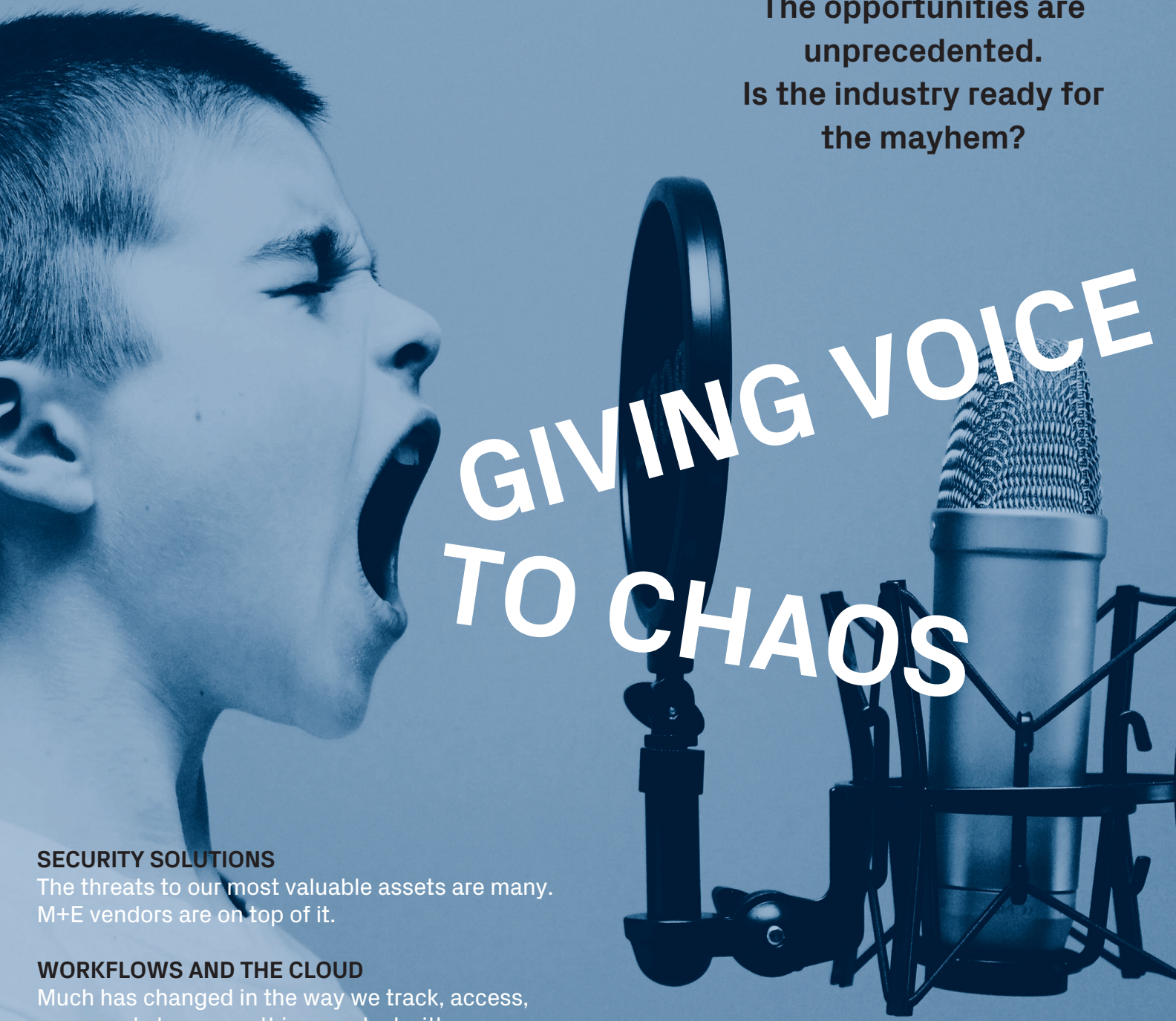
M+E JOURNAL

Today's localization challenges are enormous. The opportunities are unprecedented. Is the industry ready for the mayhem?



GIVING VOICE TO CHAOS

SECURITY SOLUTIONS
The threats to our most valuable assets are many. M+E vendors are on top of it.

WORKFLOWS AND THE CLOUD
Much has changed in the way we track, access, move and store everything we deal with.

SMART CONTENT
The many ways the industry adopts new technologies to make content smarter.

22.02

TWO KEY TRENDS THAT WILL SHAPE THE FUTURE OF YOUR SECURITY TEAM

Transition to a risk-based approach for security and focus on general scalability

ABSTRACT: The world changed when the pandemic hit in 2020, leaving organizations unsure of how it would affect the future. Security leaders may have found themselves wondering if their long-standing business approaches, processes, and tools could withstand the changes brought on by the pandemic. Fast forward, and the answer to those thoughts is both yes and no. Yes — because they have helped organizations stay afloat as they navigated change. No — because the world continues to evolve, and we need to keep up.

By Mike Johnson, Chief Information Security Officer, Fastly

According to Verizon's 2022 Data Breach Investigations Report, compromised web applications were the primary attack vector of 2021, accounting for roughly 70 percent of security incidents. This is a huge jump from 39 percent in 2020. Attacks on web applications can be attributed to the use of stolen credentials, exploit vulnerability, brute force, backdoor or C2, explore data and much more — however, the use of stolen credentials accounts for more than 80 percent of these attacks. As Rapid7 author Jesse Mack summarizes in a recent article, this large percentage emphasizes "the importance of user awareness and strong authentication protocols at the endpoint level."

This rise we are seeing in web application attacks is without a doubt directly correlated to the challenges we have been facing in our industry. While we can all agree this has brought uncertainty and a need to adapt, it has also brought unexpected opportunities for security leaders to pause and reflect on how our organizations were affected, and identify what changes are needed to be successful in the future.

After many conversations with fellow industry leaders and our own security team here at Fastly, I've found that there are two key trends we

all need to keep an eye on: transitioning to a risk-based approach for security and focusing on general scalability. In this article, I'll share my thoughts on how these two will shape the future of security in the next year.

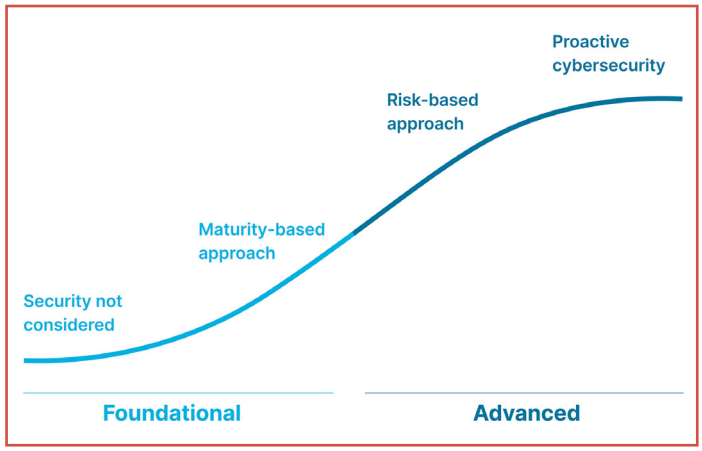
THE CYBERSECURITY JOURNEY

A common question among my CISO peers in our secret squirrel communities is how we measure our security programs and report that out. Many of us will respond and say we use the NIST Cybersecurity Framework (CSF) and examine each function and assign a maturity score (using a simple 0-5 interpretation derived from the Capability Maturity Model (CMM). This is an improvement beyond the way we used to answer the question with a "huh?" Moving from the old non-way of measuring our programs to using CSF was a positive step within an overall journey of how we think about our cybersecurity programs.

This first stage of the journey meant that security wasn't being considered. There was a lack of awareness and capability within the organization. From there, most organizations move on to what came before the risk-based approach: the maturity-based approach I mentioned. The good old maturity-based approach focuses on achieving a specific level of maturity by gradually building capabilities. We must acknowledge that the maturity-based approach is still being used and is considered the norm for some organizations. Looking forward, however, this will not be adequate, as it means security leaders are wearing blinders and focusing solely on meeting that targeted maturity score.

According to a 2019 McKinsey & Company report, "The most sophisticated institutions are moving from a maturity-based to a risk-based approach for managing cyber risk." While the maturity-based approach can work for organizations that need to build everything from the ground up, it will run into some key issues:

- ***Unmanageable growth of control and oversight. Organizations that grow organically will start to see their analysts become outnumbered by the volume of applications, resulting in unchecked monitoring.***



The approach to cybersecurity has evolved.

- ***Inefficient spending. Organizations attempting to track everything will lack the information needed to determine where spend should be properly allocated.***

- ***Demand overload for implementation. When team members are overloaded, their attention is spread across too many efforts, which leads to projects never being fully implemented.***

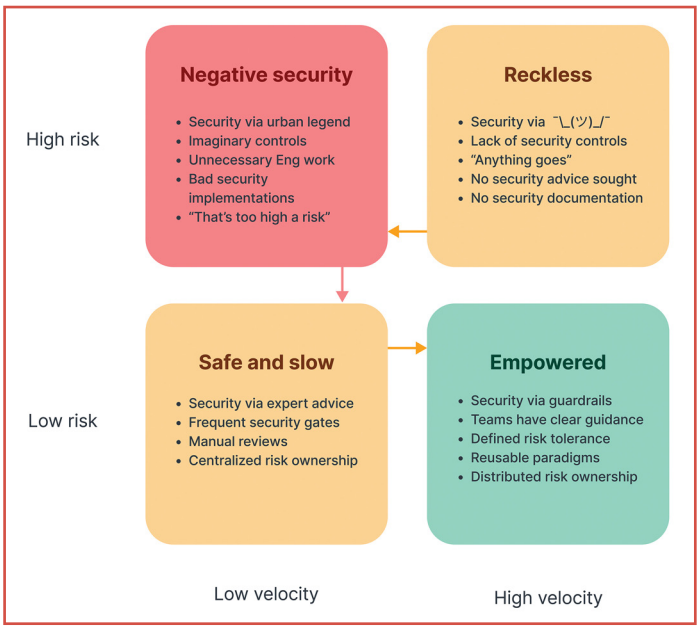
Therefore, we believe the next best step in the journey is to adopt the risk-based approach, which is a much more strategic approach and is vital to managing risk effectively and efficiently. This risk-based approach sets us up to naturally weave security resilience into our decision making, but we can't do that if we're not already baking risk into our thinking.

TREND NO. 1: LEANING INTO RISKS

In the world of security, we're all familiar with and constantly talk about risk. But what we're now starting to see are security teams using risk to make decisions.

What exactly is a risk? The Cambridge Dictionary defines risk as "the possibility of something bad happening." As a security leader this definition pushes me to rethink all the shapes and forms risk could present itself in our industry. The OWASP Top Ten list of security risks immediately comes to mind, as it brings awareness to the most critical web application risks. In 2021, we

Mike Johnson *serves as the chief information security officer of Fastly, where he leads teams focused on the security of Fastly's network, products, services, and systems trusted by the world's leading companies. Prior to joining Fastly, Johnson served as the CISO of Lyft, and led detection and response at Salesforce. info@fastly.com @fastly*



Don't be reckless with your security posturing.

see everything from Broken Access Control rising to the top and Server-Side Request Forgery being added to the list for the first time. While risks will always be changing, we can be prepared to manage them better.

But why are security teams leaning into risks? It boils down to the maturation of the security profession itself. While security professionals have already been transitioning from an old school "department of no" mentality to a "yes, but" approach, there's more to it. As security leaders and teams, we regularly need to justify budget and why certain controls are required. This has led us to double down on the risk-based approach for security.

A risk-based approach helps solve two challenges that security teams face: prioritization and explanation. When looking through a risk-based lens, priorities quickly shake out and teams can decide what the most important work is. Our teams also need to be able to explain to our peer teams why a particular approach creates an increased probability of something bad happening. The OWASP Top Ten provides precise examples of where those bad things are happening and using those examples in discussions with peer teams helps reorient. For instance, Server-Side Request Forgery was not something many teams thought about a few years ago, but product security teams are certainly guiding engineering teams on weaknesses to watch out for.

Using risk for prioritization has become crucial to being efficient and successful within our team. When we have 30-plus different security issues to solve, risk will help us prioritize and understand which issue to solve first. This is true for not only security teams, but also for the various other teams that we work with, such as engineering. We all need and can leverage security risk to help justify what needs to be worked on. While the risk-based approach to cybersecurity can be complex, there are many emerging best practices for successfully attaining it.

TREND NO. 2: UNDERSTANDING THE POWER OF SCALABILITY

The second trend that I believe is emerging and affecting the future of security is around general scalability. When I ponder scalability in this context, I'm thinking about how a team's capacity grows to keep up with the needs of a growing company. Currently, there is a challenge around scalability and how security leaders will scale security (and non-security) functions and capabilities within companies. When it comes to scalability, security teams are faced with issues including:

- ***Finding and retaining talent***
- ***Hiring just to perform manual processes***
- ***Keeping up with demand***

Achieving general scalability within a security organization helps us achieve two goals: outwardly to support the velocity of the company and inwardly to scale the functions of the security team. Let's dive deeper into each of these goals.

LOOKING OUTWARD

To support the velocity of the company and maintain a decent risk profile, security teams' bandwidth must scale appropriately. Teams made up of subject matter experts are needed to maintain velocity but staffing up simply to turn the crank of manual toil will lead to an unsustainable team.

A scalability trick is to have your team focus on developing repeatable guidance that other teams can easily follow. With this guidance in hand, you now have other teams building securely from the beginning, allowing them to maintain velocity while reducing the likelihood of security issues or breaches. Empowering teams this way allows them to maintain team velocity, while companies maintain their security posture and the velocity of the company accelerates.

AND LOOKING INWARD

We've discussed what attaining general scalability looks like when looking outward at the company, but

how does it look when you look inward? This brings us to focus on looking at ourselves and figuring out how we make our security teams more productive. To achieve this, we as security leaders must create meaningful work — which also reduces toil. As we continue to grow, we will be better able to support our efforts. With scalability as a first-class concern, we can prevent team burnout by ensuring our teams:

- ***Actually, and realistically keep up with all of their work***
- ***Aren't working extremely long hours***
- ***Recognize how their work contributes to the overall goals of the company***

VELOCITY VS. RISK

As we continue to look to the future of security, it is important to know that it is possible for teams to move both faster and safer. How is this achieved? - by understanding the interactions of velocity and risk.

At Fastly, we empower our company and all its internal functions by aiming for high velocity and low risk. With this goal, we enable teams by providing clear guardrails to work within (through clear guidance, as I mentioned earlier, as well as with reusable concepts to make things easier) and make sure that teams understand their responsibilities of risk ownership.

At a high level, we strive to practice our data governance and risk ownership with the following, and we encourage you to refer to this when assessing your own practices within your company and security teams:

- ***Data governance. A data governance program is key in assessing risk as it allows for informed decisions around risk tolerance***

- ***Risk ownership. Clear security risk ownership along with defined tolerance levels enables distributed, educated decision making***

HOW TO START FUTUREPROOFING TODAY

Preparing for the future can sometimes cause feelings of uncertainty and doubt. However, by understanding the tradeoffs between risk and velocity, you can redirect that into feeling empowered to shape your security teams for what's to come.

I hope that by sharing my thoughts and journey as an industry veteran and Fastly's CISO, I've been able to provide resources that will help you and your security teams as you continue to move along your cybersecurity journey.

Teams that evolve with a risk-based security approach and general scalability will be the leaders and faces of security in 2022, 2023 and beyond. Paired with the existing solutions today, your security teams will be armed with everything they need to provide safety and prevent attacks. ⊞

fastly

Secure your web apps and APIs, wherever they live

Traditional web application firewalls (WAF) rely on regular expression pattern-matching rules. They're difficult to manage and require never-ending rules tuning to eliminate false positives that can block legitimate traffic. The Fastly Next-Gen WAF leverages a fundamentally different approach, developed by Signal Sciences, that effectively detects and blocks malicious traffic without rules tuning, leaving your AppSec teams to focus on bigger problems. To learn more, **visit fastly.com/secure**

90%+
customers in full blocking mode

90k+
app deployments protected

100+
Cloud-native and datacenter platforms supported

4
Consecutive years as a Gartner Peer Insights Customer' Choice