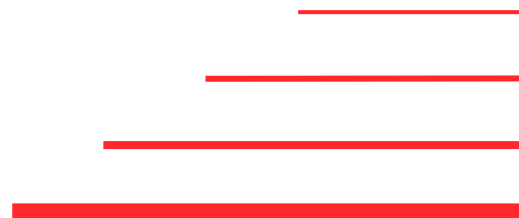**fastly**

Cybersecurity at the Crossroads

Navigating Risk, Resilience, and the Road Ahead

28 May 2025

Sarah Lim
Senior Solutions Engineer

Hi, I'm Sarah!

- Based in Singapore

- 25 years in IT, 10 years in Cyber Security & CDN across South East Asia

- The opinions in this presentation are my own

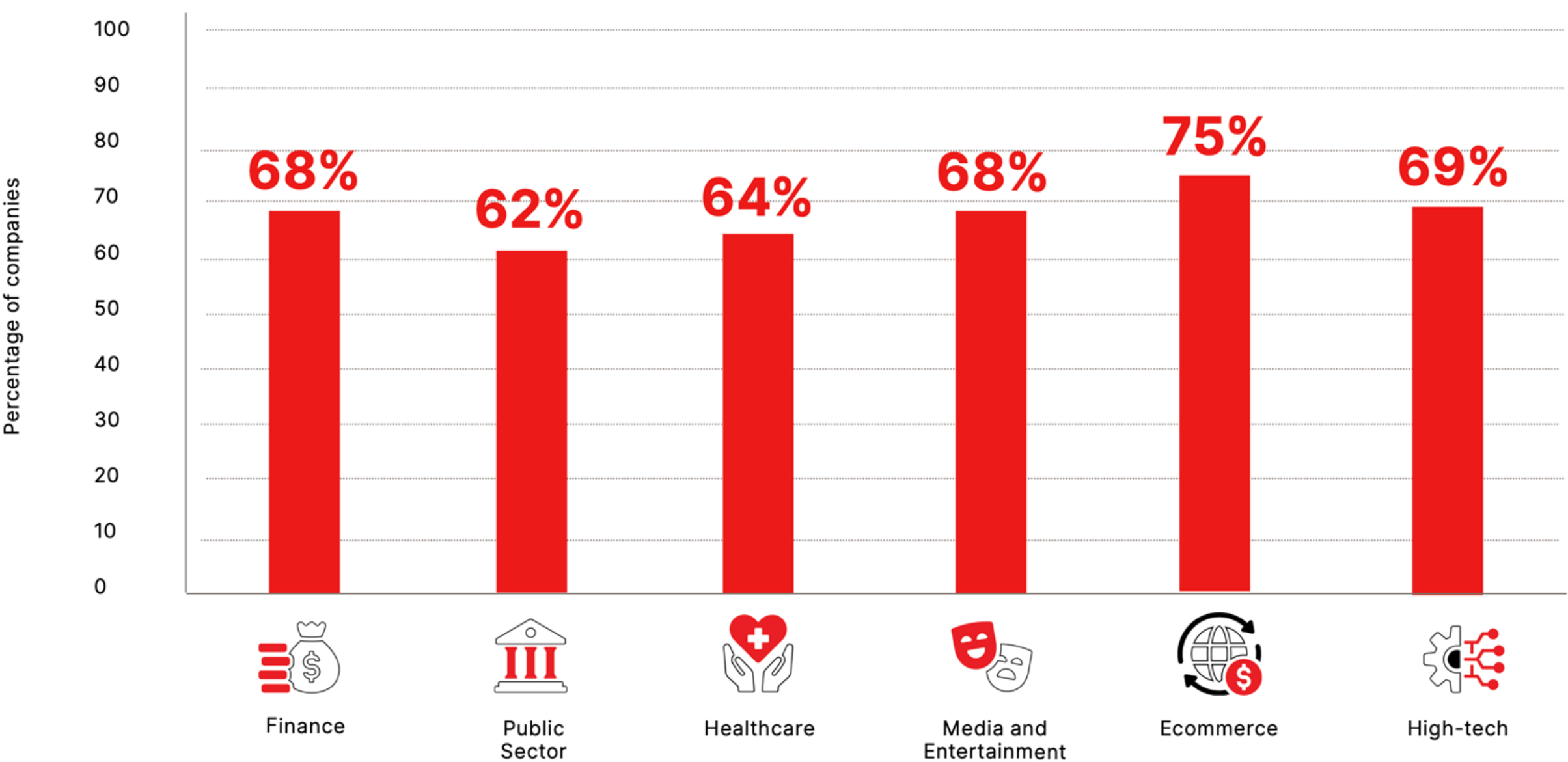**Come have a free coffee and chat with us at our Fastly booth!**

fastly

Sarah Lim
Senior Solutions Engineer

Who had security incidents in the last 12 months?

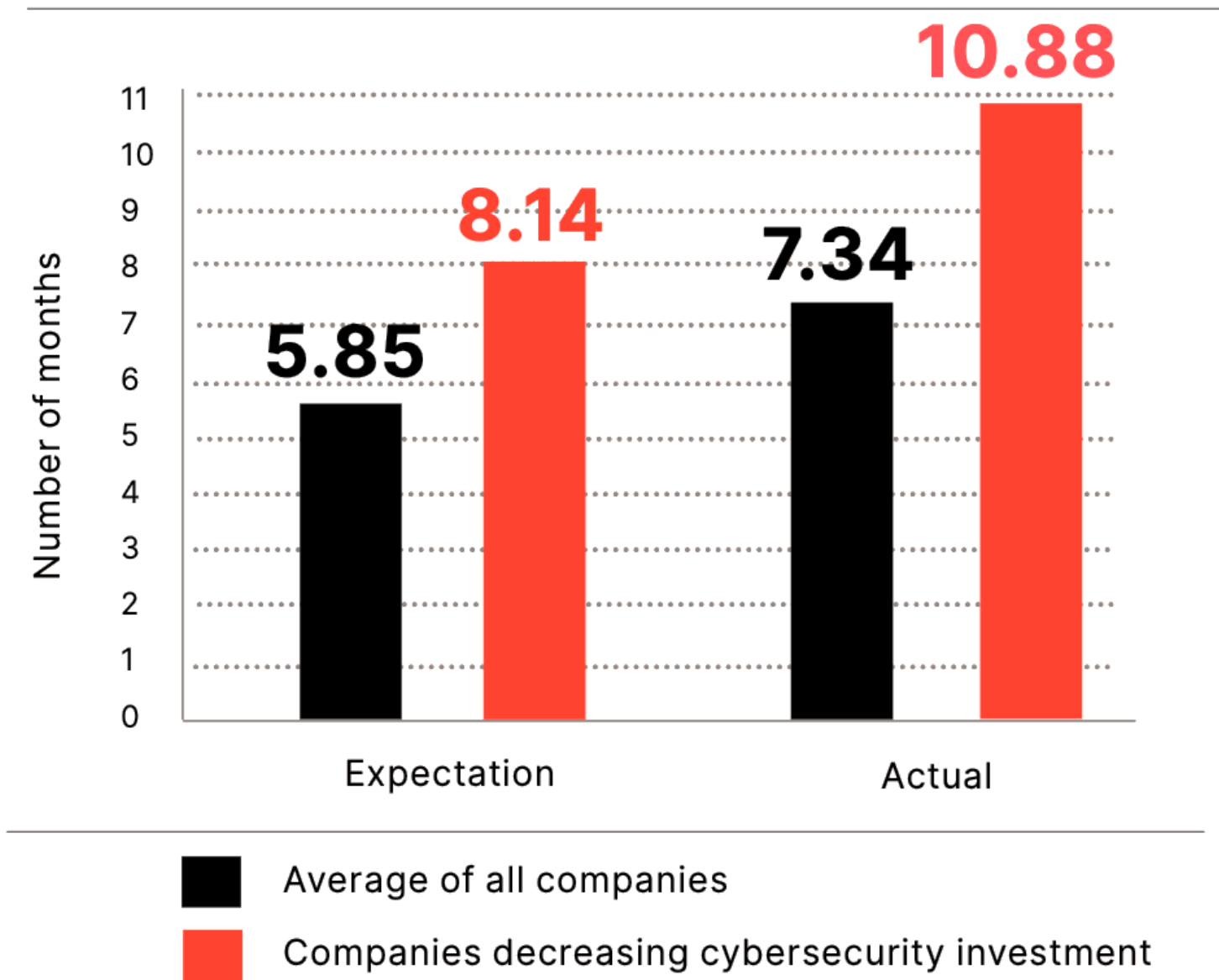**Percentage of companies that had a security incident in the last 12 months**

Percentage of companies

Finance	Public Sector	Healthcare	Media and Entertainment	Ecommerce	High-tech
68%	62%	64%	68%	75%	69%

Most common attacks

1	**29%**	Ransomware
2	**28%**	DDoS
3	**25%**	Exploitation of vulnerabilities in open source software
4	**22%**	Social engineering
5	**20%**	API/web application-related attacks

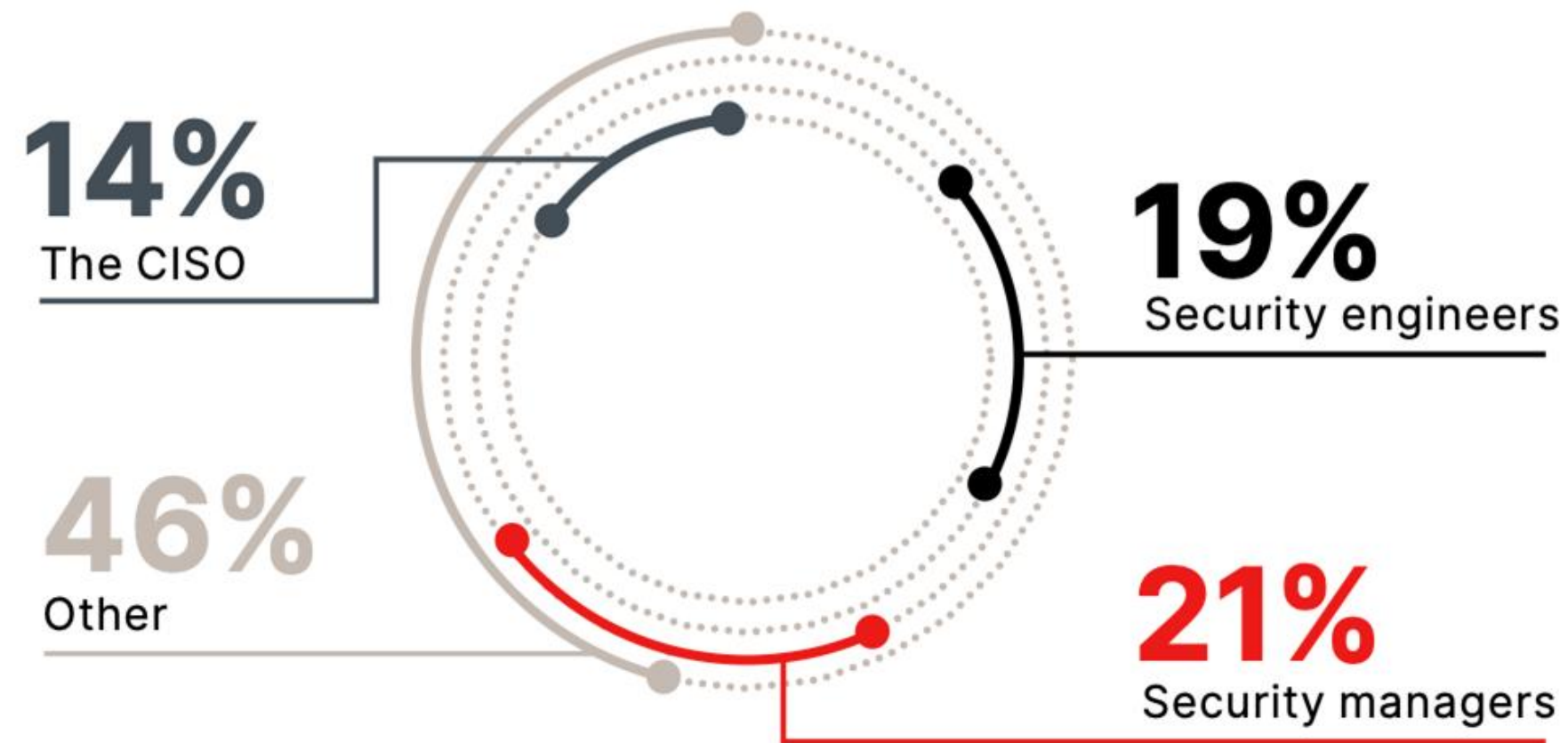# What is the impact and how long does it take to recover?

Recovery time after cybersecurity incidents

Number of months

5.85 — Expectation (Average of all companies)
8.14 — Expectation (Companies decreasing cybersecurity investment)
7.34 — Actual (Average of all companies)
10.88 — Actual (Companies decreasing cybersecurity investment)

■ Average of all companies
■ Companies decreasing cybersecurity investment

Cyber Incident Impact

Impact	Value
Customer Churn	14
Regulatory Fines	17
Trust Loss	18
Legal action	19
Customer satisfaction drop	19
Reputation damage	22
Revenue Loss	23

Who is responsible for cybersecurity incidents?

14% The CISO

19% Security engineers

46% Other
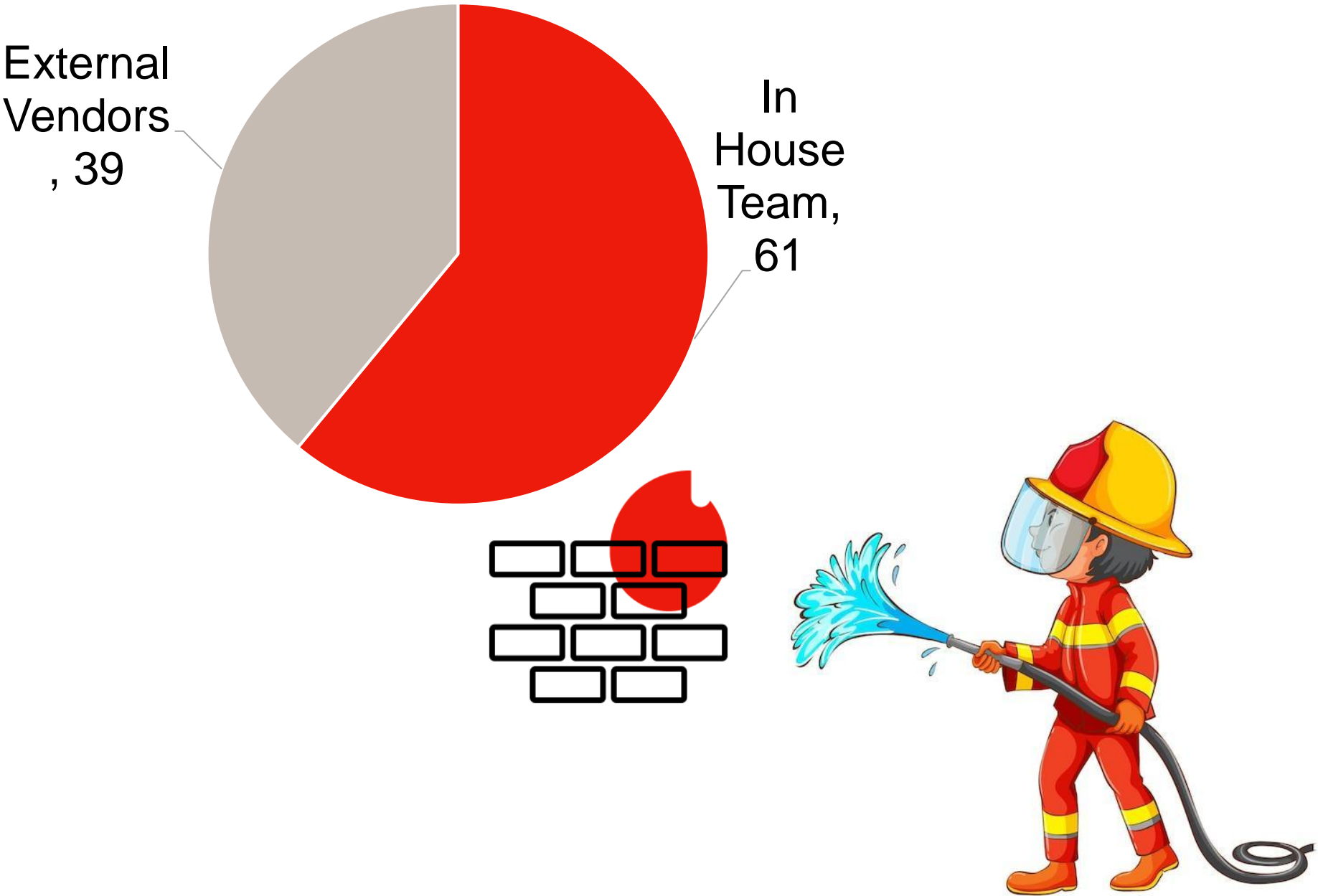
21% Security managers

"You can delegate authority, but you cannot delegate responsibility."
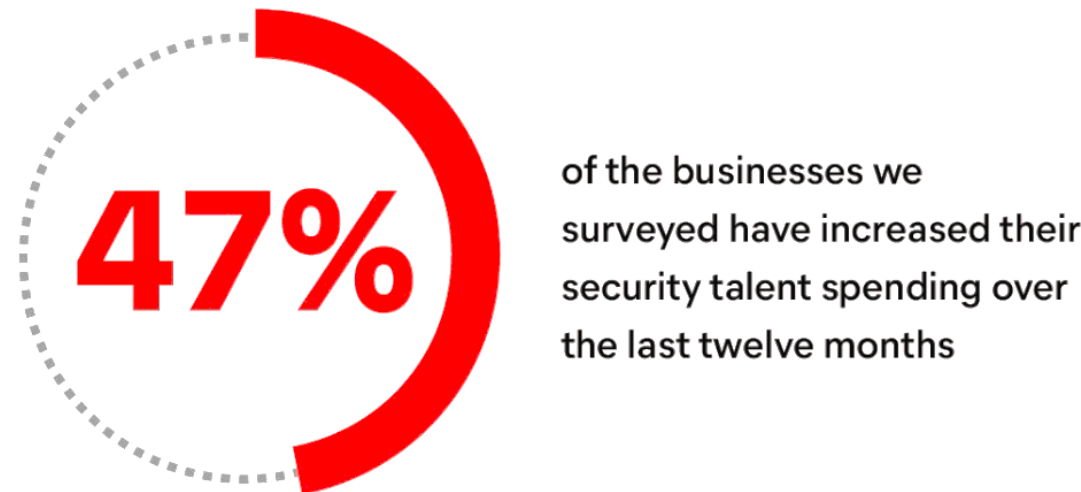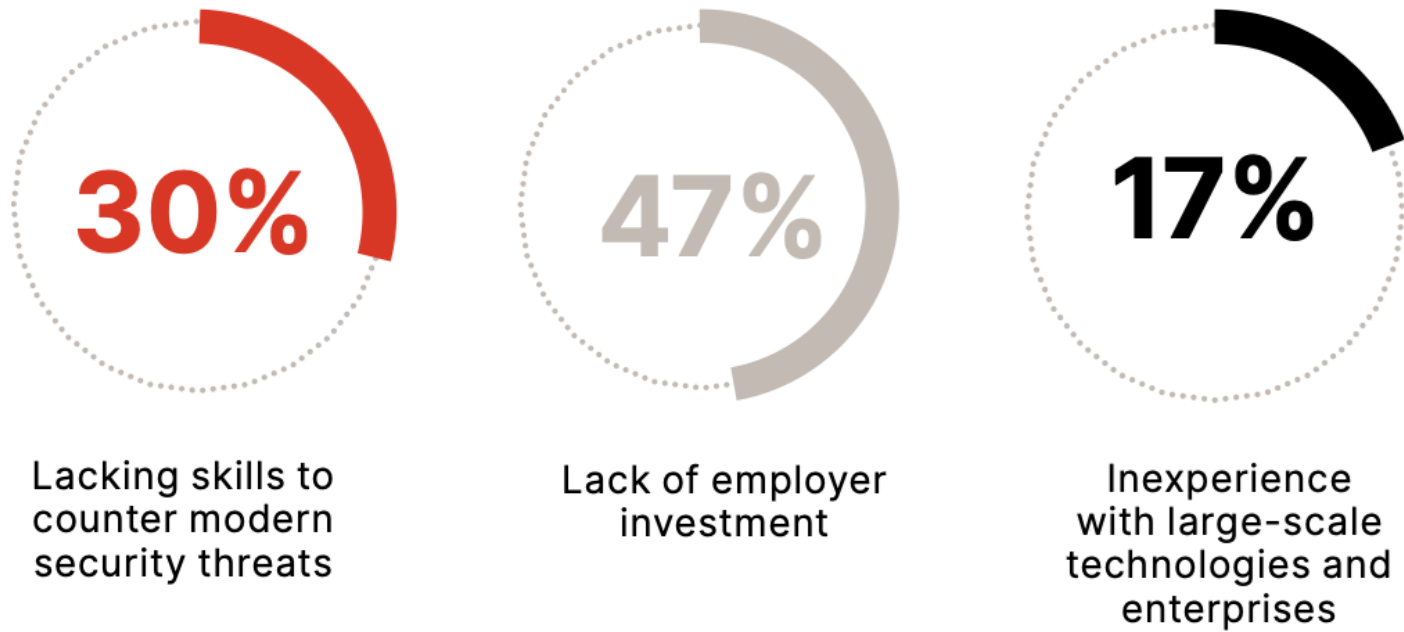*– Former U.S. Senator Byron Dorgan.*

Who is responsible for Security?

The talent crunch

Who is actually resolving cybersecurity incidents?

External Vendors, 39

In House Team, 61

30%
Lacking skills to counter modern security threats

47%
Lack of employer investment

17%
Inexperience with large-scale technologies and enterprises

36% of businesses continuing to place high-quality recruitment at the top of their investment wishlist for the coming year

47% of the businesses we surveyed have increased their security talent spending over the last twelve months

What are the areas of concern?

36%
Sophisticated threats

33%
Securing Remote Workers

36%
Lack of talent with relevant skills

26%
Damaging result of inadequate investment

35%
Generative AI

Security spending in the next 24 months

2023

1	**51%**	Generative AI security	⭐	NEW ENTRY
2	**48%**	Bot mitigation	⬇	DOWN ONE
3	**46%**	Digitisation of critical infrastructure	⬇	DOWN ONE
4	**46%**	WAF	⬆	UP TWO
5	**45%**	5G Security	⬇	DOWN FOUR
6	**45%**	Defense against nation state attacks	⬇	DOWN ONE
7	**42%**	Remote employee security	⬆	UP FIVE
8	**42%**	API Security	⬆	UP FIVE
9	**42%**	DDoS controls	⬇	DOWN SIX
10	**40%**	Managed Security Services	▬	NO CHANGE

35% feel they overspent in the last 12 months
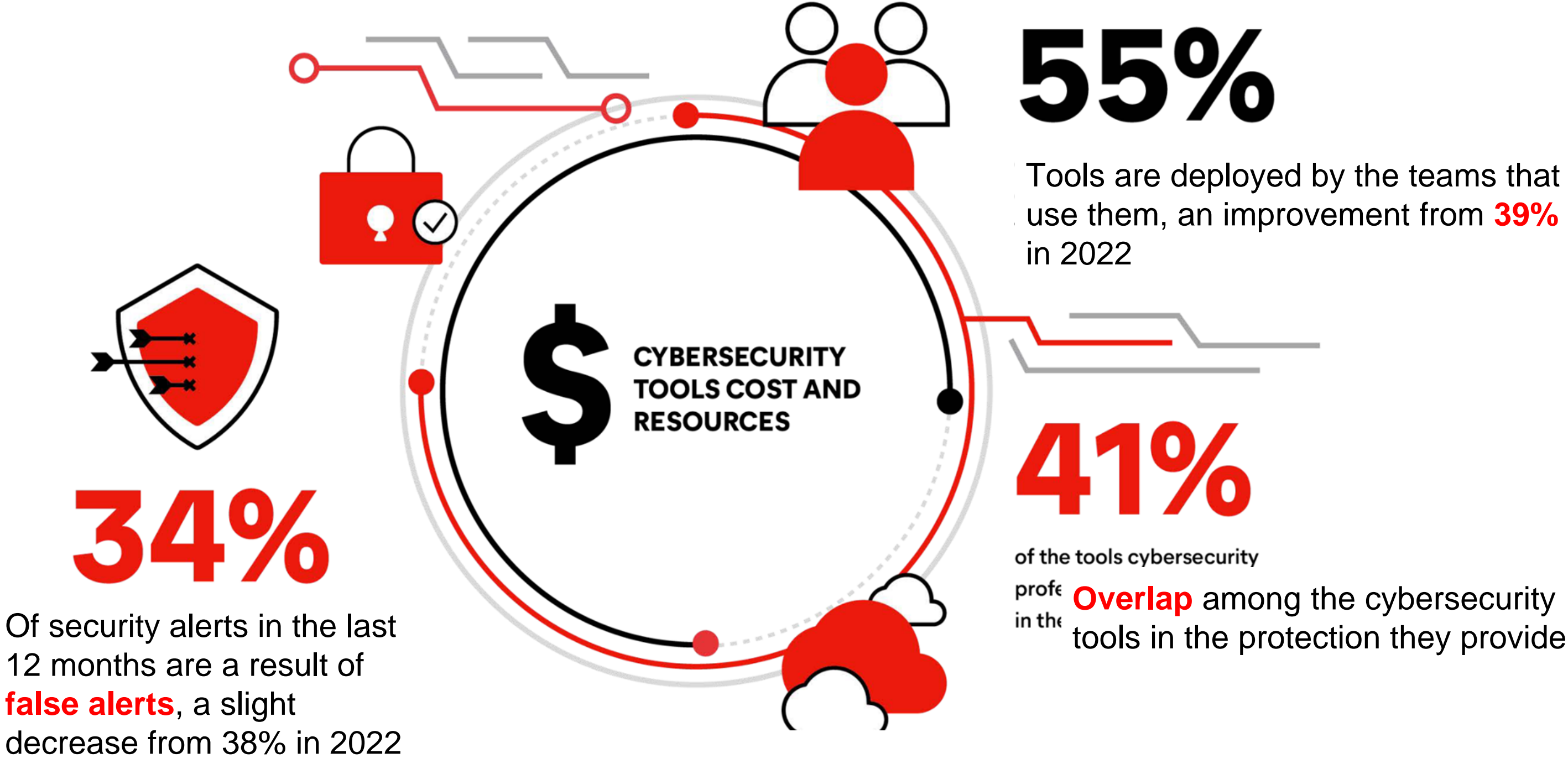
19% feel their spend was inadequate

76% will increase cybersecurity spending in the next 12 months

The complex landscape of cyber technology

Deployment of security tools

55%

Tools are deployed by the teams that use them, an improvement from **39%** in 2022

$ CYBERSECURITY TOOLS COST AND RESOURCES

41%

of the tools cybersecurity profe... in the...

Overlap among the cybersecurity tools in the protection they provide

34%

Of security alerts in the last 12 months are a result of **false alerts**, a slight decrease from 38% in 2022

Key priorities that will dictate cyber security policies

Attack impacts revenue!

Ransomware (29%)
DDoS (28%)
Open Source Vulnerabilities (25%)

Financial impact up to 9% of revenue due to cyber attacks

Complex footprint increased spending

Increased spending – 76%

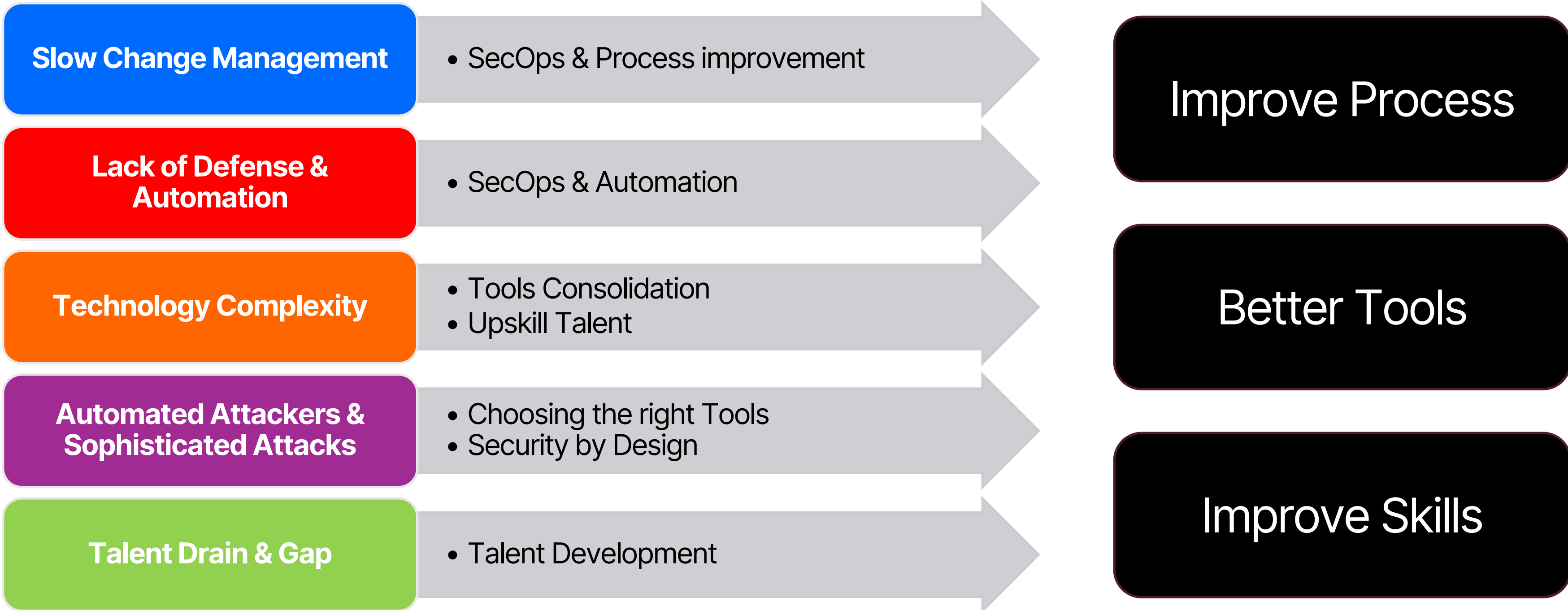Is this enough to keep you secure?

Generative AI impact

Positive impact – 77%
Major threat driver – 35%

Both the organization and bad actors are going to leverage Generative AI

Time to recover

**Decreased spending – increased time to recover by ~48%**

Why is cyber security so difficult?

Challenge	Solution	Category
Slow Change Management	• SecOps & Process improvement	**Improve Process**
Lack of Defense & Automation	• SecOps & Automation	
Technology Complexity	• Tools Consolidation • Upskill Talent	**Better Tools**
Automated Attackers & Sophisticated Attacks	• Choosing the right Tools • Security by Design	
Talent Drain & Gap	• Talent Development	**Improve Skills**

What can be done?

Improve Process

- Automation SecOps

- Have risk / incident framework

- Improve cross functional collaboration

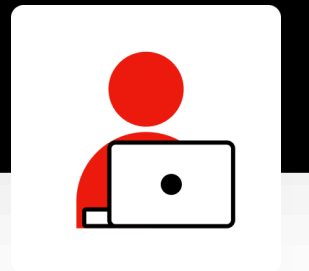- Understand your third party risk!
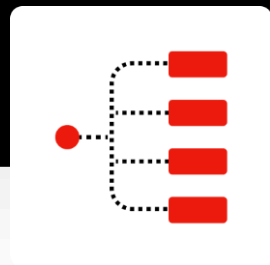
Get Better Tools

- Avoid integration by invoice

- Target security solutions that are easily integrated into existing stacks

- Tools that can be employed flexibly alongside existing systems

- Leverage Machine Learning

Decrease Expertise Gap

- Education: mentoring

- Education investment / upskill

- Outsourcing with trusted advisors

- Managed services

- External talent

Fastly resources

Download our e-books

https://learn.fastly.com/security-esgresearch-balancing-requirements-for-application-protection

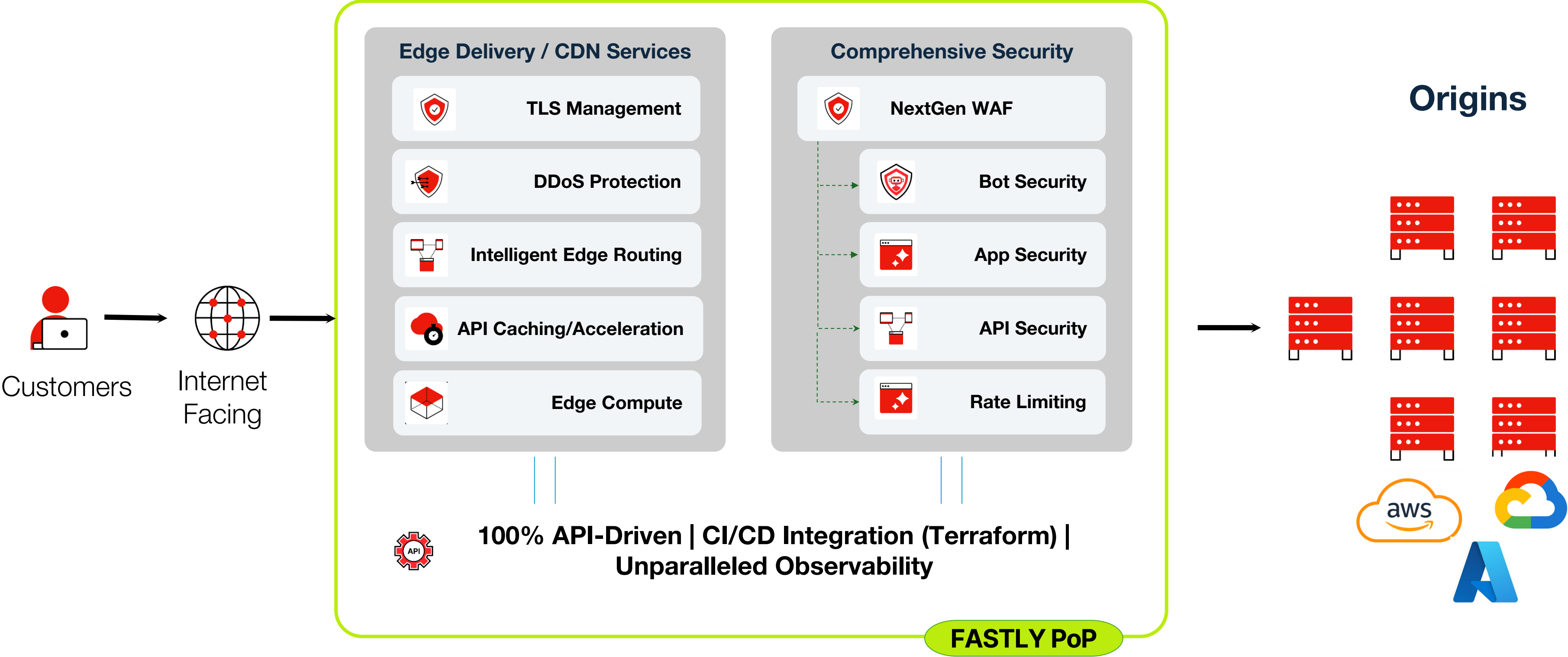*https://www.fastly.com/blog/economic-advantages-fastly-application-security-solutions*

https://www.fastly.com/blog/three-application-security-trends-to-monitor-in-2025

Making the internet a better place, where all experiences are fast, safe, and engaging

fastly

Fastly's Secure Edge Platform

Customers

Internet Facing

FASTLY PoP

Edge Delivery / CDN Services

- TLS Management
- DDoS Protection
- Intelligent Edge Routing
- API Caching/Acceleration
- Edge Compute

Comprehensive Security

- NextGen WAF
- Bot Security
- App Security
- API Security
- Rate Limiting

100% API-Driven | CI/CD Integration (Terraform) | Unparalleled Observability

Origins

aws

Fastly's global network

Single POP
Multiple POPs
Planned new POP
Planned upgrade

430Tbps of connected global capacity
98% Customer Satisfaction Score for Fastly Support
>90% of Customers use WAF full-blocking mode

Industry Report

Public Sector

Modernize, secure, and scale public sector IT with innovative edge solutions. Explore actionable strategies in our new industry report.

Read report →

Industry Report

Healthcare

Explore essential security strategies for healthcare. Learn how CDNs and edge computing can enhance data protection amidst digital transformation. Get actionable insights that protect sensitive patient data and maintain trust.

Read report →

Industry Report

eCommerce

Prepare your eCommerce site for holiday traffic surges. Get insights on managing peak season traffic, improving site performance, and protecting customer data.

Read report →

Industry Report

Financial Services

Explore the challenges facing FinServ organizations today and learn which 10 security advantages are driving big migrations within the industry.

Read report →

Industry Report

SaaS

Explore the challenges facing SaaS organizations today and learn how to regain control and deploy at the edge with flexibility.

Read report →

Industry Report

Digital Publishing

Explore the challenges facing digital publishers today and learn optimization strategies to ensure your content reaches online audiences before anyone else.

Read report →

Industry Report

Digital Publishing

The 2024 election will bring huge digital traffic spikes, requiring publishers to use scalable infrastructure for seamless, real-time news delivery and performance.

Read report →

Industry Report

Streaming Media

Explore the escalating cyber threats facing online broadcasters, including, DDoS attacks, bots, and piracy. This report highlights the need for robust security measures to protect valuable content, sensitive data and reputation while recommending advanced defenses like CDNs, WAFs, and forensic watermarking.

Read report →

Industry Report

Travel & Hospitality

The travel industry seems to be struggling with outdated IT infrastructure that hinders efficiency, innovation, and customer satisfaction. Modernizing your infrastructure with contemporary technologies can streamline operations, enhance security, minimize churn, and significantly improve user experiences.

Read report →

Industry Report

eCommerce

Explore the challenges facing ecomm companies and learn optimization strategies for performance, security, and bots.

Read report →

Industry Report

Gaming

Learn the challenges facing gaming companies and developers, and how an edge cloud strategy can help.

Read report →

Industry Report

Airlines

Explore website delivery performance from the world's largest airlines and learn how an edge cloud strategy can help.

Read report →

The values that guide us.

We have a **curious** spirit.

We **focus** on our customer.
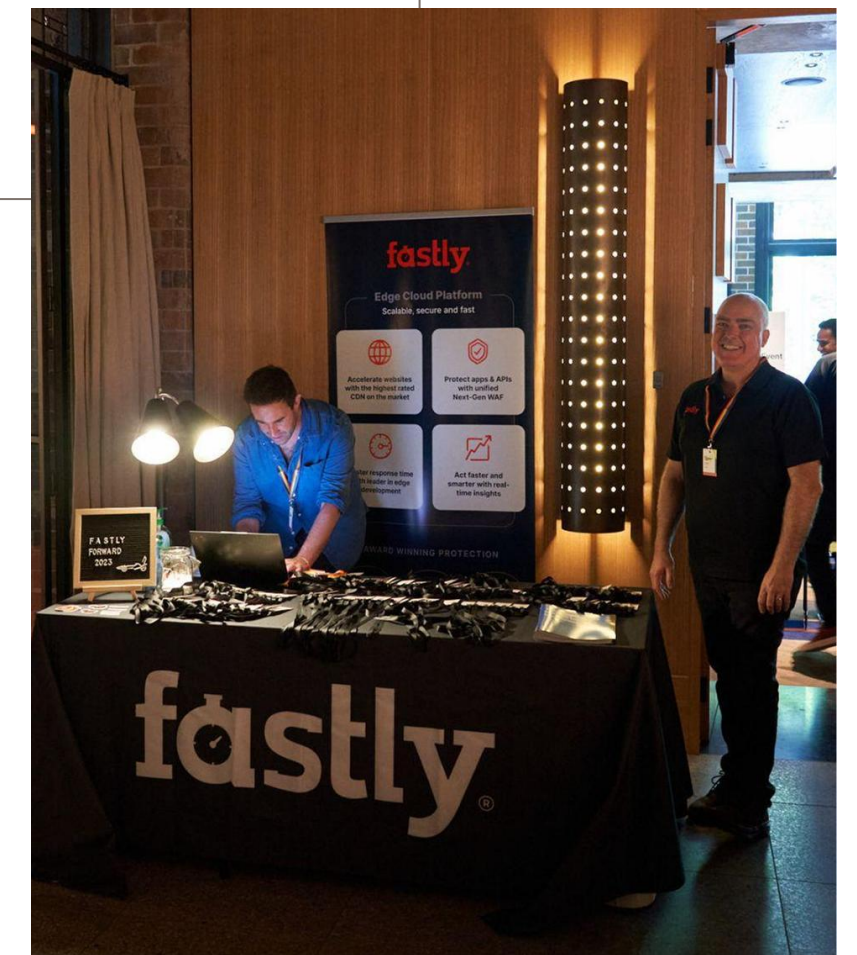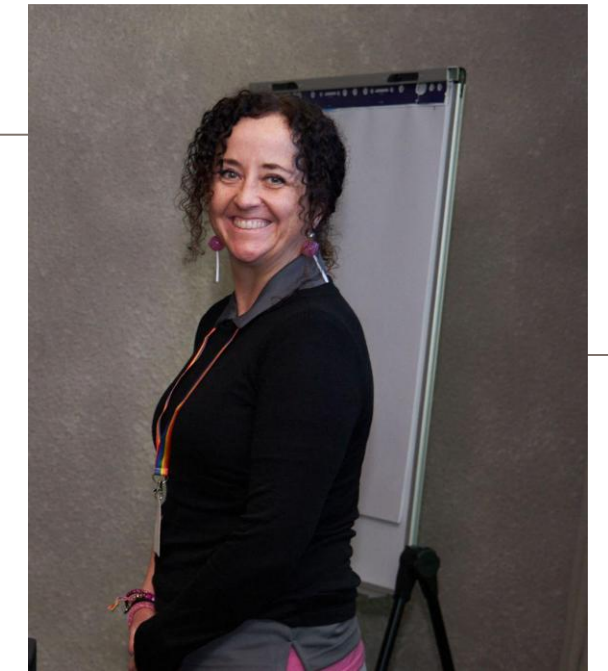
We are **trustworthy**.

We act with **passion**.

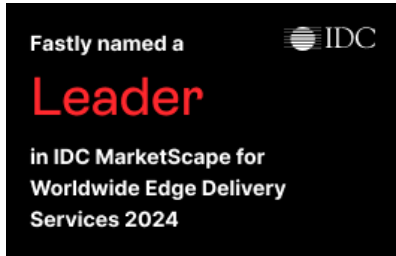We operate with **integrity**.

We are **competitive**.

We embrace **transparency**.

We are **good** people.

Recognised by analysts and customers

LEADER & CUSTOMERS' CHOICE
Worldwide Edge Delivery
Highly Innovative

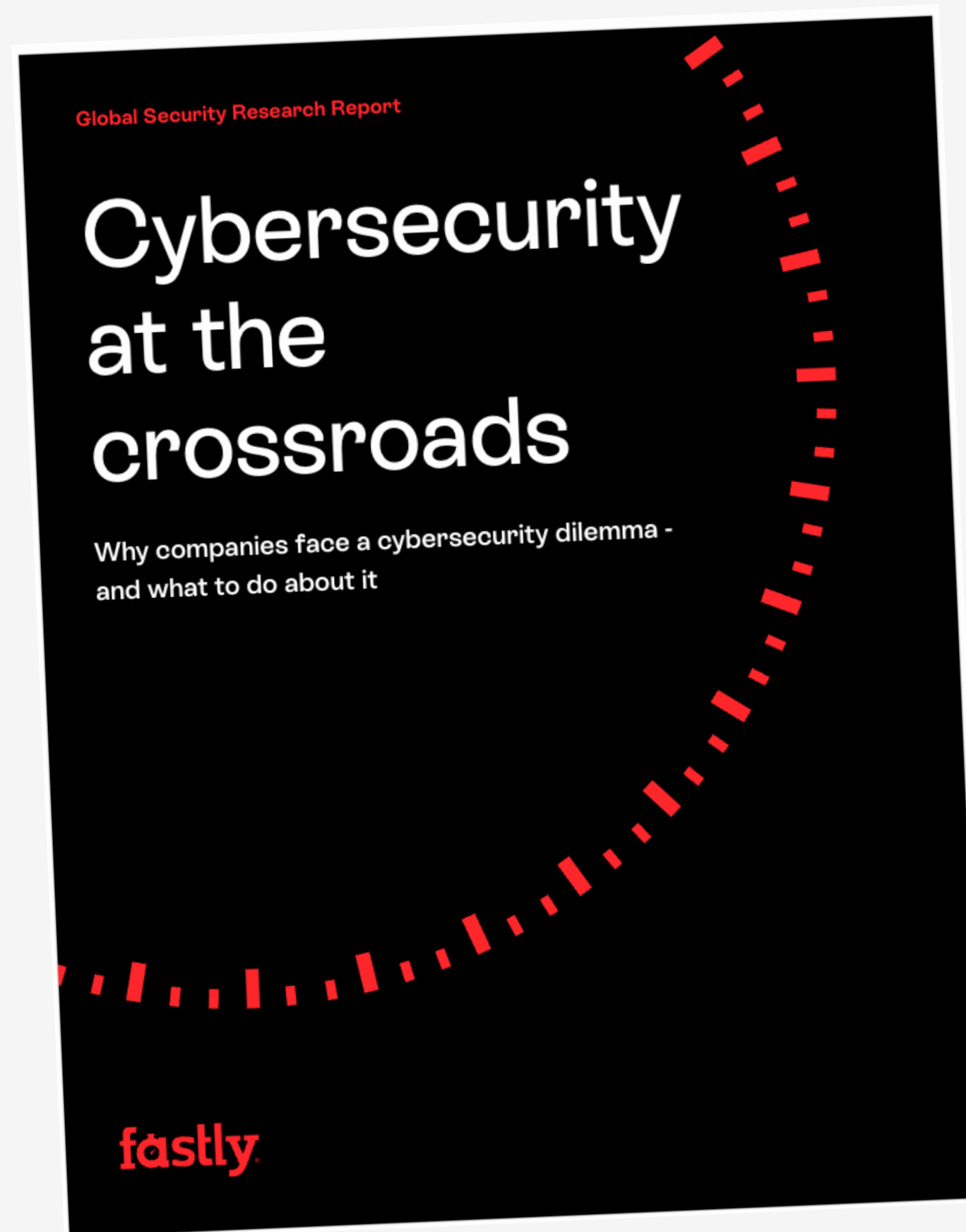**CUSTOMERS' CHOICE**
Web App/API Protection
6 years in a row

LEADER
Edge Development
Highest Security Score

CUSTOMER VALUE
Network Services
ROI 189%

1. What is the average revenue impact from cyber incidents across the Fastly Survey?

1. How many percent of incidents are handled by external vendors?

1. What is the percentage of Fastly's customers that use WAF in full-blocking mode?

Global Security Research Report

Cybersecurity at the crossroads

Why companies face a cybersecurity dilemma - and what to do about it

fastly

https://bit.ly/4jExIaT

Download your copy here!

Join us at Booth #5 for a chat and have a coffee on us!