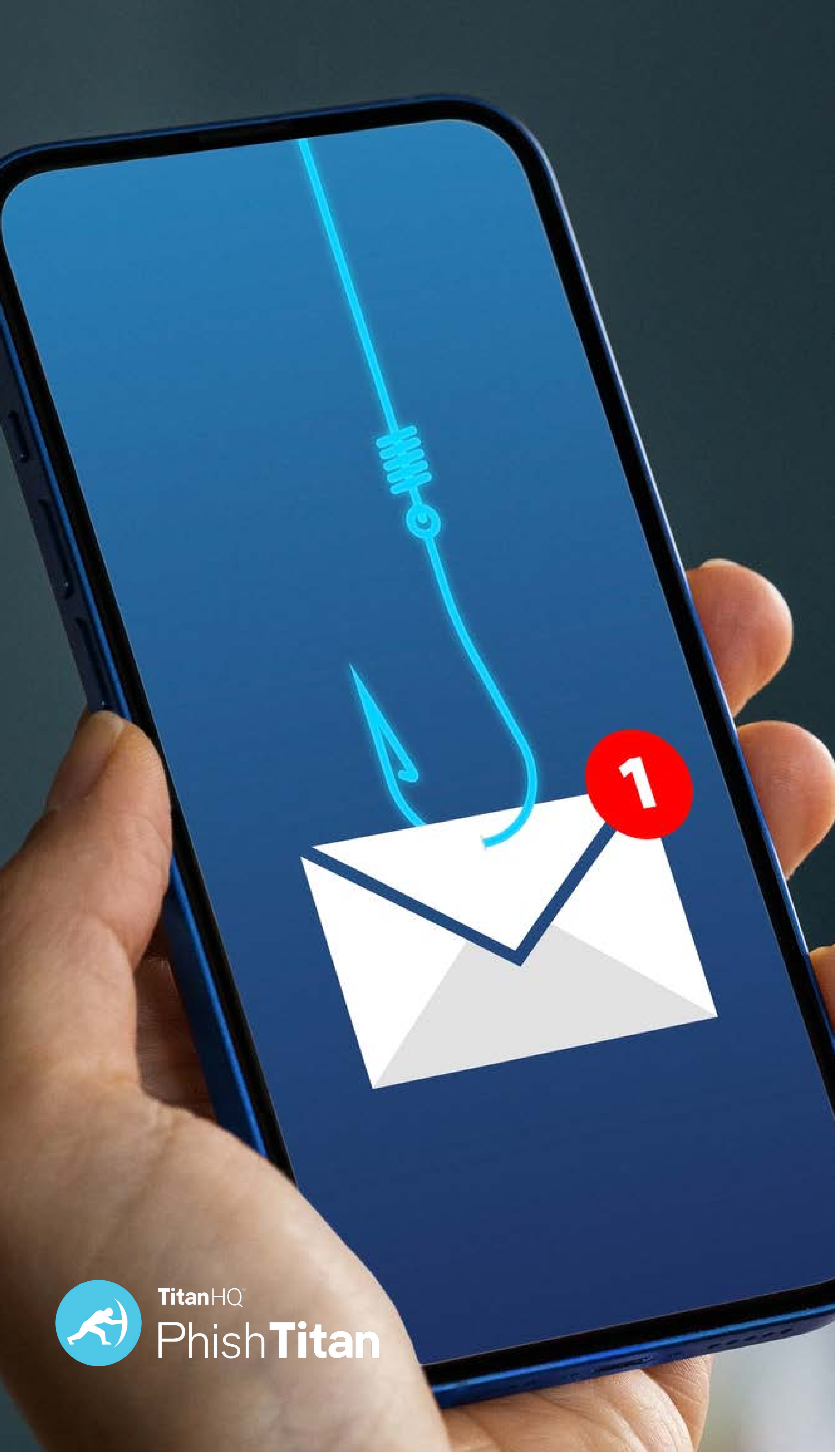
TitanHQ™
PhishTitan

Enhancing Your Microsoft 365 Email Security:

How PhishTitan Can Boost Your Email Defenses



MSPs: Secure Superior Email Protection

4 out of 5 Fortune 500 companies[1] utilize the Microsoft 365 (M365) cloud-powered productivity platform — yet cyberattacks are still possible on their M365 network. As more and more companies store important, sensitive data on their M365 accounts, it's not enough to rely on one service alone.

PhishTitan from TitanHQ is a cloud-based, AI-driven, enterprise anti-phishing solution that offers additional security for companies using Microsoft 365. It provides advanced phishing protection against malicious email, utilizing the most sophisticated tools in the IT world. PhishTitan delivers your clients best-in-class phishing protection for M365 by offering an additional layer of security after default security.

This guide helps highlight today's most dangerous threats, shines a light on the gaps in Microsoft 365's out-of-the-box defenses and details how to fortify your clients' security defenses with PhishTitan.

We cover:

- ✓ TitanHQ's heritage in email security
- ✓ The current state of play in email security
- ✓ Today's most dangerous cyberattacks and why M365 is vulnerable
- ✓ How to bolster your M365 email security with PhishTitan

Source: e2e assure[1]

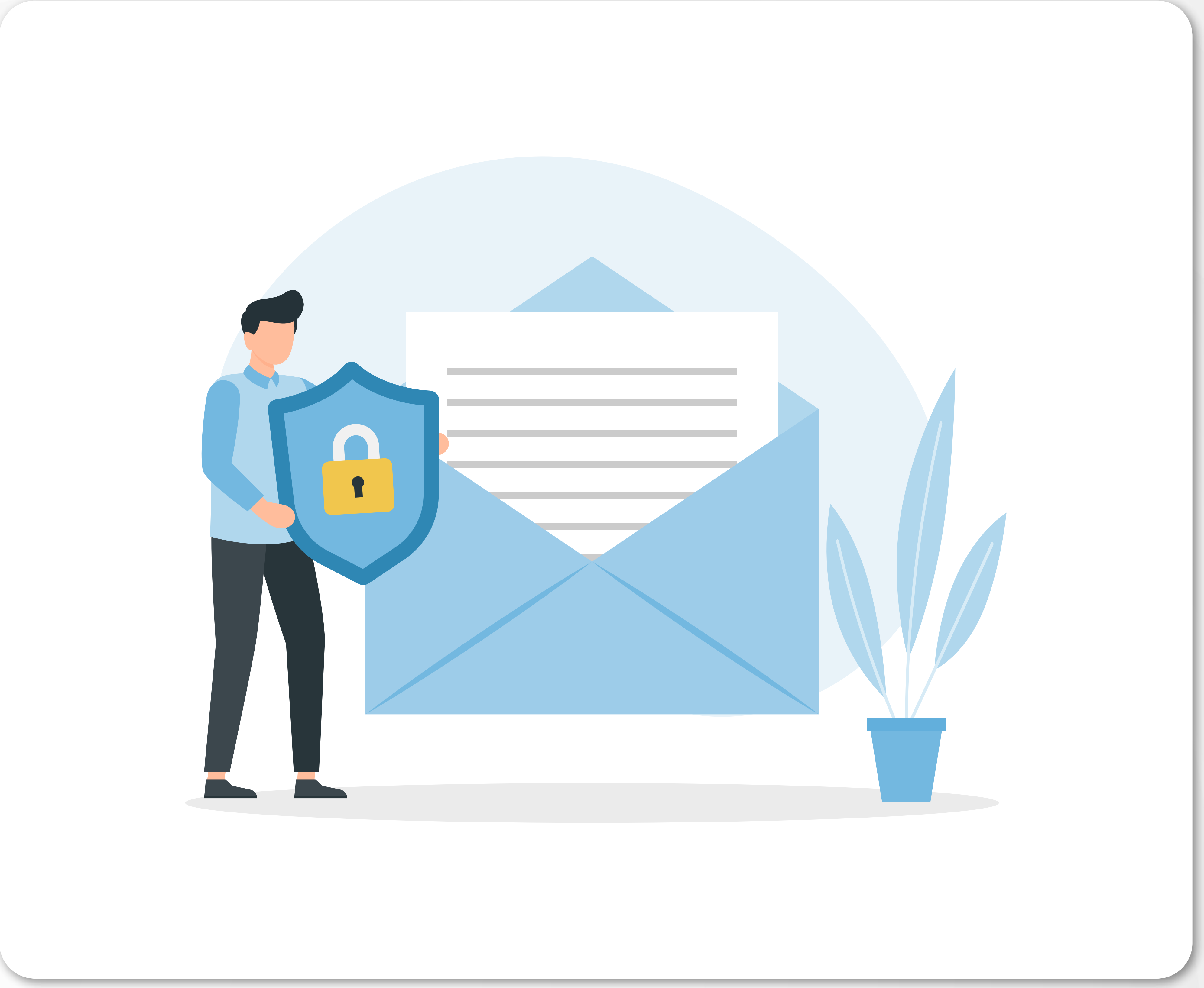
TitanHQ - A Rich History in Email Protection

With over two decades of experience, TitanHQ has been a pioneer in the field of email protection. At the heart of their commitment to safeguarding digital communications is SpamTitan, a secure email gateway that has shielded billions of emails from malicious threats for over 20 years.

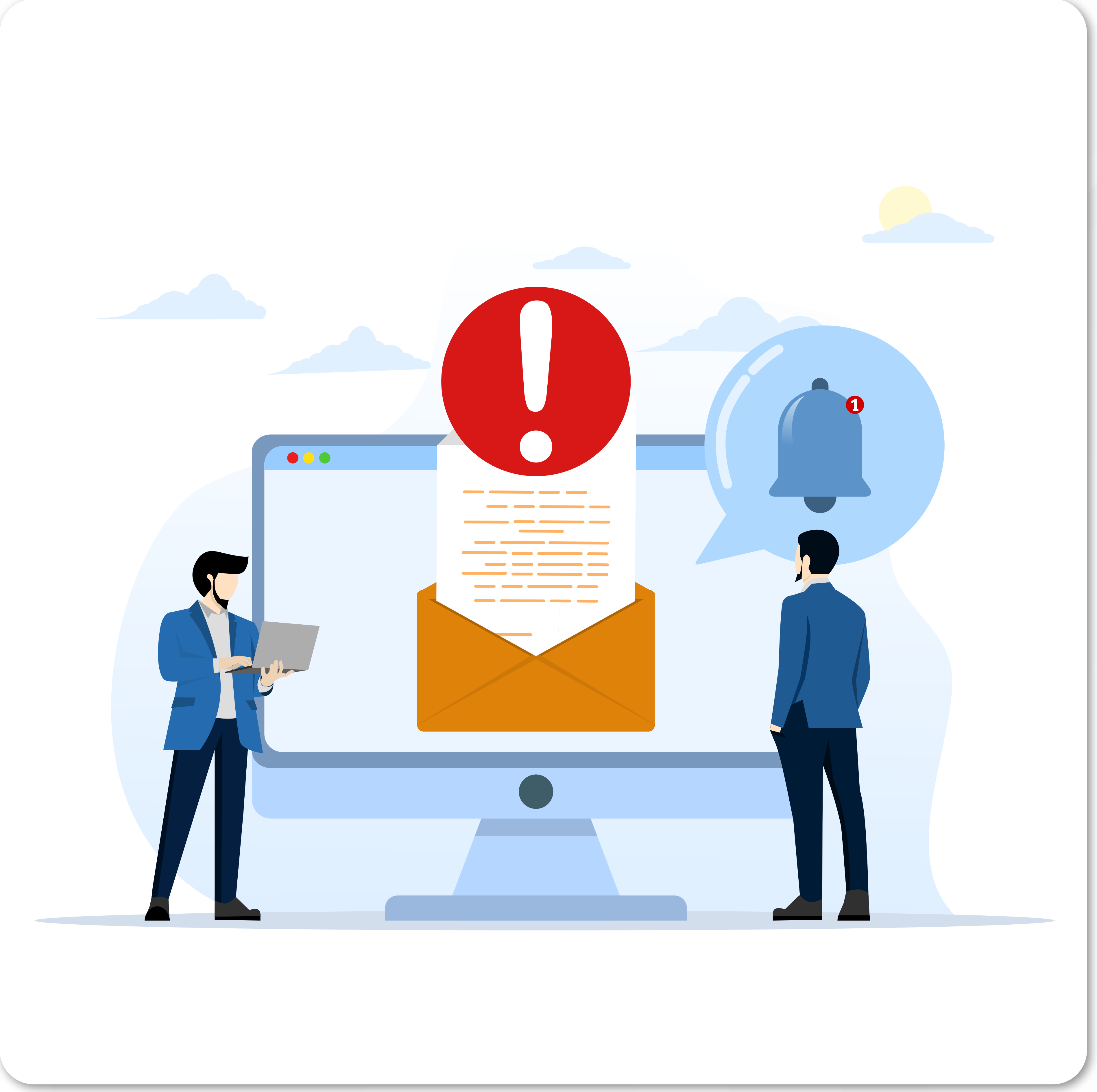
Secure email gateways play a crucial role in safeguarding businesses from cyberthreats, monitoring and filtering both incoming and outgoing emails. Specifically, they aim to identify malicious content, links and attachments, including malware or phishing attacks. As emails continue to remain a top form of communication for organizations, it makes them a primary target for cybercriminals.

Advanced secure email gateways include such defenses as threat intelligence, sandboxing and URL rewriting. These strategies not only scan for potential attacks but also aid employees in preventing them from inadvertently releasing sensitive data that can cause financial or reputational damage.

SpamTitan developed secure email gateways that use the most advanced machine learning and algorithms to land a 99.9% spam catch rate[2]. As a result, SpamTitan's leading solution has led to numerous awards and recognition in the industry.



Source: TitanHQ[2]



The Conceptualization of Email: Past to Present Day

The digital communication of email has been around for nearly 50 years and has seen much evolution since its launch. The 1950s and 1960s saw progression in the use of personal emails, but it wasn't until 1978 that email marketing made its debut with the first unsolicited mass email, which, in turn, led to the first email spam. By the 1990s, when email platforms like Outlook and Hotmail became popular, spam also became commonplace.

As a result, spam-blocking technologies and governmental legislation protecting users from spam began to develop. Since the early 2000s and the release of other devices that could accept and receive emails (mobile phones), spam and malware only became a more widespread issue for millions of users worldwide. More email platform companies, including Gmail, continued to release anti-spam technologies and strategies but also introduced personalization from gathering user data.

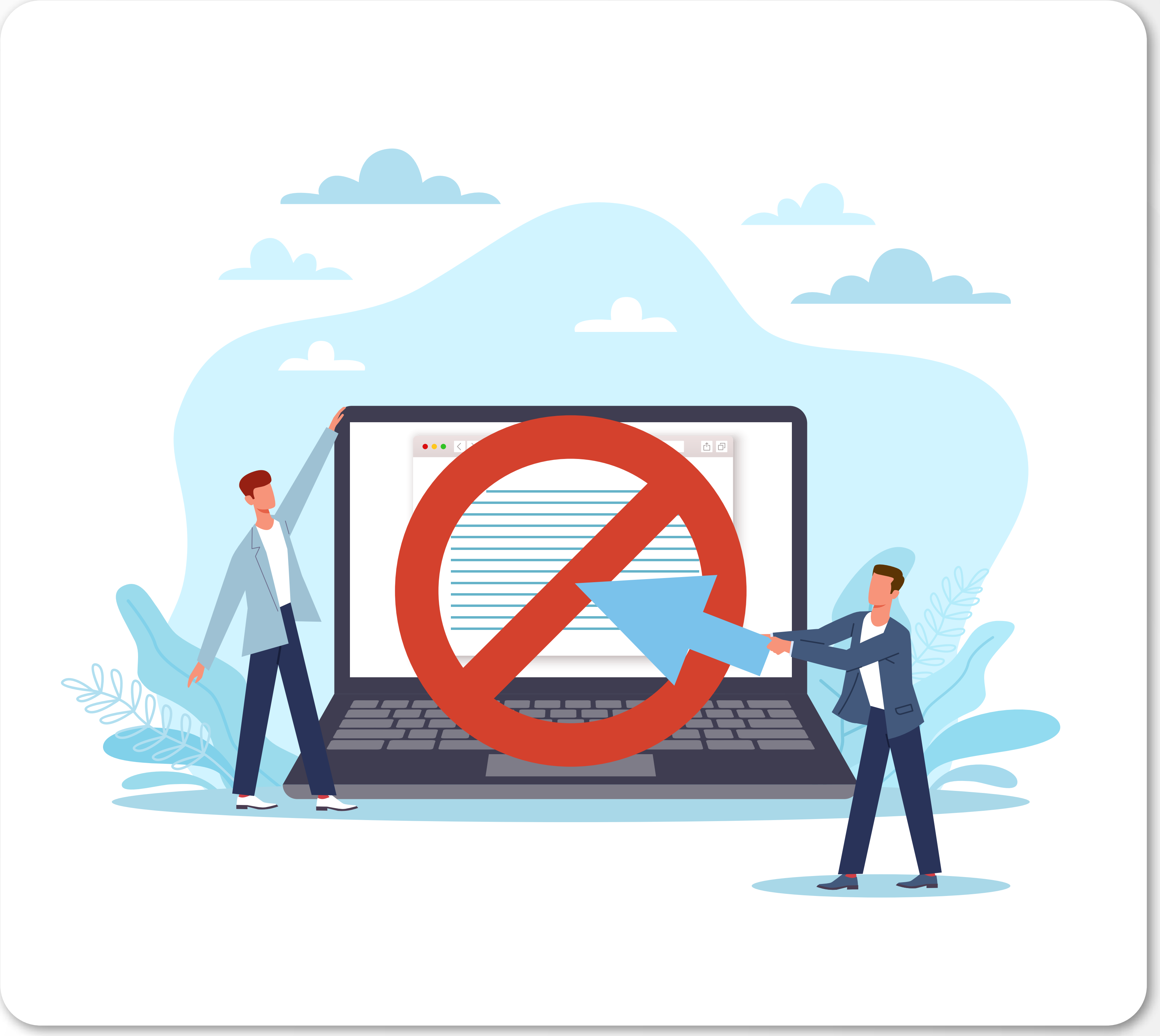
As such, email is not dead but continues to require strict monitoring to comply with worldwide governmental demands for the protection of user data and the minimization of spam.

Breaking Down Virtualization

However, it’s not just the introduction of spam technologies that have contributed to the development of email communication over the years. Virtualization has also come into play to expand the usage and advancement of emails.

Virtualization refers to creating multiple virtual email servers or instances on a single physical server or infrastructure. This enables organizations to efficiently manage and isolate email services for different purposes or clients within a shared environment. Each virtual email server functions independently, allowing for greater resource optimization and security while reducing the need for separate physical servers for each email system.

Still, virtualization comes with its own security issues. As virtualization often involves shared storage resources, data leakage, cyberattacks and unauthorized access are still possible. Virtualization requires a strict need for strong access controls, regular security audits and assessments of virtualized infrastructure.



TitanHQ
PhishTitan

TitanHQ: Adapting to Market Demands

TitanHQ's journey began as a hardware-based solution provider, purpose-built to fight email threats and ensure organizational security. As the cybersecurity landscape evolved, so did TitanHQ. It transitioned to the versatile realm of virtualization, offering organizations greater flexibility and scalability to adapt to evolving threats.

The evolution from hardware-based solutions to virtualization and, ultimately, Software-as-a-Service (SaaS) has transformed the IT landscape, presenting Managed Service Providers (MSPs) with both risks and opportunities. Initially, MSPs primarily dealt with hardware-centric infrastructure, providing on-premises solutions to clients. This model offered stability and control but often required substantial upfront costs and complex maintenance.

As the industry shifted towards virtualization, MSPs had to adapt. Virtualization allowed for more efficient resource utilization and scalability, reducing hardware costs and offering greater flexibility. MSPs that embraced this change gained a competitive edge by providing clients with streamlined, cost-effective solutions.

The emergence of SaaS marked a pivotal moment in this market shift. SaaS solutions offer clients the convenience of accessing software applications and services over the internet, eliminating the need for local installations and hardware maintenance. While this provided better flexibility and accessibility, it also posed challenges for MSPs. They faced the risk of reduced reliance on traditional MSP services like hardware procurement and maintenance. It also demanded continuous adaptation to remain relevant in an ever-changing technology landscape.

Now, TitanHQ is once again at the forefront, having evolved to become a leading Software-as-a-Service (SaaS) vendor dedicated to delivering cutting-edge email security and security awareness solutions.

Current Market Conditions: Navigating the Cloud Email Era

In recent years, the tech landscape has seen a big shift towards the adoption of cloud-based email systems, highlighted by leading research firm Gartner[3]. This transition to cloud-based email solutions represents a transformation in how organizations manage their communication infrastructure, offering unmatched flexibility in an increasingly digital world.

Transitioning to the cloud offers access to enterprise-grade applications without substantial infrastructure investment. As well as providing strict security frameworks, cloud-based email services are also scalable and accessible. This in turn encourages productivity and teamwork via collaboration tools.

As for disadvantages, it all comes down to cloud management. Cloud customers have limited control over the underlying infrastructure and services. This lack of control can lead to concerns about customization, performance optimization and the ability to address specific IT requirements.

Source: Gartner[3]

M365 and the Cloud

M365 is a stand-out example of a cloud-based email solution, gathering immense popularity among MSPs and their clients. Its diverse range of bundles and pricing options caters to the varied needs of businesses, making it a versatile choice for organizations of all sizes.

Yet, M365's popularity also makes it a prime target for cyberattacks. As organizations move their data to the cloud, questions arise about the effectiveness of built-in security like Microsoft Defender. There is uncertainty about whether these measures can truly defend against today's cyberthreats, as highlighted in these statistics:

A survey of 27 million users across 600 enterprises found that 71.4% of Microsoft 365 business users suffer at least one compromised account each month.[4]

Source: Coreview[4]

9 out of 10 cybersecurity professionals see the need to supplement Microsoft's built-in email security features.[5]

Source: Mimecast[5]

Windows Defender blocked phishing sites only 68% of the time.[6]

Source: All About Cookies[6]

The Gaps in your Defenses

So, what weaknesses does Microsoft Defender have? The main issue centers around Microsoft Defender's list of scanning exceptions, which users can set to prevent legitimate apps from being mistakenly treated as malware. However, this list lacks proper security measures, allowing any user to access it. As a result, local users can query the registry and obtain information about the excluded locations, such as files, folders and processes. Hackers with local access to a compromised Windows machine can hide and run malware from these excluded folders, evading detection.

Microsoft Defender also exhibits weaknesses in independent antivirus evaluations, sometimes falling short compared to dedicated third-party antivirus solutions in detecting advanced malware and achieving high detection rates. A 2022 study by anti-malware assessment company AV-Comparatives found that Microsoft Defender had an offline detection rate of only 60.3%.[7]

This raises concerns for users who prioritize robust security and rely on their antivirus software to defend against various threats. To address these limitations, some users bolster their security by pairing Microsoft Defender with third-party antivirus or anti-malware tools for more comprehensive protection against evolving threats.

The most common examples of attacks against M365 include:

- Phishing
- Business Email Compromise (BEC)
- Email Account Takeover
- Cloud Data Theft
- Ransomware
- Data Theft

Source: AV Comparatives[7]

An Increasingly Dangerous Threat Environment

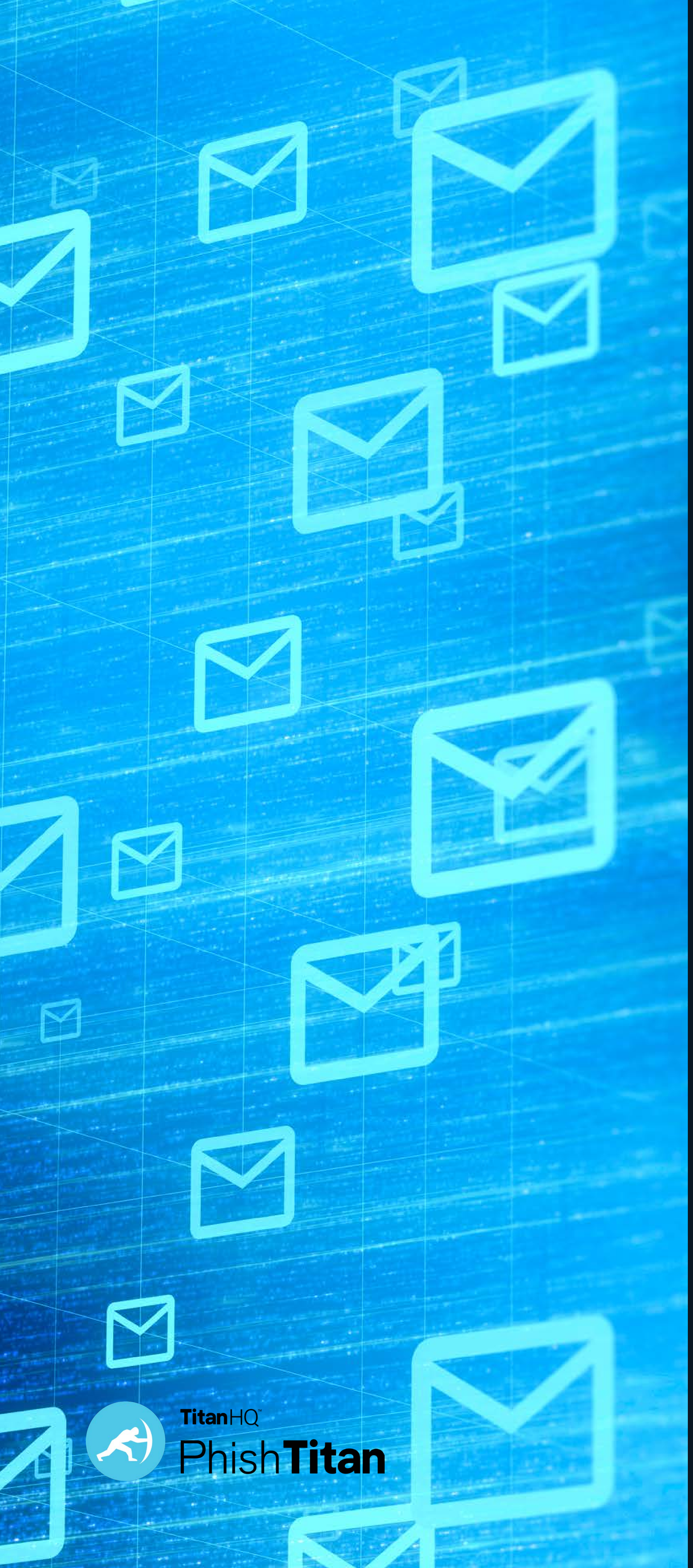
The current state of cybersecurity paints a sobering picture – it's a dangerous time in the digital realm.

For example, electronic fraud continues to grow year after year, with phishing being the most prevalent type (FBI).[8] Masquerading as legitimate email messages, these attacks trick receivers into divulging sensitive information or downloading malicious links.

Moreover, ransomware remains the highest threat in the cyberthreat landscape, according to the 2023 ENISA Threat Landscape (ETL) report[9]. The impact of these ransomware attacks is catastrophic in terms of cost, reputational damage and data loss. Quite simply, the importance of cybersecurity during these turbulent times cannot be overstated.

Source: FBI[8]

Source: Enisa Europa[9]



The Solution: Bolster Your M365 Email Defenses With PhishTitan

While M365 does a fantastic job at securing email inboxes, it's not a perfect solution. Even with its strong defenses, threats still find a way to slip through the cracks. That's why it's essential to reinforce your M365 email security.

PhishTitan delivers your clients best-in-class phishing protection for M365 by offering an additional layer of security that complements EOP and Defender.

Built-in security measures within Office 365 and Gmail still may not catch everything. In fact, 25% of phishing emails manage to evade detection by Office 365's Exchange Online Protection (EOP)[7]. This sobering statistic highlights the need for complementary products to bolster Microsoft 365 and enhance your email protection.

Why PhishTitan + M365

PhishTitan is designed to provide comprehensive phishing protection, enhancing Microsoft 365's offerings with advanced security features driven by leading-edge technology, improved detection accuracy and an unparalleled user experience. PhishTitan adds a layer of security after the default security to catch any missed attacks, providing the capability for post-delivery remediation across multiple tenants in less than 10 minutes.

Powered by cloud technology and AI, PhishTitan employs a multi-layered approach for unbeatable anti-phishing accuracy. It halts all phishing attacks through careful email analysis, real-time link checks and one-click inbox cleansing by administrators.

Source: AV Comparatives[7]

Key Features

PhishTitan leverages the following features to ensure ultimate phishing detection, prevention and protection:

AI-driven anti-phish analysis

URL rewriting for enhanced link protection

Time-of-click protection to verify website safety

Banner notifications to flag phishing emails

Detailed and insightful reporting

Native Microsoft 365 integration for seamless operation

Post Delivery Remediation for swift threat mitigation

Quick and easy deployment

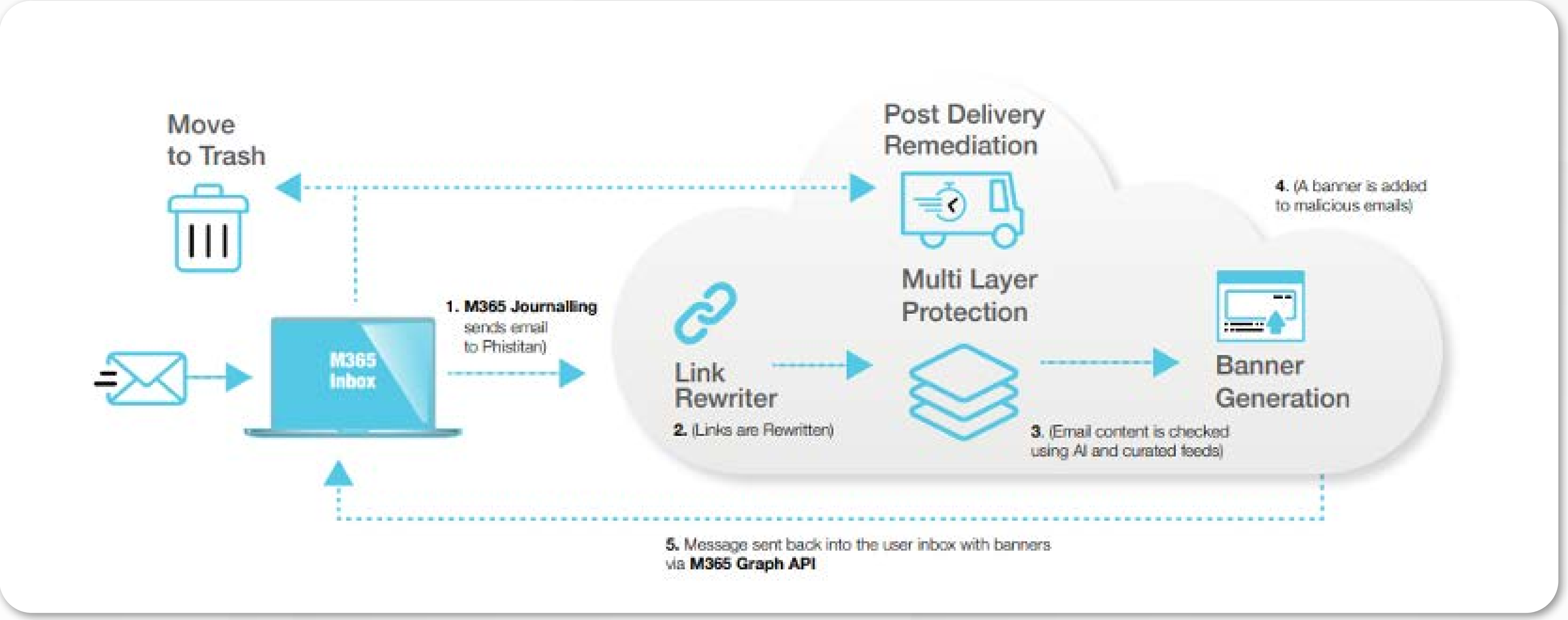
User-friendly interface

End-user feedback option

Robust malware protection

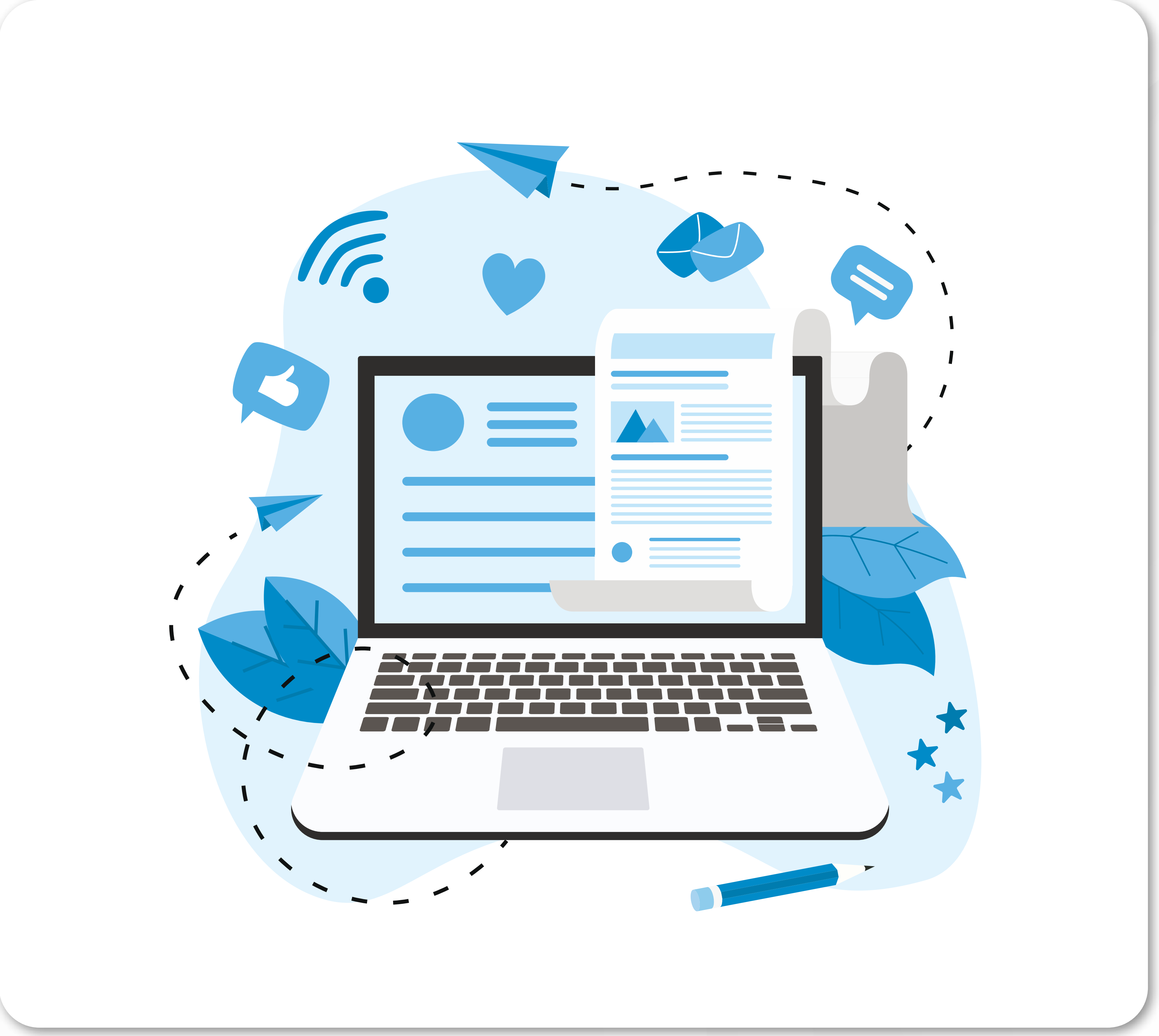
How It All Works

PhishTitan seamlessly integrates with Microsoft 365, adding a security layer that complements EOP and Microsoft Defender. Through API connectivity, it simplifies onboarding, streamlines management and enhances protection. As a bonus, it handles post-delivery remediation across multiple tenants, reducing risk


Move to Trash
Post Delivery Remediation
4. (A banner is added to malicious emails)
M365 Inbox
1. M365 Journalling sends email to Phistitan)
Multi Layer Protection
Link Rewriter
2. (Links are Rewritten)
Banner Generation
3. (Email content is checked using AI and curated feeds)
5. Message sent back into the user inbox with banners via M365 Graph API

Advanced Protection

PhishTitan employs AI to verify phishing attempts and analyze links included in emails to assess their legitimacy. It identifies zero-day attacks by mimicking human interaction with potentially malicious websites, ensuring comprehensive threat coverage. Additionally, the use of Large Language Models (LLMs) enhances threat analysis and safeguards against unknown phishing attacks. With URL rewriting and multi-point protection, PhishTitan leaves no room for email threats to infiltrate your organization.



Office 365 Native Integration

PhishTitan seamlessly connects through API and Journalling with Microsoft 365, ensuring emails are always delivered to your inbox. This integration is based on Microsoft Active Licensed Users count, simplifying vendor reconciliation. The new user interface is intuitive and aesthetically pleasing, making navigation a breeze.

User Reporting

PhishTitan provides insightful reporting to keep you informed about your email security status. Detailed real time reporting is available as both a summary page which reflects the threats targeted over time and as an Insights view, which identifies the relationships between that data. In a world where Microsoft 365 is a prime target for cybercriminals, having a multi-layered security approach is crucial. PhishTitan is tailored to meet the specific requirements of Managed Service Providers (MSPs), enabling efficient management of multiple clients and rapid response to threats across various email tenants.

Training and Support

PhishTitan additionally offers comprehensive customer support to ensure a smooth implementation process. Webinars and courses are also designed to help you effectively utilize all of PhishTitan's features and educate your users about the various phishing threats they may encounter.

TitanHQ
PhishTitan

Close the Net with PhishTitan from TitanHQ

In an increasingly saturated MSP market, we want to help you offer a comprehensive security portfolio to stand out from the crowd and grow your business at speed and scale.

PhishTitan does just that with increasing ROI, cost savings, and efficiency gains. It's designed to deliver unbeatable anti-phishing accuracy, minimal false-positive results, and ease of use. PhishTitan's world-class AI and unparalleled threat intelligence provides high detection accuracy across your customers' environments – allowing your team to focus on higher-level tasks that grow your business.

Are you ready to learn more about PhishTitan's superior protection capabilities and how it works seamlessly with Microsoft 365?

Get in touch with us to discover its powerful potential. Book your demo today.

Get in touch