The state of cyber-security

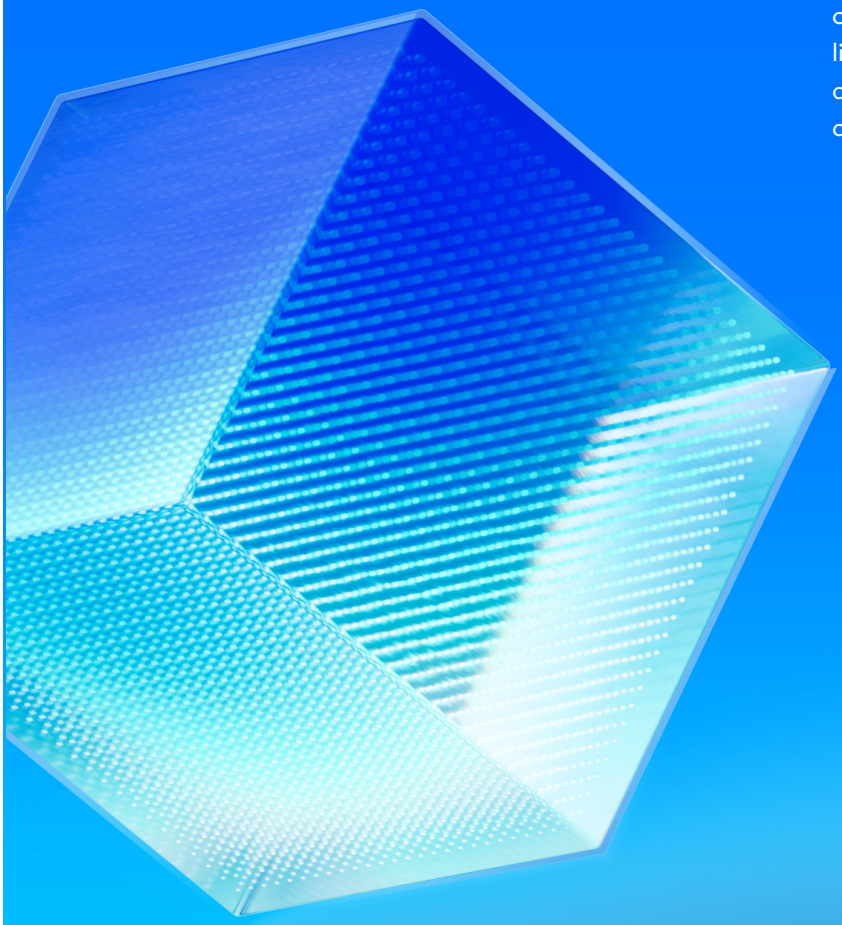
Your guide for 2025 and beyond

What we believe

Cyberattacks happen. It may seem easy to ignore cybersecurity and take the "it will never happen to me or my business" stance. We get it—cybersecurity is an overwhelming topic.

That's why Field Effect exists.

We believe all businesses deserve powerful, cost-effective, and easy-to-use cybersecurity to protect their operations from cyber threats. No matter your security knowledge, resources, or budget, cybersecurity should be approachable and attainable for you.



But where do you start?

We created this eBook to highlight the recent changes in the cybersecurity landscape and share a look ahead to the future. Inside, you'll find new and emerging threats to watch for alongside other key information that will help you keep your business secure.

More than anything, we want to stop cyber criminals from hurting businesses and people like you. We've got your back. If you have any questions, or if there's anything further we can do to help, please reach out.

Table of contents

Staying ahead of a changing security landscape

Year after year, there's one constant throughout the cybersecurity landscape: change.

Attackers relentlessly test even the strongest defenses, while defenders lose sleep trying to secure their company's attack surface.

And then, the game shifts again.

Attackers have an infuriating ability to find innovative ways to breach businesses. New tools, technologies, and processes—meant to strengthen operations—can inadvertently introduce vulnerabilities that cybercriminals are eager to exploit.

This endless cycle might feel daunting, but it's no reason to throw in the towel. Instead, make 2025 your most secure year yet. By adopting a more holistic approach to cybersecurity, you can stay well ahead of emerging exploits and attack vectors.

Before we dive into that strategy, let's take a moment to reflect on the dramatic changes the cybersecurity landscape underwent last year.

24

How cybersecurity changed in 2024

The cybersecurity landscape is in constant flux. Throughout 2024, we witnessed a surge in never-before-seen tactics, techniques, and procedures, along with fresh spins on familiar strategies.

Here are some of the standout trends our experts observed last year.

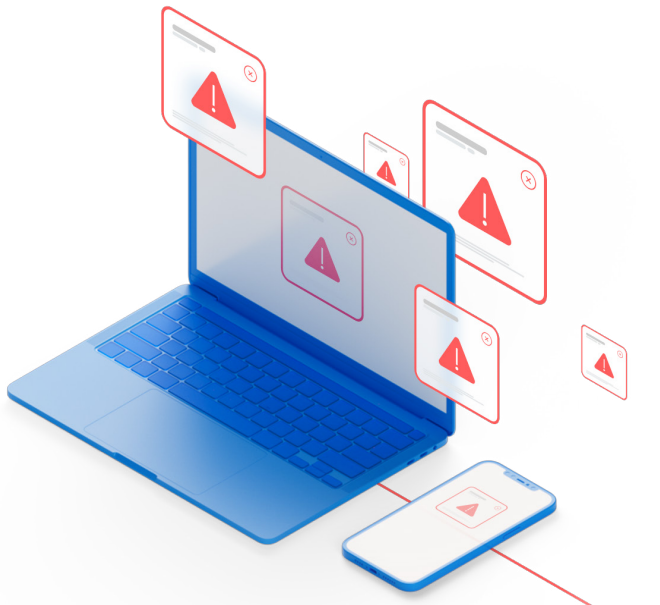
More specific targets for initial access and beyond

In 2024, attackers shifted their initial access focus from endpoint devices to critical network infrastructure, such as routers, firewalls, and VPN gateways.

There are a couple of reasons that this might be the case:

- Network infrastructure gets patched less frequently than endpoints and therefore is more likely to be running outdated and vulnerable software.
- Attackers know that a lot of organizations prioritize protecting their endpoints more than their network, cloud apps, and other areas of the threat surface.

The ArcaneDoor campaign, in which state-sponsored cyber actors targeted perimeter network devices from several vendors, is just one example of this increase. Targeting edge devices such as firewalls, switches, and routers are popular among threat actors seeking initial access to targets of interest. Control of these devices could allow threat actors to monitor and reroute traffic, obtain credentials that could provide access to more sensitive systems and accounts, or launch Adversary-in-the-Middle attacks.



Malware-as-a-service on the rise

The malware threat continued to evolve in 2024, becoming more pervasive and specialized. As the number of threat actors increased, so did the frequency, scope, and sophistication of malware attacks.

A key shift was the growing adoption of modular malware designs, enabling threat actors to quickly adapt attacks to new environments and targets. At the forefront of this trend was the rise of malware-as-a-service (MaaS) platforms. These platforms have significantly lowered the skill barrier for launching advanced attacks, allowing even inexperienced cybercriminals to deploy devastating malware.

For instance, the Redline Stealer MaaS, available on dark web forums, enables attackers to extract credentials and payment information from infected systems. With that information, the hacking opportunities are endless.

This commoditization of malware lowers the barrier to entry for cybercriminal activities, requiring better security measures and user education to properly defend against such threats. Organizations need to adopt behavior-based detection and response tools to counteract increasingly undetectable malware variants.

Dismantling botnet operations

Not all trends were negative. In 2024, law enforcement and cybersecurity organizations ramped up efforts to dismantle botnet infrastructures, marking a significant shift in counter-cybercrime strategies.

One notable success was the FBI's takedown of the Raptor Train botnet, which had exploited unpatched vulnerabilities to compromise over 260,000 devices. Similarly, the Operation Cronos Task Force targeted the LockBit ransomware group, seizing infrastructure and indicting members.

While these operations dealt significant blows to cybercriminals, groups like LockBit have proven resilient, bouncing back in a game of cat-and-mouse with authorities.

Cyber espionage campaigns on ISPs and TSPs

State-sponsored cyber espionage surged in 2024. One of the most alarming incidents involved the Chinese group Salt Typhoon, which breached major U.S.-based ISPs, including Verizon, AT&T, and Lumen Technologies.

These breaches granted unauthorized access to sensitive data, such as user billing information, communication metadata, and potentially even the content of messages. Authorities described this attack as a significant cyber espionage campaign, the implications of which can extend far beyond the immediate victims.

The attack vector—most likely a supply chain breach or zero-day exploit—also raises the possibility that other providers using similar systems could also be at risk.

LOOKING AHEAD:

Emerging threats to watch for

For years, threat actors have mirrored technological advances, continuously refining their tactics to achieve greater success. As someone with a pivotal role in securing private company data and systems, you know how critical it is to stay on top of new and emerging risks.

As you look to the future to strengthen defenses this year, keep these cyber threats top of mind.

Advanced persistent threats employing novel attack techniques

Advanced Persistent Threats (APTs) are highly sophisticated, well-funded groups—often state-sponsored—that target specific organizations or sectors to gather intelligence or disrupt operations.

In 2024, APTs demonstrated an increased use of proximity-based and infrastructure-specific attack methods. For instance, the "nearest neighbor attack" saw APT 28 breaching Wi-Fi networks by targeting devices physically close to their high-value targets. This physical closeness allowed the attackers to bypass certain technical security measures, essentially focusing on exploiting an environmental vulnerability.

This year and beyond, organizations should consider non-digital attack vectors and implement zero-trust architectures that extend to physical environments. This approach will be especially critical in high-value sectors such as energy, finance, and government.

Attacks that circumvent MFA protections

In 2024, Field Effect reported on a new adversary-in-the-middle (AiTM) attack which allowed threat actors to intercept and manipulate communications between two parties, often without detection, to capture credentials and session tokens.

This interception allowed attackers to bypass multi-factor authentication and gain unauthorized access to accounts.

During our investigation, we identified a campaign where attackers used Axios-based lookalike M365 login pages to harvest credentials. Victims were directed to these fraudulent pages, which proxied authentication requests, capturing both passwords and MFA codes. The attackers then used the Axios HTTP client to log into M365 accounts, effectively bypassing MFA.

Additionally, the rise of platforms like the Mamba MFA Phishing Kit, a phishing-as-a-service tool, made it easier for cybercriminals to replicate AiTM attacks. For a small subscription fee, threat actors were able to capture authentication tokens, circumvent MFA, and compromise M365 accounts.

The growing role of artificial intelligence

We can't talk about 2024 and what 2025 has in store without commenting on AI. It has been a huge year for artificial intelligence with tools like ChatGPT becoming mainstream, thanks to integrations into powerhouse ecosystems like Microsoft's Copilot.

However, while mainstream users are enjoying the productivity boost... so are the cybercriminals.

Deepfakes

By now we have all seen compelling examples of fake video and audio produced using AI. It can be used to create and spread disinformation and misinformation online, such as fake news and deepfakes.

Take the cyberattack on a Hong Kong firm as an example, which lost them 25 million USD9. In this attack, the cybercriminals digitally recreated the company's Chief Financial Officer who, during a video call, instructed the employee to transfer the funds.

As deepfake technology becomes more accessible, distinguishing real from fake will grow increasingly tough. Organizations should invest in employee training and AI detection tools to mitigate these risks and counter AI-driven disinformation campaigns.

LLM-powered phishing campaigns

Large language models in particular will likely play a significant role in the evolution of phishing attacks and exploit chain delivery that uses content.

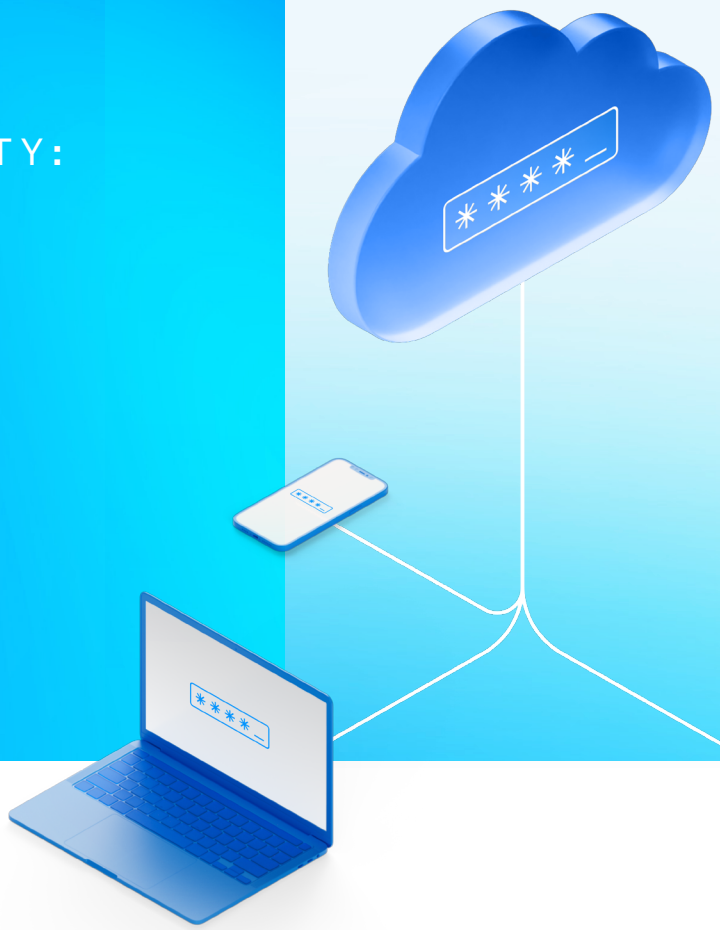
In both, social engineering plays a big part in attack preparation as content is derived and delivered (often via email or text) in hopes of convincing a target to click on a malicious link or provide personal information such as login credentials.

If a threat actor trained an LLM on publicly available information for a target, such as social media profiles or other open-source information, they'd significantly increase their chances of success.

Naturally, a personalized phishing email would be much more effective than general, reusable content. And while the quality of the attack could be greatly improved, there are still a number of other security mechanisms that get in the way, such as email filters and DNS firewalls.

THE FUTURE OF CYBERSECURITY:

Trends, threats, and more



Predicting the future of cybersecurity is no easy task. In a field as dynamic and fast-paced as this, the only certainty is change.

That said, for years we've seen the same patterns again and again. If threat actors are finding success by doing things one way, they'll continue to. Taking a look beyond the next 12 months, a few threats and trends are apparent that will likely play a bigger role.

01

Cyber insurance will drive demand for cybersecurity assessments

The cyber insurance market has faced many challenges, most notably the difficulty of assessing and pricing cyber risk due to the lack of historical data, the dynamic and evolving nature of cyber threats, and the potential for systemic and catastrophic losses.

To ease this burden, we expect cyber insurance providers may require or incentivize their clients to undergo cybersecurity assessments as part of the underwriting process or the policy conditions. This could help the insurers to evaluate the risk profile and premium of the clients, as well as to provide recommendations and guidance for improving their cybersecurity. These assessments can demonstrate a client's compliance with the cyber insurance policy requirements or lower their premiums by showing their security maturity and use of best practices.

02

A growing emphasis on social engineering

We mentioned this last year and it stands true again now. Although security solutions are more robust and powerful than ever, they still face a major challenge: human error. Users can and will continue making mistakes that lead to data loss. We'll continue to see social engineering and phishing attacks, but we'll likely see more complexity there.

We will see more use of AI, because social engineering is all about crafting messages and being able to lure a victim into clicking on a link by sending a legitimate-sounding email. Instead of the typical "password reset" or "mailbox full" scams, AI will allow threat actors to become more sophisticated with their messages.

03

Cloud services increasingly targeted

Companies are using more cloud services than ever before. This is a mix of moving traditionally on-premises services, like email and file sharing, to the cloud, as well as the rise of popular cloud-only collaboration and customer relationship management platforms.

These services are generally set up for the optimal balance between security and productivity. While more secure settings are possible, they often require extra steps that few organizations have the time or technical know-how to take.

This is part of a greater issue regarding the shared responsibility model used by cloud service providers. In this model, both provider and user are partially responsible for the management and cybersecurity considerations of the service, the extent of which is dependent on the service type.

However, organizations using these services often do not fully understand where their responsibilities start and stop, leaving a gap in the implementation of security measures and more vulnerability than necessary.

Threat actors know this, and we expect to see an increase in the targeting of these services, especially those handling high-value data that can be used for extortion or to facilitate financial fraud.

04

Continued exploitation of zero-day vulnerabilities

Cybercriminals have intensified their focus on zero-day vulnerabilities—flaws unknown to vendors—leading to significant security breaches. This trend underscores the critical need for organizations to adopt proactive vulnerability management and threat intelligence to mitigate risks associated with unpatched systems.

For example, Fortinet's CVE-2024-23113 demonstrated how delays in patching could lead to significant consequences. Eight months after its discovery, many organizations had yet to apply fixes, resulting in unauthorized command executions on unpatched systems.

The rapid exploitation of vulnerabilities means patch management must be immediate. Organizations need continuous vulnerability assessments, automated patching tools, and backup strategies. The increasing pace of disclosure-to-exploitation cycles will push this trend further.

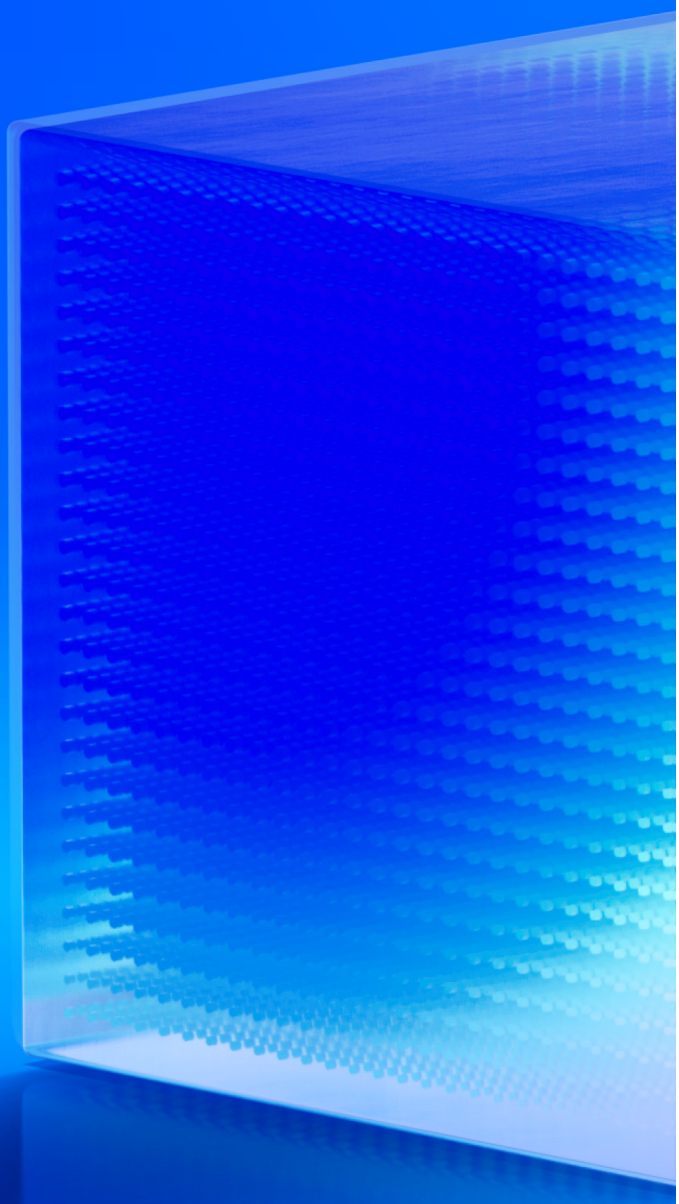
Conclusion

We hope this eBook has given you valuable insight into the future of cybersecurity.

If there's one key takeaway, it's this: cyber threats are real, evolving, and pose significant challenges for organizations of all sizes.

While tools like cyber insurance and backups are essential, they cannot stand alone. The focus, for both businesses and managed service providers (MSPs), should be on proactively securing operations and addressing emerging risks before they escalate. This proactive approach can help prevent cyberattacks, protect sensitive data, and safeguard long-term success.

Whether you're a business leader navigating today's cybersecurity challenges or an MSP supporting your clients, remember that you don't have to face these threats alone. Our mission at Field Effect is to empower organizations with the tools, insights, and expertise needed to build stronger defenses and respond to evolving risks.



Profound simplicity, powerful cybersecurity.

FIELD EFFECT / MDR

About Field Effect

Every business deserves powerful protection from cyber threats.

Field Effect's cybersecurity solutions were purpose-built to prevent, detect and respond to threats for clients of all sizes. We take on the complexity behind the scenes and deliver a solution that's sophisticated where it matters, and simple everywhere else. Consolidate your tech and eliminate the noise while empowering users of all technical backgrounds to confidently navigate cybersecurity and avoid disruptions.

Complexity out, clarity in.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
+1 (800) 299-8986