appgate

FRAUD BEAT

ANNUAL REPORT

FRAUD BEAT 2026

AI AND ADVANCED STRATEGIES TO COMBAT **DIGITAL FRAUD**

TABLE OF **CONTENTS**

Introduction: A New Era of Digital Threats 3

Top Attack types in 2024 4

Trend Analysis: 2024 vs 2023 5

Impact of AI on Major Attacks in 2024 6

The AI Arms Race: How Machine Learning Fuels Both Fraud and Defense 7

AI in Fraud Detection

Future Trends

Proactivity as the Cornerstone of Cybersecurity 8

Proactivity in Action: Appgate's Commitment 8

Compliance with ISO Standards 9

Looking to the Future 9

appgate

INTRODUCTION

A NEW ERA OF ***DIGITAL THREATS***

In 2024, the cyber threat landscape transformed dramatically, with a 57% rise in global incidents compared to 2023. Attackers exploited advanced tools like malware, phishing and fake social media campaigns to target identities and credentials. Latin America and Asia-Pacific were particularly affected, facing high volumes of phishing and malicious redirects, while the United States struggled with compromised accounts and unauthorized mobile apps.

This report uncovers key cyber threat trends of 2024, delves into the most affected regions and industries, and explores effective strategies to protect against these ever-evolving risks.

appgate

TOP ATTACK TYPES **IN 2024**

Analysts at Appgate's Security Operations Center (SOC) noted these key trends in 2024:

- ***86%*** of the threat incidents reported were due to phishing, making it the most common type of attack by cybercriminals. The attacks included malicious redirects and fake social media campaigns, with LATAM and APAC being the most affected regions.
- ***12%*** of the incidents were related to fake social networks used to impersonate brands and individuals. This attack type was particularly prevalent in LATAM, with Argentina, Brazil and Ecuador reporting the highest number of incidents.
- The exploitation of public applications accounted for ***15%*** of the incidents and was a common initial vector in both LATAM and APAC. Cybercriminals exploited insecure configurations to gain access to sensitive systems.

Appgate's Security Operations Center (SOC) made significant strides in 2024, strengthening its ability to detect, mitigate and respond to cyber threats more efficiently. Here are some of the most notable advancements:

1. **Stronger Alliance with Google** – A new collaboration with Google has enhanced our blocking speed in Chrome, leading to faster phishing mitigation for end users and improved negotiations with service providers.
2. **Trusted Reporter Status with Replit** – Appgate was officially recognized as a Trusted Reporter by Replit, reinforcing our credibility in identifying and reporting fraudulent activity.
3. **Enhanced Internal Monitoring** – Continuous improvements in our SOC monitoring processes have increased detection accuracy and response times.
4. **Insights into Phishing Trends** – Our latest analysis highlights how certain hosting providers have significantly reduced their response times to takedown requests, contributing to improved industry-wide phishing mitigation.

PHISHING *71%*

REDIRECT PHISHING *14%*

FAKE SOCIAL NETWORK *12%*

OTHERS *3%*

TREND ANALYSIS: ***2024 VS 2023***

Comparing 2023 and 2024 data reveals a significant increase in the volume of incidents, according to the attack types managed by the **SOC.**

Key findings include:

PHISHING INCIDENTS GREW BY **86%**

FAKE SOCIAL MEDIA CASES NEARLY DOUBLED, INCREASING BY **99%**

The exponential growth of phishing and fake social media incidents in 2024 demonstrates that cybercriminals are increasingly leveraging social engineering and digital platforms to execute their attacks. This increase reflects the increasing sophistication of the methods usedand the ability of attackers to exploit trust in online applications and platforms. Organizations must respond with robust detection, proactive prevention and the continuous monitoring of emerging threats.

IMPACT OF AI
MAJOR ATTACKS IN 2024

In 2024, artificial intelligence (AI) played a crucial role in the evolution of cyberattacks most affecting our customers. AI advancements have enabled cybercriminals to enhance the sophistication, effectiveness and scale of their tactics, particularly in phishing, fake social network attacks, and malware-as-a-service (MaaS).

PHISHING

AI enabled attackers created personalized messages using public data and deepfake technologies, increasing the success rate of campaigns.

FAKE SOCIAL MEDIA

Intelligent bots powered by generative AI operated fake profiles and identified vulnerable targets.

MALWARE-AS-A-SERVICE (MAAS)

AI-driven tools automated the distribution and customization of malware, making attacks more devastating.

"Losses from generative AI fraud in the US are projected to reach $40 billion by 2027. This escalation points to the urgent need for various industries to stay not just one but several steps ahead of fraudsters".

-Fraud.net

THE AI ARMS RACE: HOW MACHINE LEARNING FUELS BOTH FRAUD AND DEFENSE

AI is significantly reshaping the landscape of digital fraud, introducing both new challenges for prevention and innovative methods for fraudsters.

"Fake content has never been easier to create—or harder to catch. As threats grow, banks can invest in AI and other technologies to help detect fraud and prevent losses."

-Deloitte Center for Financial Services

AI IN FRAUD DETECTION

In response to these evolving threats, organizations are increasingly adopting AI-driven fraud detection systems. These systems utilize advanced algorithms to analyze vast amounts of data for irregular patterns indicative of fraudulent activity. By continuously learning from interactions, AI enhances its predictive capabilities, enabling quicker identification and response to potential fraud.

FUTURE TRENDS

As the sophistication of AI tools continues to grow, so does the complexity of fraud schemes. Experts predict that the integration of AI into both fraudulent activities and detection strategies will necessitate a multi-layered approach to network security. Companies are advised to employ AI, not just as a defense mechanism but also as a countermeasure against the very tactics used by fraudsters.

With Appgate's 360 Fraud Protection solutions, businesses gain access to tools that evolve with threats, such as machine learning algorithms designed to anticipate and neutralize attacks.

PROACTIVITY AS THE ***CORNERSTONE OF CYBERSECURITY***

In a world where cyber threats are constantly evolving, being protected requires a proactive approach and advanced solutions. Organizations face significant challenges due to the growth of sophisticated attacks such as phishing, information disclosure and unauthorized use of trademarks. Without a solid strategy, the financial, reputational and operational impact can be devastating.

STAYING AHEAD OF THE CURVE:

The modern threat landscape is dynamic. Attackers are leveraging generative AI to create more convincing phishing campaigns and malware. Staying ahead requires not just responding to incidents but anticipating future attack vectors with adaptive defenses. Conduct regular cybersecurity assessments to detect and fix vulnerabilities before they can be exploited.

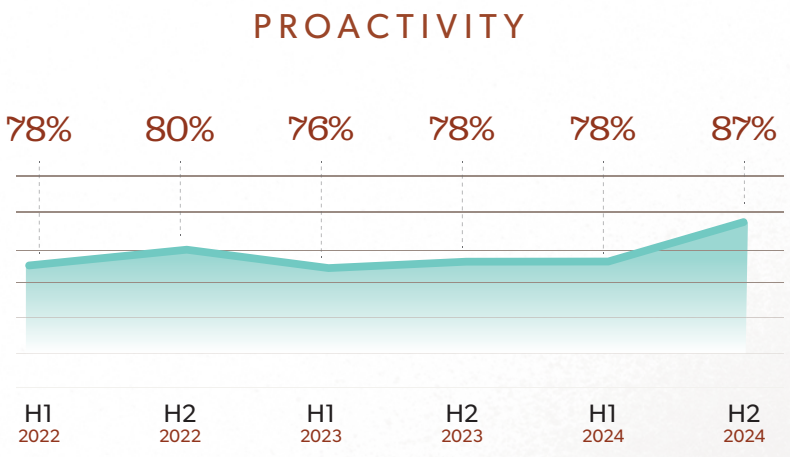
OUR STRATEGIES TO HELP YOU STAY PROTECTED INCLUDE:

1. **Real-Time Threat Mitigation:** Leveraging AI-driven technology enables organizations to identify vulnerabilities and mitigate threats before they escalate. This proactive approach ensures emerging risks are addressed as they unfold, minimizing exposure to potential breaches.

2. **Advanced Detection Solutions:** By continuously monitoring suspicious access patterns and behavior, companies can anticipate attacks rather than merely reacting to them. Proactive detection systems offer a layer of defense that evolves alongside cybercriminals' tactics.

PROACTIVITY IN ACTION: ***APPGATE'S COMMITMENT***

Since 2022, Appgate has consistently achieved a global proactivity rate above 80%, demonstrating its commitment to staying ahead of cyber threats. Despite a significant increase in ticket volume, proactive measures have driven remarkable growth in effectiveness, culminating in an impressive 87% proactivity rate in the second half of 2024. This upward trend underscores the strength and adaptability of Appgate's solutions in the ever-evolving threat landscape.



COMPLIANCE WITH ***ISO STANDARDS***

Appgate's 360 Brand Guardian helps the financial industry comply with multiple ISO standards by detecting and eliminating digital threats that compromise information security, cybersecurity and fraud prevention. For example, ISO 27032, which focuses on cybersecurity and protection against online attacks, aligns with 360 Brand Guardian's ability to prevent brand identity exploitation. Here's how we can help your organization:

ISO 27032 (Cybersecurity)

1. **Cyberattack protection:** Detect and neutralize phishing attacks, fake sites and online fraud.
2. **Web and dark web threat mitigation:** Identify malicious domains before they are used in fraud campaigns.
3. **Collaboration with other security measures:** Integrates with fraud detection and identity protection tools for a comprehensive security strategy.

360 Brand Guardian acts as an essential layer of protection for companies looking to strengthen their digital security and comply with international regulations. Its ability to identify and eliminate threats on the web, coupled with its integration with broader cybersecurity strategies, makes it a key tool within any risk management and compliance program. By reducing the risks of fraud like phishing and, it helps organizations maintain the trust of their customers and operate securely within the framework of international best practices.

LOOKING TO ***THE FUTURE***

The future of cybersecurity demands a multi-layered approach that balances cutting-edge technology with a vigilant, forward-thinking strategy. By investing in robust defenses and fostering a culture of awareness, organizations can protect their data, their operations and—most importantly—the trust of their customers.

ABOUT **APPGATE**

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards thousands of enterprises and government agencies worldwide. Learn more at appgate.com.

appgate