

Paysafe 

Cybersecurity Report: Strategies for a safer future





Contents

1.	Leadership perspective	3
2.	Security by the numbers	4
3.	Navigating the threat landscape	6
	AI-powered attacks: A double-edged sword	
	Credential theft: The new normal	
	Supply chain risks: The weakest link	
	On the horizon	
4.	Our actions	9
	Trust and resilience	
	Visibility and control	
	Agility and innovation	
	Compliance and assurance	
5.	Culture of security	12
	Building awareness and habits	
	Fostering ownership and accountability	
	Working together across borders	
	Earning recognition for leadership	
6.	Looking ahead	15
	Priorities for 2026	
	Innovation at the core	
	A commitment to transparency and trust	

Leadership perspective

A message from Paysafe's CEO:



Bruce Lowthers

CEO

“Every transaction is an opportunity to build trust. As we continue to expand Paysafe globally, our focus remains on delivering secure, seamless payment experiences that empower our customers and partners. We operate in a fast-moving industry, but our values stay the same: security, clarity, accountability, and a commitment to doing what’s right. That’s how we create long-term value.

Our strategy encompasses more than just technology. It’s about building confidence in every transaction and every relationship. Whether we’re expanding into new markets, launching innovative products, or strengthening our security posture, we’re guided by a simple principle: protect what matters most. We’re proud of the progress we’ve made, and we’re even more excited about what’s ahead. Together, we’ll continue to raise the bar, challenge assumptions, and put the ‘safe’ in Paysafe - not just as a name, but as a promise.”

A message from Paysafe's CISO:



Alan Osborne

CISO

“At Paysafe, we don’t just react to threats; we look to anticipate them. Cyber threats are rapidly becoming increasingly sophisticated, so our strategies must evolve just as quickly to stay ahead. That’s why we’re investing in technologies like quantum computing and AI, not as experiments, but as strategic tools to future-proof our business. These innovations will redefine how we protect our customers’ data against theft and fraudulent use, and deliver secure financial experiences at scale.

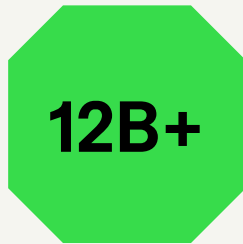
However, technology alone isn’t enough. Our strength comes from our people, our culture, and our unwavering focus on security and governance. We believe trust is built through strong controls, ongoing monitoring, and open communication. Looking ahead to 2026 and beyond, our priority is clear: to protect what matters most and to move forward with purpose, safeguarding every customer, every partner, and every transaction.”

Security by the numbers





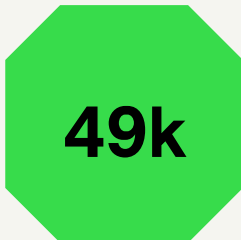
Potentially harmful emails blocked, including 2.9M malicious threats and 4.1M spoofed addresses.



Unauthorized network connections blocked, detected and responded to 136,335 intrusion attempts.



Security training modules issued to Paysafe employees with a 99.9% completion rate.¹



Phishing simulations launched.



Automated cloud security checks continuously monitored across our environments, with our 24 x 7 security operations center.



Invested in bug bounty ethical hacking program to ensure our systems remain resilient from web-based threats.



Third-party risk analyses conducted on critical and high-risk vendors.



Audit controls tested across PCI, SOC-2, and ISAE3402 frameworks.

***Figures recorded September 2024 – September 2025**

¹The deviation from 100% reflects employees who leave Paysafe before completing the training modules. The training is mandatory, and disciplinary actions are taken if training is not completed (up to and including termination of employment).



Navigating the threat landscape



Cyberattacks are becoming more sophisticated and complex. Threats such as AI-driven malware, credential theft, social engineering, and supply chain manipulation and activity linked to nation-state actors require agile and adaptive defenses. Threat actors now have access to better tools, made more powerful by the widespread use of AI. In the near future, quantum computing may pose new risks to cybersecurity by undermining current encryption methods, potentially allowing attackers to decrypt sensitive information and increasing the scale and severity of cyber threats. Paysafe has responded with a layered strategy to adapt quickly, spot threats early, and maintain consistent protection.



AI-powered attacks: A double-edged sword

Artificial intelligence has been the most transformative technological shift since the advent of the Internet. Its rapid advancement is unlocking new possibilities across industries, but it also introduces complex threats that challenge our defenses, governance frameworks, and detection capabilities in unprecedented ways. While organizations use AI to streamline operations and detect anomalies, threat actors are weaponizing it to supercharge attacks. Today, generative AI is being used to craft polymorphic malware that adapts in real-time, evades detection, and spreads autonomously across networks. These attacks are no longer manual; they are automated, precise, and relentless.

Recent incidents observed in the industry have highlighted how AI can be used to insert malicious code into software updates, hijack firmware in connected devices, and impersonate trusted users with remarkable accuracy. These methods enable attackers to move laterally across networks, escalate privileges, and avoid detection for long periods.

In response to emerging threats, Paysafe acted quickly to deploy AI-powered threat detection across its infrastructure, integrating anomaly detection tools and behavioral analytics to strengthen our defenses and improve real-time monitoring. Our Cyber Threat Intelligence Center uses machine learning to proactively spot emerging threats, allowing quicker containment and response.



Credential theft: The new normal

Attackers are increasingly logging in using stolen credentials instead of breaking in through malware or cyberattacks. According to IBM, 74% of cyberattacks now depend on valid credentials, making identity theft the leading tactic.²

Paysafe has taken decisive steps to reduce credential-based risks. We have implemented passphrases and passkeys across our workforce to lessen reliance on traditional passwords. Just-in-time access controls, ensure that privileged access is closely managed and time-limited. Over the past year, we've blocked multiple customer account takeover threats, nearly all of which came from stolen customer credentials.

² [ibm.com/reports/threat-intelligence](https://www.ibm.com/reports/threat-intelligence)



Supply chain risks: The weakest link

Recent research shows that supply chain cyberattacks surged by 179% year-over-year in 2024³, while 35.5% of all data breaches originated from third-party vendors.⁴ Attackers exploit trusted relationships by targeting smaller suppliers with weaker security and injecting malware into software updates and APIs.

Modern supply chains rely heavily on APIs, which continue to be a target for attackers. To strengthen our security posture, Paysafe conducted 114 detailed vendor assessments over the past year, reinforcing our third-party risk management and ensuring tighter controls across our ecosystem.

These assessments help find and fix vulnerabilities before they can be exploited. We have also enhanced our API security monitoring and implemented continuous cloud posture checks. Over 2,500 cloud controls are scanned every day and are automatically risk assessed to ensure secure configurations are consistently maintained across our systems, following industry best practices.



On the horizon

The threat landscape is evolving, and so are we. Paysafe's layered defense strategy uses AI-powered detection, identity-first security, and thorough third-party oversight. We don't just respond to threats; we're prepared for them.

As attackers grow more sophisticated, our commitment to proactive security, transparency, and innovation remains unwavering.



³ checkpoint.com/resources/items/report--cyber-security-report-2025

⁴ securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/



Our actions



Paysafe strengthened its defenses to stay resilient in this shifting threat landscape. From blocking malicious traffic and securing credentials to expanding threat visibility and embedding security into our code development, our actions reflect a commitment to agility, innovation, and compliance.



Trust and resilience

Over recent months, we've strengthened our infrastructure to withstand evolving threats and ensure business continuity and operational resilience. Our strengthening of Web Application Firewall configurations across all payment platforms blocked malicious traffic and secured online transactions, bringing further defence-in-depth security, and additional layers of communication inspection and control.

To decrease the risk of insider threats and credential misuse, we introduced passphrases and passkeys, replacing traditional passwords. Our just-in-time access controls ensure privileged access is granted only when necessary, reducing exposure.

Paysafe also conducted 13 IT disaster recovery exercises and multiple tabletop simulations over the last 12 months to validate our crisis response capabilities.



Visibility and control

We expanded our detection and monitoring capabilities to gain deeper insight into threats.

Our Cyber Threat Intelligence Center delivers real-time analysis of emerging risks, while our AI-based Network Detection and Response and Endpoint Detection and Response tools continue to evolve to address the latest threats, offering visibility across endpoints and network traffic.

We also deployed User Behavior Analytics tooling to detect anomalies and policy violations, and enhanced our Email Security controls to further protect against the latest phishing, business email compromise, and social engineering threats.

“The key challenges facing the industry are the proliferation of identities, securing AI-driven workloads, and maintaining resilience against increasingly sophisticated attacks.” - Alan Osborne (CISO)



Agility and innovation

Security is embedded into our development lifecycle and cloud operations. We conducted an independent Security SDLC review to verify secure coding practices and benchmarked our systems against industry benchmarking standards.

Our Cloud Security Posture Management platform continuously monitors for new vulnerabilities and any misconfigurations. On a daily basis, we conduct over 2,500 automated cloud security checks, enabling quick remediation, if required, and enhanced posture awareness.

We also enhanced our security controls for end user computing devices (laptops) by standardizing the security controls across all device types, strengthening access controls, and reflecting strong identity, device, and data protection across our environment.



Compliance and assurance

Paysafe maintains rigorous compliance with global standards. We achieved PCI DSS 4.0.1 certification across all payment card products and completed 1,867 audit controls within PCI, SOC-2, and ISAE3402 frameworks.

An independent Cyber Maturity Assessment validated our program's strengths and guided continuous improvement. We also enhanced our quantum computing readiness, and joined a research consortium to explore quantum machine learning for fraud detection.

Additionally, our Data Sensitivity Labelling and Data Loss Prevention (DLP) implementation guides proper classification and classification of sensitive information across the organization.

“By using internal security tools, we can centralize identity governance, reduce operational overheads, reduce risk, and improve our compliance posture overall.” - Alan Osborne (CISO)

Culture of security



Security at Paysafe is more than just a technical discipline. It's a shared duty that influences how we work, communicate, and create. Over the past year, we have strengthened our commitment to fostering a culture where every employee contributes to safeguarding our business and customers.



Building awareness and habits

We distributed 32,000 security training modules over the past 12 months, achieving a 99.9% completion rate, up from 99.6% the previous year.⁵ These modules covered phishing awareness, secure data handling, and authentication best practices, tailored to roles and regions.

Our phishing simulation program launched 49,000 targeted campaign emails, which helped strengthen vigilance, and improve response times across the organization. With this program, we've consistently met industry benchmark standards in key metrics such as click rate, data input and reporting.



Fostering ownership and accountability

Security is embedded in our daily operations at Paysafe. Employees are expected to report suspicious activities, challenge assumptions, and take part in tabletop exercises. Our SOC team works around the clock, supported by a global network of over 100 dedicated security professionals, who are complemented by numerous teams across Paysafe, where a security culture is ingrained in everything we do.

Regional security champions help localize training and drive adoption, ensuring that security is relevant and actionable across all teams.

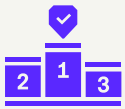
To ensure our cybersecurity controls are not only strong in theory but also effective in practice, we recently brought in an independent team of cybersecurity experts to conduct a red team exercise. A red team simulates the tactics, techniques, and procedures of real-world attackers, trying to breach our systems just like a sophisticated cybercriminal would. This thorough test aimed to challenge our ability to prevent, detect, and respond to advanced threats. By partnering with an external firm, we ensured the exercise was unbiased and comprehensive, giving us valuable insights and confirming our security posture. The results were very encouraging, boosting our confidence in the maturity of our cybersecurity program and highlighting areas for ongoing improvement.



Working together across borders

Over the past few months, we've strengthened our cross-functional security efforts by increasing integration across product development, IT operations, and compliance, emphasizing our commitment to embedding security throughout the organization. Our Cyber Threat Intelligence Center shares insights across departments, which enables quicker decision-making and coordinated responses.

⁵The deviation from 100% is the result of employees who leave Paysafe before completing the training modules. The training is mandatory, and disciplinary actions are taken if not completed (up to and including termination of employment).



Earning recognition for leadership

Paysafe's dedication to cybersecurity has earned industry recognition. Most recently, Paysafe was awarded the 2025 Global Fintech Award for Sustainable Fintech. This acknowledgment highlights how our focus on secure innovation and responsible growth continues to set industry standards and reinforce our cybersecurity leadership.

In 2024, we were listed on the BusinessCloud FinTech 50, honoring the UK's most innovative financial technology developers. In the same year, we were awarded 1st place in the Cybersecurity category at Bulgaria's Company of the Year Awards. We also appeared in The Times' Financial & Legal Portfolio for our leadership in secure digital payments.

These accolades reflect the strength of our security culture and the trust we've built with customers, partners, and regulators.

“Protecting confidential data is at the heart of everything we do. It’s about building brand reputation and customer trust.”
- Alan Osborne (CISO)



Looking ahead

As we enter 2026, Paysafe remains committed to advancing our cybersecurity approach through innovation, transparency, and ongoing improvement.

Our goal is simple: to keep putting the “safe” in Paysafe; not just in name, but in every transaction, every system, and every decision.



Priorities for 2026

Our cybersecurity roadmap for 2026 focuses on three key areas: expanding threat detection, enhancing identity and access controls, and strengthening oversight of third-party risks. We will continue to invest in automation and AI-powered security operations to reduce response times and improve accuracy.

We continue to conduct disaster recovery exercises and cyber crisis simulations across business units to verify our response capabilities and strengthen cross-functional coordination. We will continue to expand our cybersecurity program testing, increasing the frequency of tabletop simulations and conducting additional red team exercises to further enhance our preparedness.

These efforts will enable us to test resilience more broadly, simulate emerging threat scenarios, and ensure readiness across different regions and teams.



Innovation at the core

We are exploring how quantum computing can change fraud detection and risk modeling. Paysafe is investigating quantum algorithms that could identify fraud patterns more quickly and accurately, enabling us to approve legitimate transactions with greater confidence while blocking threats more effectively. This effort is part of a larger innovation plan that includes expanding our use of AI and automation to improve anomaly detection, streamline compliance processes, and personalise security experiences.

These technologies will help us grow securely while maintaining the trust of our customers and partners.



A commitment to transparency and trust

Security isn't just about technology; it's about trust. In 2026, we'll continue to share our progress openly, collaborate with regulators and industry peers, and release insights that help elevate standards across the sector.

Our dedication to transparency involves conducting continuous cyber maturity evaluations, engaging in external audits, and participating in collaborative threat intelligence networks.

We believe that transparency is key to strengthening resilience and building trust. Sharing insights and experiences with peers and competitors is not only the right thing to do, but also a crucial step toward improving industry-wide security and safeguarding the broader digital ecosystem.

Paysafe's mission is to provide secure, seamless payments worldwide. As threats evolve, so will we, with more innovative tools, stronger partnerships, and an unwavering focus on protecting our systems, data, and customers.



About Paysafe

Paysafe is a leading payments platform with an extensive track record of serving merchants and consumers in the global entertainment sectors. Its core purpose is to enable businesses and consumers to connect and transact seamlessly through industry-leading capabilities in payment processing, digital wallet, and online cash solutions. With 30 years of online payment experience, an annualised transactional volume of \$152bn in 2024, and approximately 3,000 employees located in 12+ countries, Paysafe connects businesses and consumers across 260 payment types in 48 currencies around the world. Delivered through an integrated platform, Paysafe solutions are geared towards mobile-initiated transactions, real-time analytics and the convergence between brick-and-mortar and online payments.

Further information is available at www.paysafe.com.