Welcome to the Velocity IQ Cybersecurity Guide 2025

As a trusted leader in managed cybersecurity services, Velocity IQ has developed this essential guide to help you navigate the complex world of digital threats and protection strategies. Whether you're reassessing your current security posture or building a cyber defense plan from the ground up, this guide will empower you to make informed decisions that safeguard your business. Let’s explore how the right cybersecurity partnership can protect your data, ensure compliance, and strengthen resilience in today’s ever-evolving threat landscape.

Table of contents

Introduction

In 2025, technology won't slow down.

With new advancements come new challenges, and the global cost of cybercrime is expected to reach $10.5 trillion. This is driven by the increasing integration of AI, cloud infrastructure, and remote work. These emerging technologies, while offering operational efficiency and innovation, also create fresh vulnerabilities. Which is why taking a proactive approach to cybersecurity is essential.

$4.45M

Average Cost of Data Breaches

in 2023, are becoming more subtle and sophisticated. As AI evolves and automation increases, businesses need to stay vigilant in addressing new attack vectors.

Security leaders are no longer operating in isolation. Collaborative, cross-departmental efforts are growing, supported by larger cybersecurity budgets and executive backing. This shift in culture integrating IT and security practices across all levels of business—has become necessary to enhance organizational resilience.

While navigating the cybersecurity landscape may seem overwhelming, every business can take small, actionable steps to mitigate risks and future-proof their operations. In this whitepaper, we will explore strategies to help your business stay ahead of cybersecurity trends and threats, with a focus on what lies ahead.

What's to come in 2025

The increased reliance on cloud infrastructure and remote work continues to dominate, making organizations more dependent on distributed networks. This has expanded the attack surface for cybercriminals, who now exploit vulnerabilities in hybrid environments with greater precision.

At the forefront of technological innovation, AI and machine learning are becoming deeply embedded in business processes. However, the same AI systems that enhance operations are also being weaponized by cybercriminals to develop more sophisticated and persistent attacks. Ransomware attacks powered by AI-driven automation are expected to rise, as are phishing schemes that use machine learning to mimic human behavior more convincingly.

While these trends may appear daunting, understanding these shifts allows businesses to adapt. With the right strategies in place, organizations can remain innovative while staying protected.

Cloud Dependence

Expanded attack surface for cybercriminals in distributed networks

AI Integration

Both enhances operations and enables more sophisticated attacks

Strategic Adaptation

Organizations can innovate while implementing protective measures

Understanding the risks of cloud and remote infrastructure dependence

In recent years, businesses have increasingly relied on cloud infrastructures and remote work models, revolutionizing how IT infrastructure is managed and operationalized. This shift has not only redefined organizational landscapes but has also introduced a shared responsibility model in cybersecurity that demands careful consideration.

While hybrid cloud infrastructures offer enhanced flexibility and scalability, they simultaneously expand the attack surface, creating new vulnerabilities for cybercriminals to exploit. Transferring risk to a cloud vendor does not absolve organizations from responsibility; instead, it requires a deeper understanding of risk management. Users must remain vigilant in their interactions with cloud services, as sharing sensitive information or misconfiguring access controls can lead to significant breaches.

Effective cloud management is essential in this landscape. It ensures that security measures are integrated throughout the entire environment. Organizations must maintain clear communication with their cloud service providers, setting expectations for security and compliance while actively managing their own security posture.

Shared Responsibility

Cloud vendors and organizations must both take active roles in security management

Expanded Attack Surface

Hybrid infrastructures create new vulnerabilities that require vigilant monitoring

Effective Management

Clear communication with providers and active security posture maintenance is essential

Remote and hybrid work infrastructures

The COVID-19 pandemic was the catalyst for remote work environments. Although some businesses have returned completely to office work, the majority of organizations are now set up for **hybrid** work in a way that has reshaped the security landscape. Examples of this include remote working seeing an **increase** in **cyber-attacks** involving ransomware and magnified vulnerabilities in VPNs. While many businesses were slow to adapt their security requirements, 2025 will see an urgency to respond to the wider attack surface that remote and hybrid work presents.

> "When employees work remotely, our ability to maintain direct oversight is reduced. Combined with our dependence on cloud infrastructure, this introduces significant shifts in how we manage operations. The gap between where people work and the security posture of their home networks has created notable challenges from a cybersecurity perspective."

Key Challenges of Remote Work Security

- Increased ransomware attacks targeting home networks
- Magnified vulnerabilities in VPN infrastructure
- Limited control over employee home network security
- Wider attack surface requiring new security approaches
- Delayed adaptation of security requirements by businesses

The impact of AI and emerging technologies on cybersecurity

AI is poised to be one of the most influential elements of innovation, shaping technology and cybersecurity. The potential to leverage it for cybersecurity is immense, providing organizations with unprecedented capabilities to predict and mitigate threats while enhancing overall resilience. However, the integration of it also introduces new security risks, particularly during the onboarding of AI partners.

Vendor due diligence has become increasingly important as organizations assess the security implications of partnering with AI providers. Companies must evaluate the security protocols and practices of these vendors to ensure they align with their own standards. Key considerations include data handling practices, compliance with regulations, and the robustness of the AI solutions themselves.

1

Enhanced Threat Prediction

AI enables unprecedented capabilities to anticipate and identify potential security breaches before they occur

2

New Security Risks

Integration of AI systems introduces vulnerabilities, especially during vendor onboarding processes

3

Vendor Due Diligence

Organizations must thoroughly evaluate AI providers' security protocols, data handling practices, and regulatory compliance

Zero trust and the rise of connected ecosystems

As we move into 2025, the emphasis on Zero Trust is becoming the norm for many vendors. It is driving a significant shift away from traditional perimeter-based security measures. In an increasingly connected digital and physical ecosystem, where boundaries are blurred, threats can emerge from any direction. Implicit trust in internal users is no longer a viable strategy; instead, Zero Trust promotes continuous verification regardless of user identity or location.

This evolving landscape necessitates strong security frameworks such as Secure Access Service Edge (SASE), integrating network and security functions into a unified cloud service. Zero Trust Network Access (ZTNA) further enhances this approach by ensuring only authenticated users have access to specific applications and services, effectively minimizing the attack surface.

Zero Trust Principles

- Never trust, always verify
- Assume breach mentality
- Verify explicitly
- Use least privilege access
- Implement continuous monitoring

Key Security Frameworks

- Secure Access Service Edge (SASE)
- Zero Trust Network Access (ZTNA)
- Micro-segmentation
- Identity and Access Management (IAM)
- Continuous authentication

The rise of sophisticated cyber threats and attacks

As noted above, the year will see a proliferation of cyberthreats, from Advanced Persistent Threats and ransomware to supply chain attacks. Generative AI will be used in phishing attempts via email and SMS, as well as other social engineering methods including voice and video, making these attacks seem more authentic and harder to guard against.

Businesses will need to maintain a state of constant vigilance and be increasingly adaptable and agile to stay safe.

Advanced Ransomware

More sophisticated encryption and targeting techniques

Supply Chain Attacks

Targeting vulnerable points in connected business ecosystems

AI-Powered Phishing

Using generative AI to create highly convincing fraudulent communications

Voice & Video Spoofing

Sophisticated social engineering using deepfake technology

Cybersecurity threats to pay attention to in 2025

These transformative shifts don't just have an impact on organizations' security postures.

The increased ability and sophistication of threat actors to identify and exploit weaknesses in an organization's perimeter defenses prompts the need for more adaptive security measures, as well as increasingly robust incident response frameworks.

But more importantly, it will require a cultural shift and a change of mindset, instilling cybersecurity consciousness across all levels of an organization. Cybersecurity can no longer be seen as 'just an IT issue', but must be reimagined as a fundamental part of business strategy - something proactive and anticipatory, and embedded in operational processes.

Adaptive Security

Evolving defenses that respond to changing threat landscapes

Robust Response

Comprehensive frameworks for handling security incidents

Strategic Integration

Security as fundamental to business operations

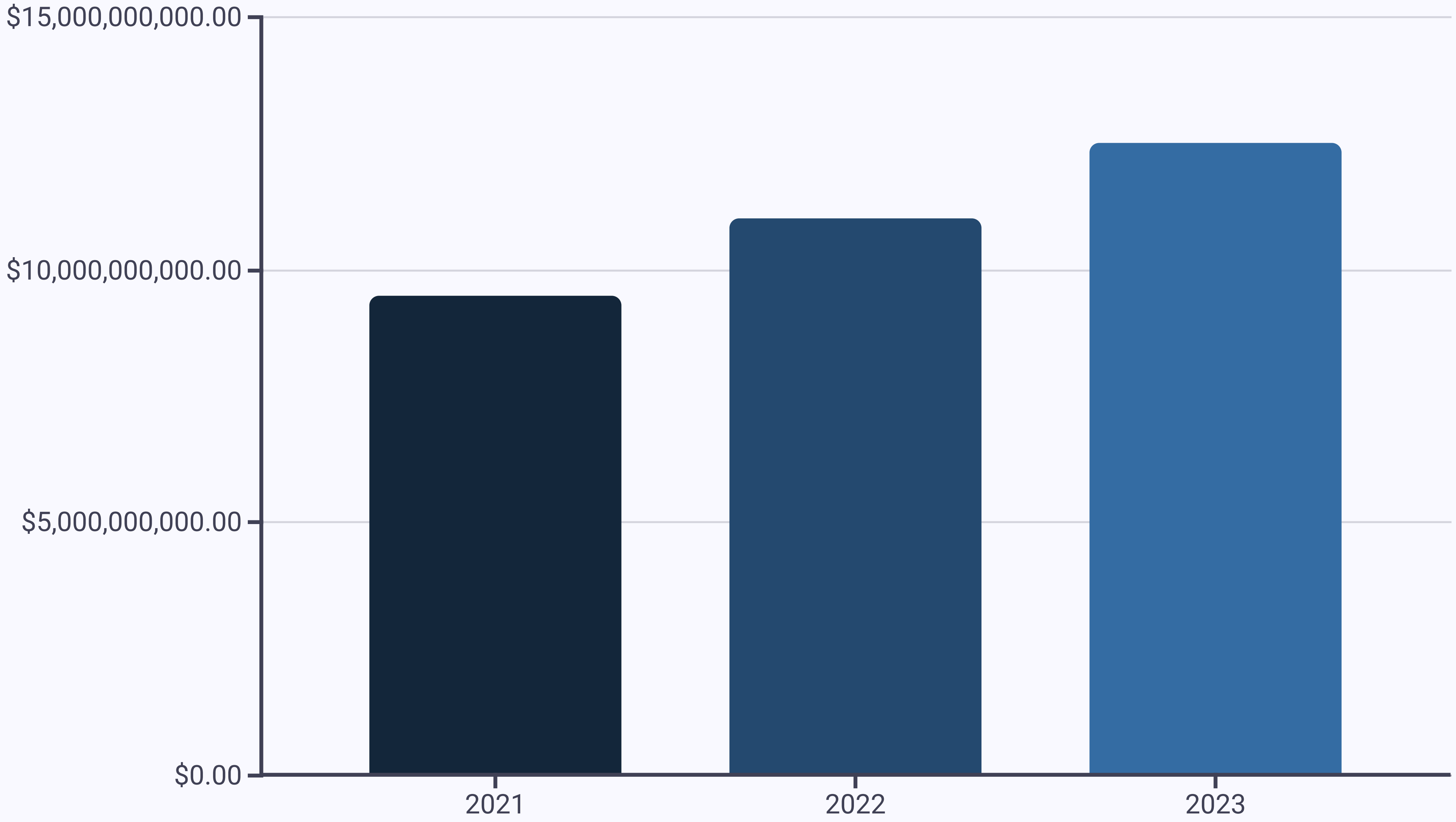
Cultural Shift

Organization-wide cybersecurity consciousness

Business email compromise: the constant threat

Business Email Compromise (BEC) consistently ranks as the top method for cybercriminals to infiltrate businesses and access sensitive data.

According to the FBI, losses from BEC incidents reached over $12.5 billion in 2023. This sophisticated form of phishing exploits trusted relationships by impersonating executives or legitimate vendors. It often leads employees to unwittingly disclose confidential information or initiate unauthorized transactions. With attackers increasingly employing social engineering tactics to craft convincing emails, the risk of falling victim to BEC schemes is heightened.



⚠ Common BEC Tactics

- Executive impersonation requesting urgent wire transfers
- Vendor/supplier email compromise requesting payment changes
- HR/payroll impersonation requesting W-2 information
- Attorney impersonation claiming to handle confidential matters
- Data theft through requests for sensitive company information

The maturation and challenges of generative AI in cybersecurity

> "ChatGPT can be a powerful ally, but it also has its risks. If not used carefully, it can become a liability."

Generative AI exploded into the public consciousness in 2021 with the release of a slate of AI language and image models. The last few years have seen a maturation in the abilities of AI, driving innovation across the IT sector and bringing remarkable capabilities and new challenges to the world of cybersecurity. AI will continue to be one of the defining trends of 2025.

> "I prefer not to share any sensitive or personally identifiable information with AI systems, especially anything that could potentially be misused or traced back to me."

Generative AI also empowers security measures with an unprecedented level of predictive analysis and threat detection, while simultaneously introducing a wide variety of complexities, from an expanded threat surface to a slate of ethical considerations. Many organizations are quick to integrate the use of AI into their operations, without understanding where information is going and who has access to it.

AI Security Benefits

- Enhanced threat detection capabilities
- Automated security response systems
- Predictive analysis of potential vulnerabilities
- Improved pattern recognition in attack vectors

AI Security Challenges

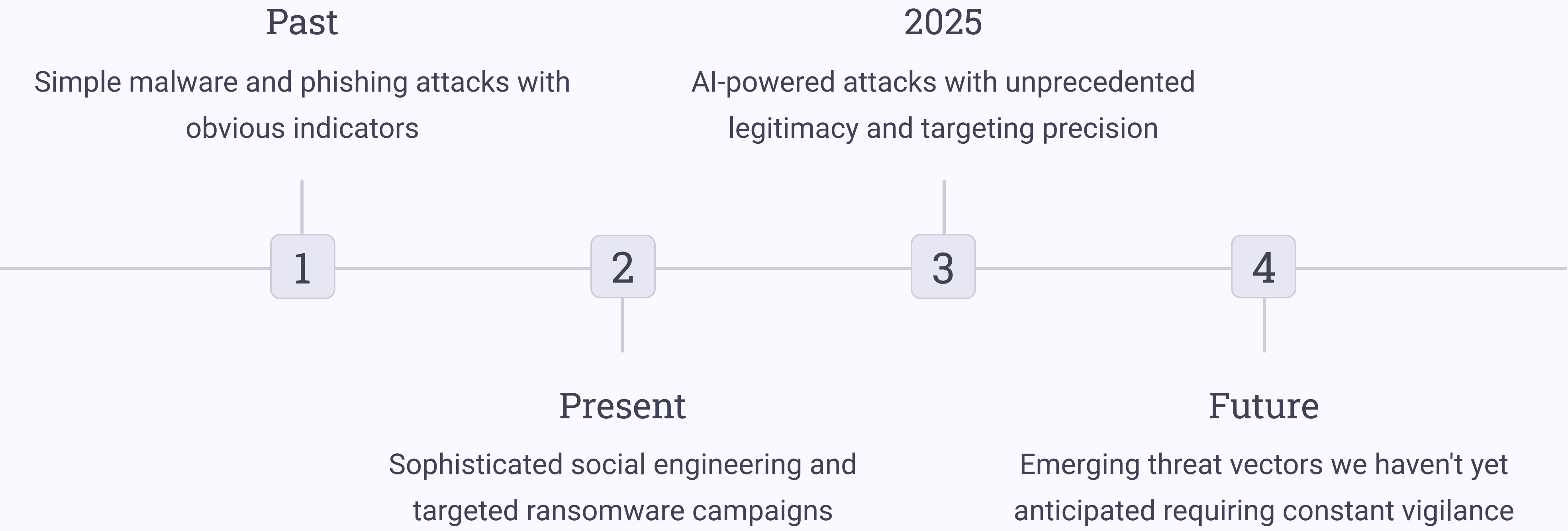
- Expanded threat surface
- Data privacy concerns
- Ethical considerations in AI deployment
- Lack of transparency in information handling

The continuous evolution of malicious actors and defense strategies

We are likely to see an even more pronounced evolution of the ways that bad actors frame their attacks. Technologies like AI make it harder than ever to identify threats given it can be more challenging to determine the legitimacy of apps, software, and IT players.

As technology develops, cyber adversaries are often at the cutting edge of innovation as they discover and develop ever more sophisticated tactics for breaching defenses and sniffing out vulnerabilities.

These threats underscore a pivotal shift in the way cybersecurity will work going forward. Embracing and addressing these issues isn't just a good idea, it's a must.



1 Past

Simple malware and phishing attacks with obvious indicators

2 Present

Sophisticated social engineering and targeted ransomware campaigns

3 2025

AI-powered attacks with unprecedented legitimacy and targeting precision

4 Future

Emerging threat vectors we haven't yet anticipated requiring constant vigilance

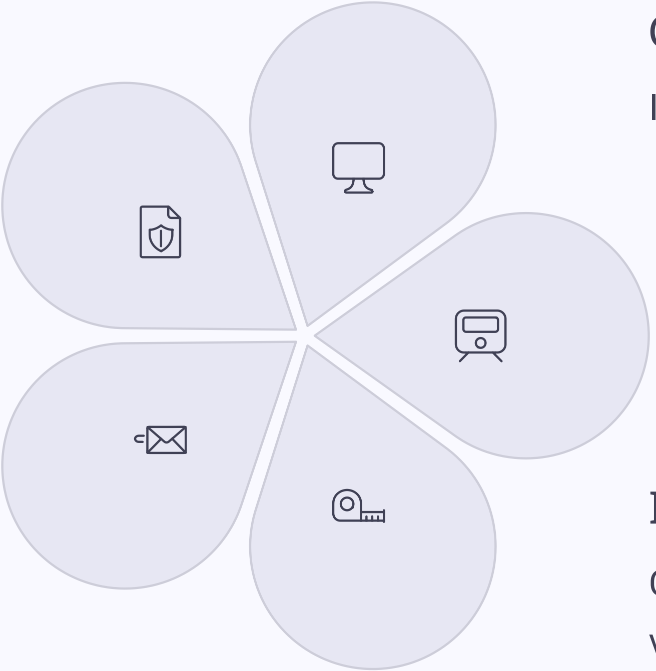
There's so much your business can do to protect itself

As cyberthreats become more sophisticated and frequent, building a strong security culture is essential. A proactive approach to cybersecurity starts with fostering a mindset that prioritizes security at every organizational level. This includes constant monitoring and end-user training to enhance resilience, ensuring that every employee understands their role in protecting sensitive information. By instilling a security-first mentality, organizations can empower their workforce to recognize potential threats and respond appropriately.

Taking action to predict and prevent attacks before they occur is the most effective way to stay secure. This includes implementing regular security assessments, encouraging open communication about vulnerabilities, and creating an environment where employees feel comfortable reporting suspicious activities.

By emphasizing the importance of a collaborative approach to cybersecurity, businesses can create a culture that not only mitigates risks but also enhances overall organizational effectiveness.

Let's dive into specific strategies.



Security Culture

Foster organization-wide security awareness

Constant Monitoring

Implement continuous threat detection

User Training

Educate employees on security best practices

Regular Assessments

Conduct security audits and vulnerability testing

Open Communication

Create channels for reporting suspicious activities

Proactive defense

The general rule of thumb when it comes to protecting your sensitive data is to adopt a multi-layered approach.

This includes using advanced security platforms, educating users on cyber threats, enforcing strong authentication methods, and keeping systems and software up to date. Additionally, backing-up data in separate locations, monitoring for vulnerabilities, and controlling access to sensitive information also reduces risks and improves overall security.

> "Previously, we were receiving urgent, reactive outreach—often from individuals who weren't even clients yet, just looking for immediate help. Fortunately, that's no longer the case. Now, we're seeing more proactive engagement from people who are planning ahead and seeking structured support."

Multi-layered Security

- Advanced security platforms
- User education programs
- Strong authentication methods
- Regular system updates

Data Protection

- Segregated data backups
- Offline backup copies
- Regular backup testing
- Controlled access to sensitive information

Continuous Improvement

- Vulnerability monitoring
- Security posture assessments
- Proactive threat hunting
- Adaptation to emerging threats

End-user training and security awareness

Raising awareness of cybersecurity issues amongst your staff and training them and protect themselves and the company against threats is the most all-around effective cybersecurity measure.

Human error is one of the most significant gateways for cyberthreats, but it also represents an area that is easy to fortify and can be vital in the fight against malicious actors. Leveling up staff and cultivating a culture of cybersecurity awareness is a huge part of any security arsenal and a great way to take a proactive approach to security.

> "The most cost-effective investment in cybersecurity is end-user training—it delivers the greatest impact for the resources spent."

Here are some ways to drive this culture change:

Improve employee awareness about the importance of securing information, of legitimizing third-party requests, two-factor authentication, and protecting private and personal information.

Promote cross-functional collaboration across all departments when it comes to security. When engineering, IT, and marketing work together, it can prevent smaller security incidents from spiraling out of control, help to quickly remediate the issues that do arise, and generally create a more adaptable environment, essential to surviving the IT and cybersecurity landscape.

Reach out to a certifiable third-party partner who has deep expertise in crafting security strategies, providing training, and acting as a resource for organizations.

Awareness Building

Educate on securing information, verifying requests, and implementing two-factor authentication

Cross-Functional Collaboration

Integrate security practices across engineering, IT, marketing, and other departments

Expert Partnerships

Engage with third-party security specialists for strategy development and training

Continuous risk management and assessment

Cyberthreats are always changing, so cybersecurity efforts need to shift to match them. Businesses always have to monitor current and potential threats, assess and manage risk, and develop robust incident response plans. This ensures an agile, responsive, and effective security infrastructure that can adapt quickly to threats as they evolve and grow.

Updates and tests aren't just a nice-to-have (or an annoying pop-up getting in the way of day-to-day work). They are an essential part of protecting a business in a time of constantly changing threats. Security protocols go from effective to obsolete faster than ever before, so regular updates and rigorous testing are imperative if you want to patch vulnerabilities and stay safe in the face of emerging threats.

> "Security is an ongoing process, not a final destination. You'll never reach a point where you're completely protected. It's essential to continuously evaluate how the business evolves and identify new areas where additional safeguards can be implemented."

Here are some ways that organizations can proactively manage their cybersecurity exposure:

Data Protection Strategies

- Have offline, regularly tested, and segregated backups
- Ensure data is segregated through storage and operability
- Maintain business continuity in the event of an attack

Organizational Readiness

- Clearly define maintenance responsibilities
- Conduct regular vulnerability tests
- Run pressure tests on systems
- Implement organization-wide security exercises

Application whitelisting

Application whitelisting offers an effective layer of security by allowing only pre-approved applications to run within an organization's network. This proactive measure significantly reduces the risk of malware and unauthorized software, as it prevents potentially harmful applications from executing - even if they manage to infiltrate the system. By maintaining a curated list of trusted applications, organizations can create a controlled environment that limits exposure to vulnerabilities.

Application whitelisting aids in compliance efforts by ensuring that only verified software is used, reducing the likelihood of data breaches and enhancing overall cybersecurity posture. Implementing this strategy not only helps safeguard sensitive information but also reinforces a culture of security awareness among employees, as they become more engaged in understanding which applications are deemed safe for use.

Leveraging AI technology

The potential of AI and automation in the cybersecurity sphere has only just begun to be explored, and 2025 will see exponential growth in its application. These innovative technologies stand to become linchpins in augmenting cybersecurity efforts, thanks to AI-driven data analysis and automated threat detection, response, and mitigation.

Though time will tell exactly how AI will transform the technology industry and by proxy, cybersecurity, it's clear that it will help organizations move more quickly in the case of incidents, from detection to protection to mitigation to business continuity.

> Cyber defenders will use gen AI and related technologies to strengthen detection, response, and attribution of adversaries at scale, as well as speed up analysis and other time-consuming tasks such as reverse engineering.'

-**Cybersecurity** Forecast 2024, Google Cloud

Adopting CIS compliance

Compliance that anyone can adopt is the Center for Internet Security's (CIS) Critical Security Controls Implementation Group 1 (IG1). It focuses on basic cybersecurity hygiene that is essential for all organizations, regardless of size or resources.

This group emphasizes foundational practices such as inventory management of hardware and software, continuous vulnerability management, and secure configuration of systems and applications. By prioritizing these fundamental controls, organizations can significantly reduce their exposure to common cyberthreats and establish a solid security framework.

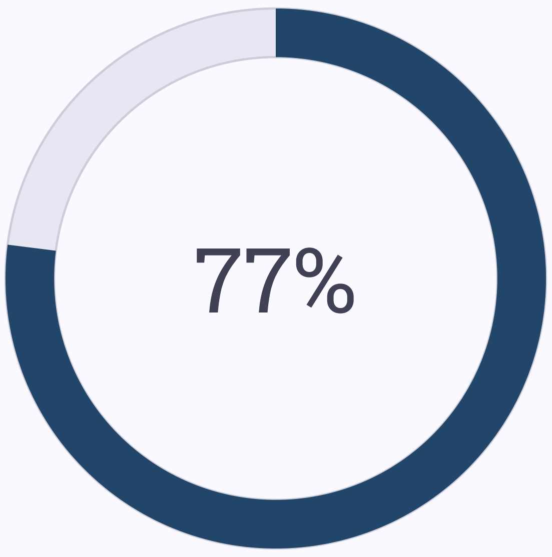
By **implementing** CIS IG1 compliance, businesses can be protected against 77% of malware attacks; 78% of ransomware; 86% of web application hacking and 85% of insider privilege and misuse.

Furthermore, the implementation of IG1 helps organizations develop a culture of security awareness, as employees are encouraged to actively participate in maintaining security standards. Plus, it aligns organizations with industry best practices, providing a structured approach to cybersecurity that can evolve as threats do.

Engaging trusted security partners for comprehensive solutions

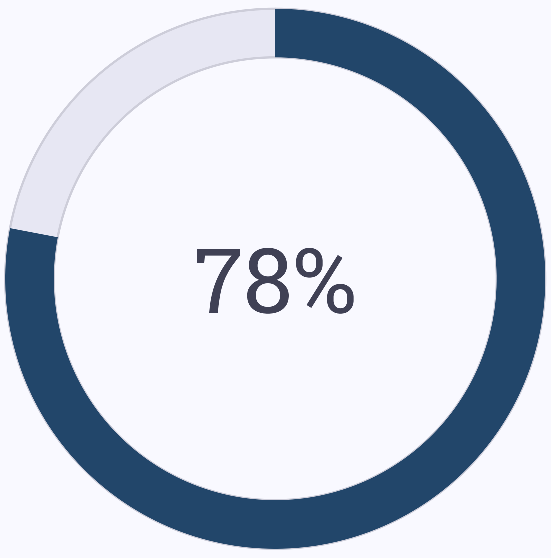
Teaming up with trusted cybersecurity experts is one of the best strategies to deal with the intricate and complex cybersecurity landscape in front of us.

From the latest technology to bespoke, comprehensive strategies tailored to specific organizational needs, a trusted partner is a key part of making a business more resilient.



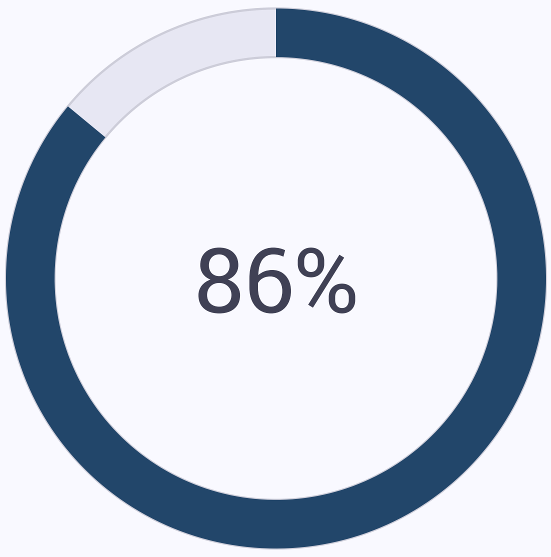
Malware Protection

Percentage of malware attacks prevented with CIS IG1 compliance



Ransomware Defense

Percentage of ransomware attacks mitigated through compliance



Web Application Security

Percentage of web application hacking attempts prevented

Conclusion

As we enter 2025, technology will be driven by an even greater reliance on cloud infrastructure and advancements in AI technologies. Businesses will continue harnessing these innovations to streamline operations, enhance efficiency, and explore new opportunities. With this rapid evolution comes a host of challenges that demand our attention.

The persistent evolution of cyberthreats, coupled with the complexities of hybrid work environments and interconnected systems, necessitates a proactive and adaptable approach to cybersecurity. Organizations must not only embrace cutting-edge technologies but also prioritize building a strong security culture and implementing secure preventive measures.

The journey ahead is filled with possibilities, and prioritizing cybersecurity is not a nice to-do but a must-do for business that want to succeed. Those that neglect their security posture do so at their own risk.

At Velocity IQ, we stand ready to act as a trusted partner. We help businesses navigate the complex landscape and become stronger and more resilient across the board. Our expertise and innovative solutions are tailored to allow organizations to take proactive strategies and fortify their defenses.

Contact us today for a personal assessment to explore how customized IT solutions can secure your business.

Embrace Innovation

Harness cloud infrastructure and AI advancements while maintaining security

Build Security Culture

Prioritize organization-wide awareness and proactive defense strategies

Partner for Success

Engage with cybersecurity experts to navigate the complex threat landscape