blog/phishing-statistics-industry-trends/

Web Filtering

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

60,000 malicious destinations are discovered daily by web filtering leader Cisco Umbrella. [4]

On all managed endpoints, 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.



[4] Source: https://umbrella.cisco.com/why-umbrella/a-new-approach-to-cybersecurity

Endpoint Detection & Response (EDR)

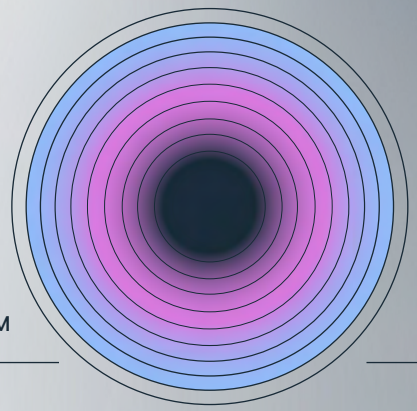
Built to notice what your people won't, and act before it matters.

People move fast. They click links, open files, join networks, and connect devices without hesitation. Velo equips every managed endpoint with advanced EDR (Endpoint Detection and Response) technology to protect those moments when things go wrong.

Traditional antivirus tools rely on signatures to detect known threats. EDR takes a more intelligent approach. It monitors real-time activity on each device, detects suspicious behavior, and acts automatically.

Our EDR tool watches for abnormal file changes and unexpected activity. If something looks off, it responds immediately. The system can isolate the device, stop the threat, and even roll back the device to a clean state.

	Traditional Antivirus	Endpoint Detection & Response (EDR)
Threat Model	Known threats only (signature-based)	Known and unknown threats (behavior-based)
Detection	Scans files against a database	Monitors activity and behavior in real time
Response	Blocks known malware	Automatically isolates, kills processes, and can roll back systems
Visibility	Limited insight after infection	Full forensic detail and attack storyline
Protection Scope	Static and reactive	Dynamic and adaptive



It's Not If, But When.

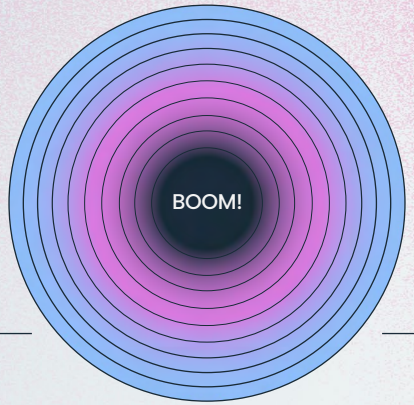
THE MOMENT THE INEVITABLE HAPPENS

In cybersecurity, **Boom** is the moment an incident happens. It's when prevention fails and a threat breaks through. Ransomware locks your systems, an attacker gains access, or sensitive data is compromised.

This is not theoretical. Boom moments happen every day, to companies of every size, in every industry. They are rarely dramatic at first. Sometimes it's just one strange alert or an employee reporting something off. But what happens in the hours that follow determines whether it becomes a headline or a quick recovery.

We help you define what a cyber incident looks like, what needs to happen in the first few minutes, hours, and days, and who is responsible for what. We gather the forensic data, maintain logs, and keep your documentation ready to support legal teams, cyber insurance carriers, and third-party responders.

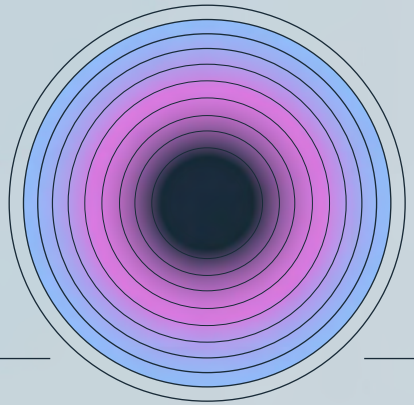
Boom is not the end of the story. With the right partner and proper preparation, it can be a controlled moment — more of a speedbump than a crisis.



Incident Response

When things go wrong, you need a plan—and a partner.

The best time to prepare for a breach is before it happens.



RIGHT OF BOOM

What happens immediately following the Boom is what truly defines your resilience.

A well-executed Incident Response (IR) plan limits damage, restores operations, and keeps your team focused. At Velo, we help you prepare for that moment long before it happens. We create IR plans, guide risk-based discussions, and ensure the right tools and teams are in place to act fast when needed.

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 counsel, public relations teams, and more. Velo prepares for these potential incidents with regular review of our IR Plan, 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.

Velo builds and documents your Incident Response strategy in advance, so you're not scrambling when every minute counts.

Managed Detection and Response (MDR) and SIEM

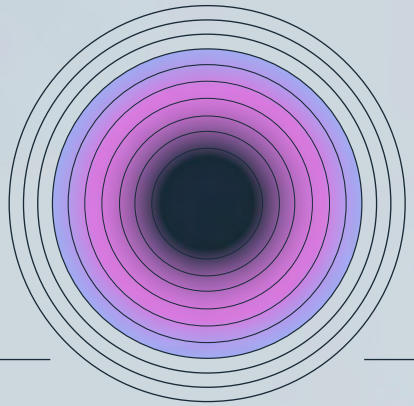
Because when something gets through, minutes matter.

Attackers are persistent, creative, and constantly adapting. That is why Managed Detection and Response—commonly called MDR—is one of the most important parts of your Right of Boom strategy.

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). These events are logged in our Security Information Event Management (SIEM) platform. 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 24/7 by our 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.

This work happens behind the scenes, often without disruption to your team. But the benefit is deeply human. MDR protects your people from lost productivity, your customers from data exposure, and your leadership from extended downtime or financial fallout.



Data Backup

Giving you a path forward when you need it most.

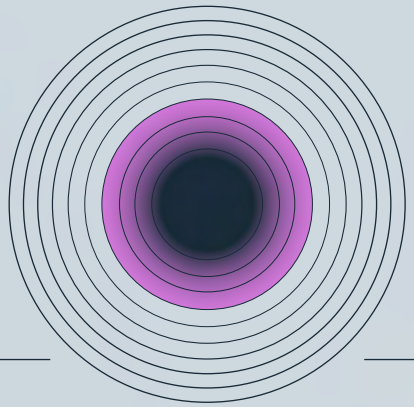
In 2024 68% of organizations relied on backups to recover from ransomware. [5]

Data loss doesn't always come from a dramatic breach. It can start with one wrong click, a failed update, or a power outage at the wrong moment. But when systems go down, people still need to work. Clients still expect delivery. Leaders still need options.

That's why data backup isn't just a safeguard—it's a business imperative.

Velo includes secure, tested backups as part of the Velo Method. We deploy both onsite backup appliances and offsite, isolated data repositories to ensure redundancy and resilience. These backups are immutable, separated from your production network, and protected from ransomware and internal failure alike.

Your dedicated strength engineer regularly tests and validates your backups in addition to our automated testing and data validation technologies, so you know recovery will work when it matters most.



RIGHT OF BOOM

[5] Source: https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.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.

PARTNERSHIP

Our business model rewards stability, aligning our success with your seamless operations.

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 visit our website.