theNET
BY CLOUDFLARE

Simplifying security in the age of complexity

Leadership perspectives

Contents

Contributors:

Grant Bourzikas
Chief Security Officer, Cloudflare

Emily Hancock
Chief Privacy Officer, Cloudflare

Daragh Mahon
EVP and CIO, Werner Enterprises

Introduction

In an effort to achieve “digital transformation,” businesses have found that technology investments have actually outpaced their ability to see and secure everything.

As they add more API integrations, they’re also increasingly exposed to risks from shadow APIs. As they experiment with generative AI and large language models (LLMs), they must be more vigilant against data loss while also navigating complex privacy and compliance regulations.

For IT and security leaders, it’s a tricky balancing act: They’re expected to secure the entire organization, yet they do not have visibility or control over all of the organization’s digital initiatives. And, for business leaders, enablement for GenAI is a key performance indicator for their success, having to deal with security budgets and internal resources that are strained.

It is no wonder, then, that — according to a survey of more than 4,000 business and technology leaders — 64% of business leaders expect a cyber security incident in the next 12 months, but only 29% feel highly prepared to defend against them.

This guide shares perspectives on how organizations can realize the vision of a secure ***and*** modern distributed enterprise. In it, you’ll hear from a leading CSO on the future of AI, from a privacy expert on advocating for security investments, from an enterprise CIO on battling human error and inattention — and more.

Keep reading, or jump to the chapter that interests you most:

Preparing for the future of AI in cyber security

By Grant Bourzikas
Chief Security Officer, Cloudflare

AI is on everyone's mind today. Large language models (LLMs), like those that power OpenAI's ChatGPT, have sparked our imagination: We are seeing new possibilities for using generative AI to build innovative solutions.

As security professionals, we're thinking about how cyber criminals are using AI to create new types of attacks and strengthen their existing methods. Meanwhile, we're contemplating defensive AI and exploring ways to use AI to better detect and defend against threats.

Still, too many organizations are focusing only on what AI can do today or in the short term. Too few are looking ahead to the tremendous impact AI will likely have on our businesses and our lives in 5, 10, or 20 years. We need to envision that future, though, because to adequately prepare for it, we have to start planning now.

> "Too few are looking ahead to the tremendous impact AI will likely have on our businesses and our lives in 5, 10, or 20 years."

Understanding today and envisioning tomorrow

AI is still a somewhat immature technology. While machine learning (ML) is more mature, the application of ML is still in its early stages. Organizations today are mostly collecting data and doing basic analytics. Some are experimenting with LLMs to generate text or using AI-infused design tools to create unique illustrations. But true AI inference is not yet available: Models cannot yet draw conclusions or generate meaningful insights from live data, even if some vendors tell you otherwise.

That lack of inference is clear when we attempt to use AI and ML for anything more than generating text or images. When I was working on my master's degree in data science and ML, we had a project to try to predict which baseball players would be inducted into the Hall of Fame. The model we created found that the top predictor was the number of at-bats — how many times the player batted over his career. The longer the career, and the more at-bats, the greater likelihood he would make it into the Hall of Fame.

It was an interesting result, but the model couldn't produce any insights from it. The model couldn't tell us why at-bats might be the best predictor. We humans realized, though, that to have a long career, with lots of at-bats, you need to be an excellent player. And when you have a lot of at-bats, you are more likely to have a decent number of hits and home runs.

When models start to understand meaning and gain the ability to make inferences, then we'll see more dramatic effects from AI.

Given the speed of change in AI, inference will be here before we know it. Just think about how far LLMs have progressed in the past few years. They have gone from providing basic text completion to supporting robust text-based conversations that allow for long prompts, accept visual input, and retain context between sessions. Meanwhile, continual increases in computer power are enabling models to rapidly ingest and learn from more and more data, which in turn helps those models produce better, more accurate results.

In 20 years, AI and other advanced technologies will likely reshape our world considerably. For example, we might see fewer people owning cars, because we'll be able to summon fully autonomous cars on demand. Grocery shopping, house cleaning, lawn mowing, and other daily tasks will likely be streamlined by technology.

And yes, it's possible that in the future AI will change many of our current jobs. In the tech industry, we might not have to write code anymore, for example. But we'll still need people to understand how to design AI-based solutions that meet business needs, how to manage this technology, and how to secure it.

Taking the first steps toward a long-term strategy

How do you start developing a strategy today that will help your organization maximize the value of AI in the future?

1 Understand the technology

The first step in building a long-term AI strategy is to understand the technology enough so that you can use it. You don't have to become an expert in data science or ML. But as a security leader, you should understand how attackers are using AI and how your team can apply AI to anticipate and defend against those attacks.

You should also start thinking about how your organization can aggregate data sets, which you will need to do for AI and ML to work. You'll then need to secure those aggregated data sets.

2 Plan to support business use cases

Today, some organizations are so eager to adopt AI that they are immediately focused on choosing the best ML model. Then they try to find a business problem to solve. But you should identify the business problems you need to address first. It's vitally important to lead with the business problem instead of the technology.

What types of business problems might be good candidates for AI? Many repetitive tasks — such as summarizing meetings or responding to initial customer service requests — are already handled by AI.

In the future, organizations could use AI and ML in situations where the models are learning more from experiences and external inputs. For example, in the banking industry, fraud teams could employ AI to improve the accuracy of fraud detection by learning from actual outcomes. In addition, marketing teams across industries could use AI to streamline content creation: They could input writing preferences and styles, and they could provide feedback that the models would use to improve subsequent results.

As security leaders, we need to start planning for these and other business use cases. We need to find ways to help business teams incorporate AI into their workflows to solve business problems without jeopardizing compliance and security.

Modernizing security

To prepare for the AI future, we need to modernize security — and we need to start that modernization now. Many security teams are still operating the way they have for the past 15 or 20 years. They are reacting to the latest threats and implementing multiple point solutions to address vulnerabilities. But this type of approach led to where we are now: More and more breaches occur every day. We need to be less enamored with the next great point product and more focused on the mission of protecting our customers, workers, and companies.

As security teams lag behind, attackers are moving forward quickly. In the not-too-distant future, we'll see more attempts to bypass AI models used for cyber security by exploiting data that is not factored into those models. We'll also see AI-driven malware that can learn from defensive methods and rapidly modify its attack.

To modernize security, we have to rethink what tools we need, what skills we need, and how we should work. Envisioning where we'll be in 5, 10, or 20 years will help us figure out what we need to do today.
Here are four recommendations on how to get started:

1 Implement the right technologies and tools

Modernizing security requires advanced tools. Organizations need technology that can automatically anticipate and detect new types of AI-driven threats. Tools with AI capabilities could also help us streamline compliance. We might have tools that could recommend changes in controls or policies whenever new regulations are introduced.

2 Address the skills gap

Because AI will take over some low-level tasks, IT and security teams will need people with more advanced skill sets. IT teams will need people with expertise in data science, ML, and neural networks.

At the same time, IT and business teams will need domain expertise: If you want to use AI to improve medical decision making, for example, you'll need to collaborate with medical professionals. Data science should be the intersection of computer science, math and statistics, and domain knowledge.

Security teams need people who can interpret the results generated by AI models and determine how strategies or policies should change to address evolving threats. One of the most common mistakes I have seen is listening to the output of the model without understanding the meaning. Remember that baseball Hall of Fame example: If we only listen to the output (which found that at-bats are the best predictor of who gets in), young players might assume that they should just focus on having the most at-bats. In fact, they should work on developing their skills so they can have a long and outstanding career.

> "One of the most common mistakes I have seen is listening to the output of the model without understanding the meaning."

3 Modify operations

Security teams also need to change how they operate. Will we still need a 250-person, globally dispersed SOC, operating 24/7 in the future? We might need round-the-clock operations, but we'll likely be able to complete many of those existing human tasks with computers, so we'll be able to focus humans on other tasks.

We could have an autonomous SOC in 5 to 10 years — which means that we should start formulating a plan now for how it will operate. We need that lead time because of the complexity of our security environments. It's difficult enough to secure those environments — incorporating AI will be challenging.

If we're able to save some time with an autonomous SOC, we'll also need to invest more time on maintaining data integrity and sustaining regulatory compliance. The more we use AI models internally, the more data we'll need to manage and control. We need to know where data is, make sure it is accurate, and ensure we can safeguard confidentiality.

There has been a lot of discussion about AI governance, but the most important factor is data. There are already numerous global laws about how and where we can use and store data. Security teams will have to ensure that their organizations continue to comply with data sovereignty laws as well as data privacy regulations. Compliance might become more difficult if IT teams shift where they are running AI models, for example, moving data from the cloud back to on-premises environments.

4 Begin to consolidate technology partners

It can be difficult to aggregate data and generate the AI-driven insights you need when you use solutions from numerous vendors. Our IT and security environments are complex enough without having to manage all of those distinct solutions. As your organization looks toward the future, you should start to consolidate solutions. Working with four or five key partners is much simpler than trying to manage data from 50.

Looking ahead — and planning in the present

AI is here, but we've only seen the first glimpses of its impact on our work and our lives. As security leaders, we have to start planning now for the changes to come. With the right longer-term strategy, we will be better positioned to support internal use of AI for business objectives, employ AI to bolster security, and defend against AI-driven threats.

> "The more we use AI models internally, the more data we'll need to manage and control."

Balancing privacy and business risk

By Emily Hancock
Chief Privacy Officer,
Cloudflare

Keeping personal data private and company resources safe are two of the primary goals of a corporate cyber security program.

In this article, we'll dive into the risks and costs of failing to invest in security, and how security and privacy leaders can be powerful partners in convincing their organizations why the investment in security is so important. When security and privacy leaders work together, they can find the right security tools to protect an organization from the risks of data breaches and make an informed decision about what solutions are the right choice for the business.

Where does the real harm lie?

Ideally, an organization's security and privacy leaders should be working closely with one another. The best way to ensure the privacy of customer and corporate data is by implementing an effective data security program.

Privacy leaders recognize the value of security measures for protecting customer data. However, in some cases, it can be difficult for a security leader to sell a privacy leader on the benefits of certain security technologies. Without a clear understanding of how a security solution works and what its purpose is, it could appear to be a risk to data privacy. For example, a privacy leader may be quite skeptical when their security leader proposes onboarding an email security tool that scans all of a company's emails to thwart phishing attempts, or using a secure web gateway that might allow a company's IT team to see what websites employees visit on their work computers in the course of trying to block employees from visiting websites that host malware.

When thinking about security investments for a corporate network, it's important to consider — what is the real privacy harm the organization is trying to protect against? A company's privacy leader needs to weigh the privacy harm to a company's employees from a machine that merely scans company emails to say, "Yes, good" or "No, bad" against the harm that could come to the company if such security protections aren't in place. If such protections aren't in place, an employee could easily become the victim of a phishing exploit that results in a threat actor using that employee's credentials to access internal systems and exfiltrate the sensitive personal data of the company's customers.

"A company's privacy leader needs to weigh the privacy harm to a company's employees from a machine that merely scans company emails to say, "Yes, good" or "No, bad" against the harm that could come to the company if such security protections aren't in place."

In my opinion, having a really strong sense of what privacy harms are the biggest risk for your organization is essential to implementing effective privacy-led security. In many cases, the benefits of security investment outweigh the potential costs. In the example above, it's worth noting that employees in most jurisdictions globally have few privacy protections in the emails they send to a company's system. But if the personal data of a company's customers is exfiltrated, a company could face data breach notification obligations, regulatory penalties, and contractual damages.

Calculating the cost of underinvesting in security

Corporate cyber security solutions are designed to address a variety of different threats to an organization. For example, one common threat is the potential for data breaches, which had an average cost of $4.45 million in 2023. However, this number overlooks the reputational damage to the companies that suffer the breaches and the impact on the customers whose data has been breached.

While we can't know the number of data breaches an unprotected organization might suffer in a given year, we can estimate it. For example, 85% of companies suffered at least one ransomware attack in the past year, and 24% of data breaches are caused by ransomware. That means there's a good chance that a company will experience both a ransomware attack and non-ransomware data breaches within a year.

While this is only a rough estimate, it demonstrates that the potential annual cost to an under-protected company is likely in the tens of millions, if not more. Additionally, the potential impacts of cyber security incidents on an organization's customers are incalculable. Diving into the details of major data breaches, you'll quickly find that most were made possible by a number of fundamental security issues. Weak passwords, expired certificates, and other failures of basic security hygiene are often the root cause of major security incidents. Cyber security solutions that help to mitigate these risks and protect against the most common types of security breaches — such as anti-malware, email scanning, and Zero Trust access control — offer substantial potential benefits to the company and its customers.

Investing in layered security systems reduces risk

In many cases, the benefits of a new security solution are clear: It provides a certain reduction in the risk of a cyber attack. Preventing even a single cyber attack can provide significant cost savings for the organization. By the numbers, if the annual cost of a cyber security solution is less than the anticipated savings, then it's a worthwhile investment.

But, it's important to invest with the right security vendor. Any time a vendor has access to a company's systems and data, that company must assess whether the vendor's security measures are sufficient. There are several examples where security vendors have been victims of cyber security attacks and, as a result, their customers' systems and data could be exposed to risk.

> "Any time a vendor has access to a company's systems and data, that company must assess whether the vendor's security measures are sufficient."

The Okta breaches are a prime example of the potential impacts that a breach of a security vendor could have on its customers. Many organizations use Okta as an identity provider to implement single sign-on (SSO). With access to Okta's environment, an attacker could potentially gain access to the user accounts of Okta customers. If those customers don't have additional layers of access protection, they could be left vulnerable to hackers who might steal data, plant malware, or take other malicious actions.

When evaluating the privacy risks of security investments, it's important to consider an organization's security track record and certification history. For example, in 2020, only 43.4% of companies had full PCI-DSS compliance at a mid-year assessment, indicating that security controls were allowed to slip between audits.

On the other hand, companies that actively pursue optional certifications such as ISO 27001 and 27018, SOC 2, and others are less likely to have these security gaps that place them and their customers at risk. Cloudflare maintains compliance with required and optional certifications and has pursued independent audits of its 1.1.1.1 DNS resolver service, where no applicable certification exists. Cloudflare also leverages security technologies such as end-to-end encryption, data localization, and Zero Trust access management to maximize user privacy and comply with the unique requirements of regional data privacy laws and regulations.

Weighing the risks and benefits

While the ROI of security investment can be difficult to calculate, the risks and benefits are clear. Weak cyber security practices mean a company will almost certainly experience a data breach sooner rather than later, and then the only question is the order of magnitude of dollars lost, reputational damage, and downstream harms to the individuals who trusted the company with their personal data.

Investing in security is almost always a good idea from a data privacy and risk management perspective. Minimizing the privacy risks of security investment amplifies its potential privacy benefits. Security and privacy leaders not only have the evidence of costly personal data breaches and security breaches on their side, but, when advocating for additional security investments, they can also shift this balance further in their favor by looking for solutions with good security, privacy, and compliance track records.

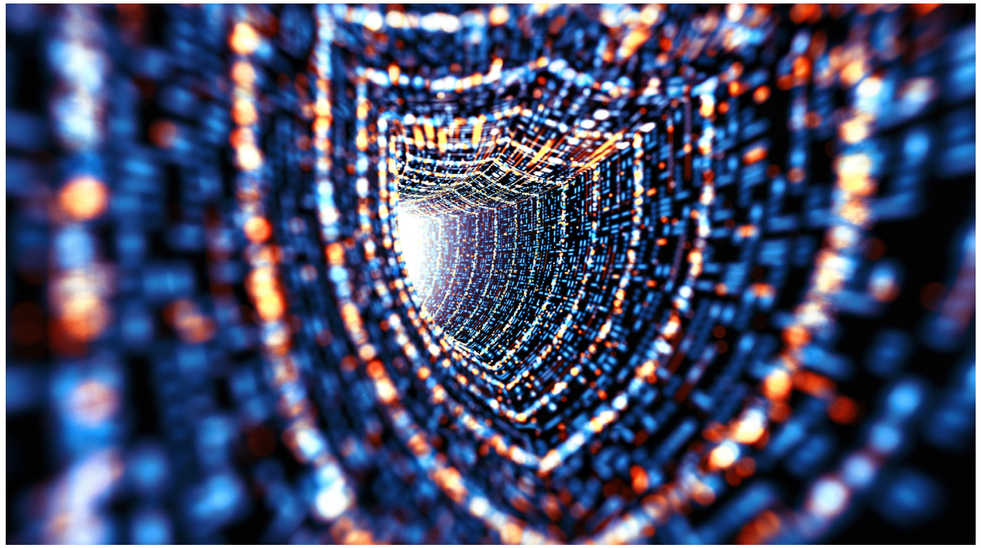
State of application security

Three surprising web app and API threat trends

Web applications are rarely built with security in mind. Yet, we use them daily for all sorts of critical functions, making them a rich target for hackers.

Given the critical nature of web applications and APIs and the data they hold, exploited or unprotected apps can lead to business disruptions, financial losses, and critical infrastructure collapses.

Insights from Cloudflare's State of Application Security report show organizations struggle with outdated security approaches for web apps and APIs, while online threat actors are operating more efficiently and quickly than ever. The research was based on aggregated traffic patterns (observed April 2023 – March 2024) from the Cloudflare global network, which identifies and blocks 158 billion cyber threats each day. This article highlights three key trends from the report that require urgent attention and action from CISOs.



Trend one

Organizations overwhelmingly use outdated API security

Consumers and end users expect dynamic web and mobile experiences — which are increasingly enhanced and powered by APIs. For businesses, APIs fuel competitive advantages — greater business intelligence, swift cloud deployments, integration of new AI capabilities, and more.

Yet, for many, API security has fallen behind the fast pace of API deployment. Cloudflare uses machine learning models to identify API traffic that may otherwise be unaccounted for. In the application security report, organizations had 33% more public-facing API endpoints than they knew about. (This number was calculated by comparing the number of API endpoints detected through machine learning-based discovery vs. customer-provided session identifiers.)

Despite the fact that APIs present different security challenges compared to web apps, we found that 66.6% of API traffic defended by some form of layer 7 security is primarily protected with traditional negative security WAF rules rather than with specialized API rules employing a positive security model. Negative security models work by blocking bad traffic and allowing everything else, while positive security models specify what traffic is explicitly allowed while denying everything else.

Recommendation

As businesses expose more services via APIs, they should augment web app security tools (like WAFs and DDoS) with purpose-built API security and management enhanced by unsupervised machine learning.

Rather than rely on negative security model rules to protect APIs, industry best practices encourage protecting APIs with a positive security model. A positive security model for API security allows organizations to protect APIs by only accepting traffic that conforms to set OpenAPI schemas, while blocking malformed requests and HTTP anomalies that could contain attacks.

Continue to enhance your API security by discovering shadow APIs. A robust API security tool should constantly scan for every public API in your landscape, even those that are unmanaged or unsecured.

Furthermore, as more organizations race to incorporate generative AI-based APIs, they should consider partnering with a cloud security provider to proactively and continuously monitor the development and deployment of third parties. This can reduce the risk of cyber attacks, and increase data governance and protection.

Trend two

Third-party code has caused an increase in supply chain risk

Most organizations' web apps rely on separate pieces of code from third-party providers (often JavaScript). The use of third-party scripts accelerates modern web app development and allows organizations to ship features to market faster, without having to build all new app features in-house.

The latest research shows how the average Cloudflare customer website contains 47 third-party scripts, 50 connections to JavaScript functions and their destination, and serves 12 cookies.

Third-party code, as well as cookies, represent security risks to your web visitors due to the fact that this code is often loaded in the user's browser, and cookies can be tampered with to take over a session or account, for example. Attackers can gain access to modify the code of JavaScript components used in websites in a variety of ways, such as using stolen account credentials or exploiting zero-day or unpatched vulnerabilities. Then, they use this privileged access to launch a downstream attack on every website using that JavaScript code.

Recommendation

Look for a security vendor that automatically identifies third-party script risks, and provides a full, single dashboard view of all.

Staying ahead of emerging risks

Many organizations have a tapestry of legacy security hardware, cloud-native security, and home-grown security to address all of their application security challenges. But this fragmented approach makes it harder to connect and protect SaaS apps, web apps, and other IT infrastructure. IT sprawl makes it easier for attackers to find and exploit vulnerabilities.

IT and security leaders should shift toward a more proactive approach that addresses application and API security challenges alongside key stakeholders in order to leverage API-specific technical controls, and that way harness the power of GenAI while safeguarding their critical assets and data.

A consolidated platform approach helps ensure better security, latency-free connectivity, and improve business growth by allowing organizations to comply with local regulations when expanding into new markets, and strengthen customer trust.

Trend three

One-third of all Internet traffic stems from bots, but some industries are more impacted than others

On average, bots comprise one-third (31.2%) of all application traffic processed by Cloudflare. This percentage has stayed relatively consistent (hovering at about 30%) over the past three years.

The term bot traffic may carry a negative connotation, but in reality bot traffic is not necessarily good or bad; it all depends on the purpose of the bots. Some are "good" and perform a needed service — such as customer service chatbots and authorized search engine crawlers. But some bots misuse an online product or service and need to be blocked, given the disruptions to revenue that they can potentially cause. In fact, the typical business in the US and UK loses over 4% of their online revenue every year due to malicious bot attacks.

Recommendation

If your industry tends to experience more bot traffic, consider boosting investments in bot management to preemptively stop threats from bad bots.

Look for a bot management service that:

- Accurately identifies bots at scale by applying behavioral analysis, machine learning, and fingerprinting to a diverse and vast volume of data
- Integrates easily with your other web application security and performance services (e.g., WAF, CDN, DDoS)
- Allows good bots, such as those belonging to search engines, to keep reaching your site while preventing malicious traffic

These industries see the highest median daily share of bot traffic:

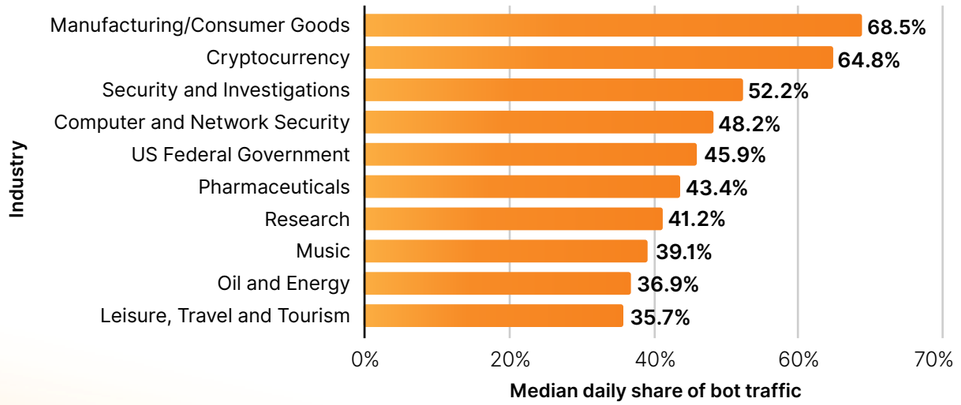


Image source: State of Application Security 2024

Staying ahead of scammers

Fighting phishing through smart cyber security

By Daragh Mahon
EVP and CIO, Werner Enterprises

Transportation ranks among the top 10 industries that suffer data breaches. As you can imagine, that is of extraordinary concern and focus at Werner Enterprises, one of North America's largest transportation and logistics companies. At Werner EDGE — the innovation arm that I lead — our responsibility is to keep goods moving through sophisticated and secure networks, including an approach to cyber security that must extend to protecting our large workforce.

To that end, we must stay vigilant about our approach to phishing — the root cause of most breaches. In fact, the "human element" is still a factor in three out of four breaches, despite enterprises increasing cyber security training. With a single click on a malicious link, an employee could jeopardize an entire company — the FBI says (for example) that business email compromise has cost more than $50 billion to date. Attackers are using increasingly sophisticated methods to infiltrate businesses, and AI is helping them accelerate the speed and scope of their attacks.

In other words: The phishing problem isn't going away. No matter how strong your network architecture and security are, there will always be a weak link, and it's often a single individual. A momentary lapse can spell disaster for the entire organization. Therefore, it's become increasingly clear that we need to collectively adjust our security awareness training to shore up that line of (human) defense.

When it comes to training, the carrot is better than the stick

At the personal level, cyber security is about adopting a few simple habits. Just like learning to look both ways when crossing the street, it needs to become second nature to thoroughly read an email and check email addresses before responding or clicking on a link. At Werner, we typically run seven or eight security training sessions a year, including a mandatory annual training session that lasts 45–60 minutes. It's relatively simple, straightforward, and covers the basics. We also run quarterly refreshers and ad hoc training that is five to seven minutes long to keep everyone up to date, especially when new threats emerge. These are also mandatory.

Year-round security training is a best practice for several reasons:

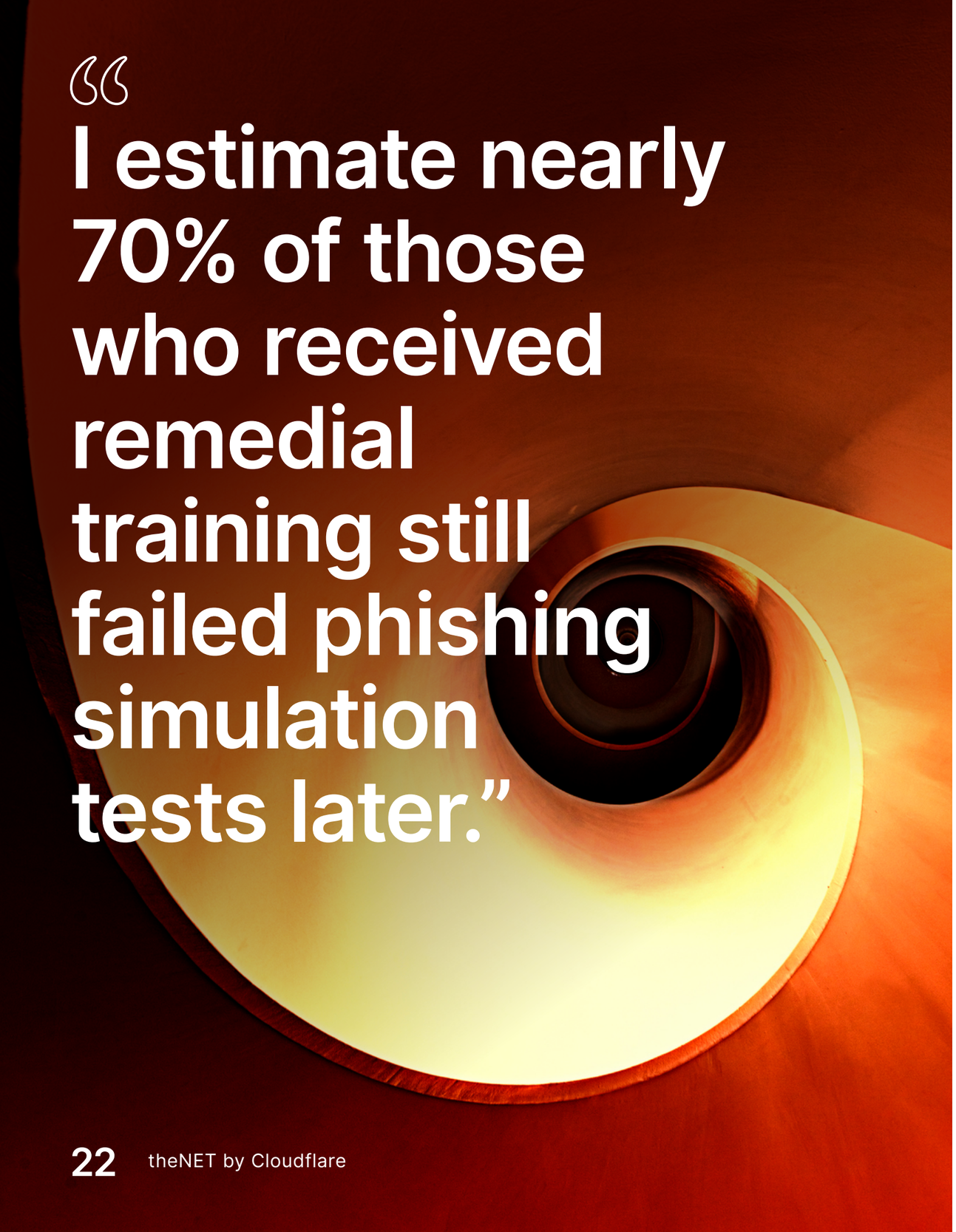
- From a compliance perspective, ongoing training is required by insurers.
- The threat landscape is ever-changing. Attackers are constantly finding new ways to slip past even the most vigilant users, and staff need to know the latest tactics to look out for.
- It's human nature that people tend to lower their guard over time. Training serves as a reminder to take phishing and other threats seriously.

While we've incorporated a lot of best practices into our training practice, we've also identified some things that don't work well.

The least successful strategy was remedial training. When an employee clicks on a known phishing link, we can block outbound communications and identify who responded to the offending content. We then give the person who fell for the scam a quick refresher on what not to do.

But, we've noticed that within a matter of weeks, the same person would fall for another phishing attempt. I estimate nearly 70% of those who received remedial training still failed phishing simulation tests later.

Talking to the repeat offenders gave me a new perspective: Some people felt they were being punished with the extra training; for others, the training made them more nervous about doing the basic tasks required for their jobs, such as reading emails or even opening Word documents.



While ongoing awareness training is a critical way to stay ahead of the scammers, I’ve also come to the conclusion that punitive measures aren’t as successful. Anyone in charge of cyber security needs to find engaging ways to incentivize employees to pay attention to their actions — while respecting their time.

You need a carrot, not a stick, to get the best response.

Gamifying security training is one way to create positive reinforcement and reward people for good behavior, like reporting suspicious communications. For example, incentives like leaderboards, cash rewards, gift cards, or company swag, can offer tangible reasons for busy colleagues to want to do better on training and to know more about evolving phishing threats.

Constant vigilance through multifaceted security measures

Improving training is only one side of the coin. Someone will let their guard down eventually and organizations have to be ready to continually strengthen their cyber security posture.

Human error and inattention are two of the biggest threats to a company’s security. It’s impossible to eliminate these threats entirely, but technology can be leveraged as a safety net to minimize what gets through.

Starting with a Zero Trust approach, companies can also leverage preventive tools like multi-factor identification (MFA) and preemptive email security (which might include optical character recognition to scan images) to relieve the burden on IT and security teams.

It’s also important to have endpoint security tools to automate the isolation and removal of a compromised device from your network. Just as scammers leverage AI for their attacks, the business community must respond by applying AI to identify and respond to security breaches much faster. Any business that can harness these technologies improves its odds of preventing a breach.

Cyber security is very much about covering all the bases. Werner runs penetration tests at regular intervals, including a red team test, where we hire ethical hackers to try to attempt an attack on the network from the outside. This practice helps locate vulnerabilities.

Our red teams also test physical security. They walk around parking lots and check for unlocked cars with laptops, backpacks, or documents in the back seat. They get into buildings by following people who swipe magnetic cards or scan badges to enter. They check for unlocked and unattended laptops and smartphones and see if it’s possible to steal files from those devices. Sharing the results of these tests can be a great wake-up call for employees who might feel far removed from cyber security concerns.

Every IT leader recognizes the financial, operational, and reputational costs of a breach, and knows that they can’t skimp on security technology. The challenge is making sure everyone else in the organization is equally vigilant against threats.

Fighting phishing with every solution available

I’m all about action, urgency, and keeping things simple. Businesses have to keep pace with IT innovation to stay competitive, but we can’t move so fast that we forget to attend to the security basics. Optimizing every aspect of operations, systems, and infrastructure will not only reduce human error, but it will reduce capital and operational expenses, making it possible to allocate more funds and resources to cyber security — which should be as robust as your budget will allow.

Phishing costs businesses millions of dollars and can disrupt production, interrupt services, alienate customers, and drive companies out of business. If an organization tries to ‘save money’ on cyber security, or reduce employee training, they put everything at risk. Instead, make security integral to your operations and culture, giving your people and business a fighting chance when attackers attack. The health and safety of our companies demand it.

Conclusion

Modernizing security for the evolving business environment

In various ways, the perspectives and trends in this guide all reveal the importance of choosing the right underlying architecture to simplify security in an increasingly complex world.

To defend against new threats, organizations need the ability to connect and protect their people, apps, and networks across any endpoint or infrastructure, anywhere.

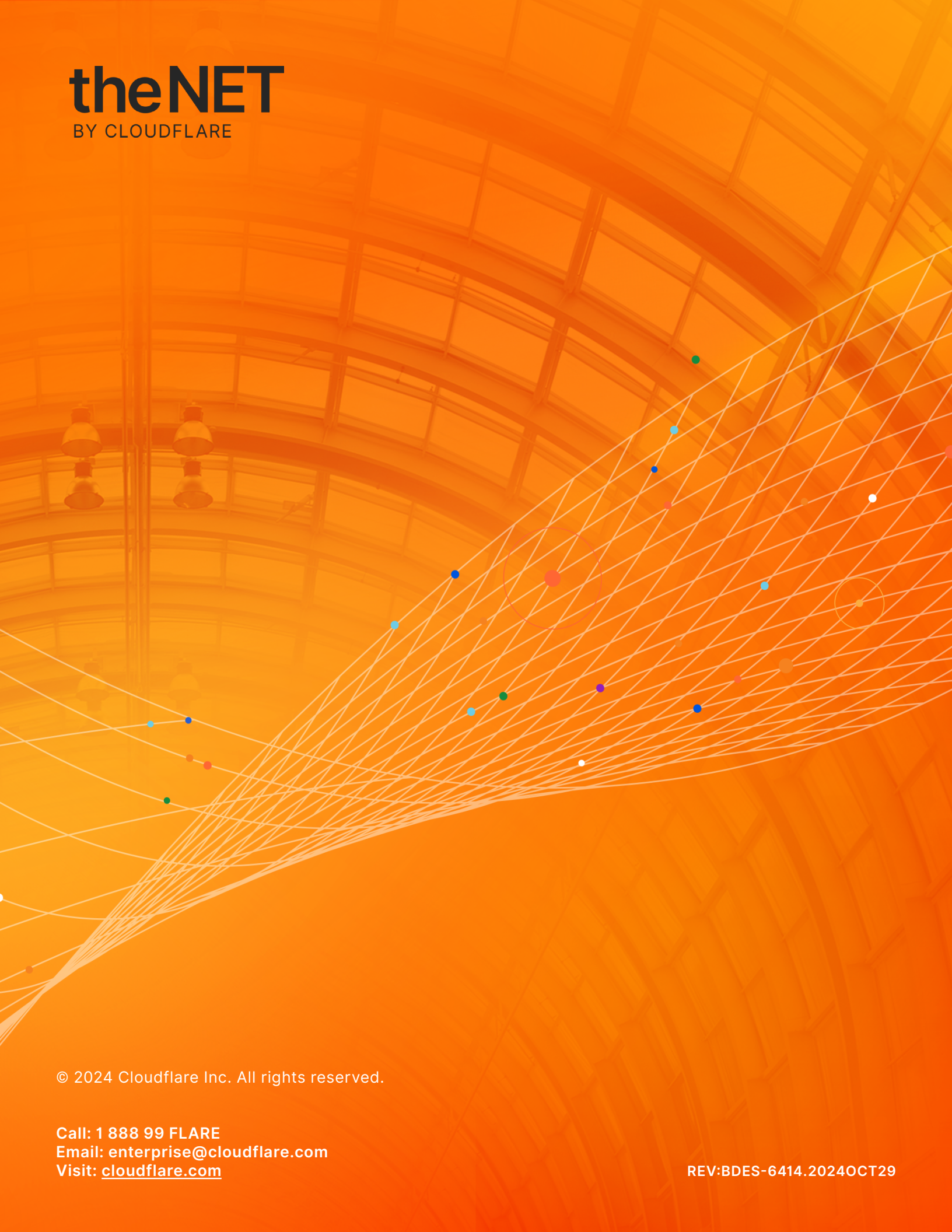
Cloudflare's connectivity cloud delivers this "everywhere" security approach through a single, composable platform that helps security leaders accelerate their strategic priorities.

These results are made possible via Cloudflare's:

- **Unified & composable platform** — Converge web app and API protection (WAAP), security services edge (SSE), email security, and more security domains on one platform and control plane.
- **See more, protect more** — Security efficacy starts with having the best data. Cloudflare's network gathers millions of data points from the following sources (and others) to continuously enhance AI/ML-powered threat intelligence models:
  - **~20%** of all websites
  - Telemetry from **millions of customers** in over 120 countries providing **over 8 billion** preemptive attack signals per day
  - Analysis of **3.4 trillion** DNS requests per day
- **A network built to scale** — Cloudflare's global network spanning more than **330 locations** (including **165+ AI inference locations**), with **296 Tbps of capacity**, is purpose-built for performance and scale. Every security service is available for customers to run in every location, such that policy enforcement is always fast, consistent, and resilient.

Want to learn more about securing people, apps, and networks everywhere? **Visit** cloudflare.com/cybersecurity.

For more perspectives on the latest trends and topics impacting today's technology decision-makers, **visit** theNET.



Call: 1 888 99 FLARE
Email: enterprise@cloudflare.com
Visit: cloudflare.com

REV:BDES-6414.2024OCT29