



The Role of AI in Email Security

KnowBe4

Erich Kron

Security Awareness Advocate

Osterman Research

Michael Sampson

Principal Analyst

About the speakers



KnowBe4

Erich Kron

Security Awareness Advocate



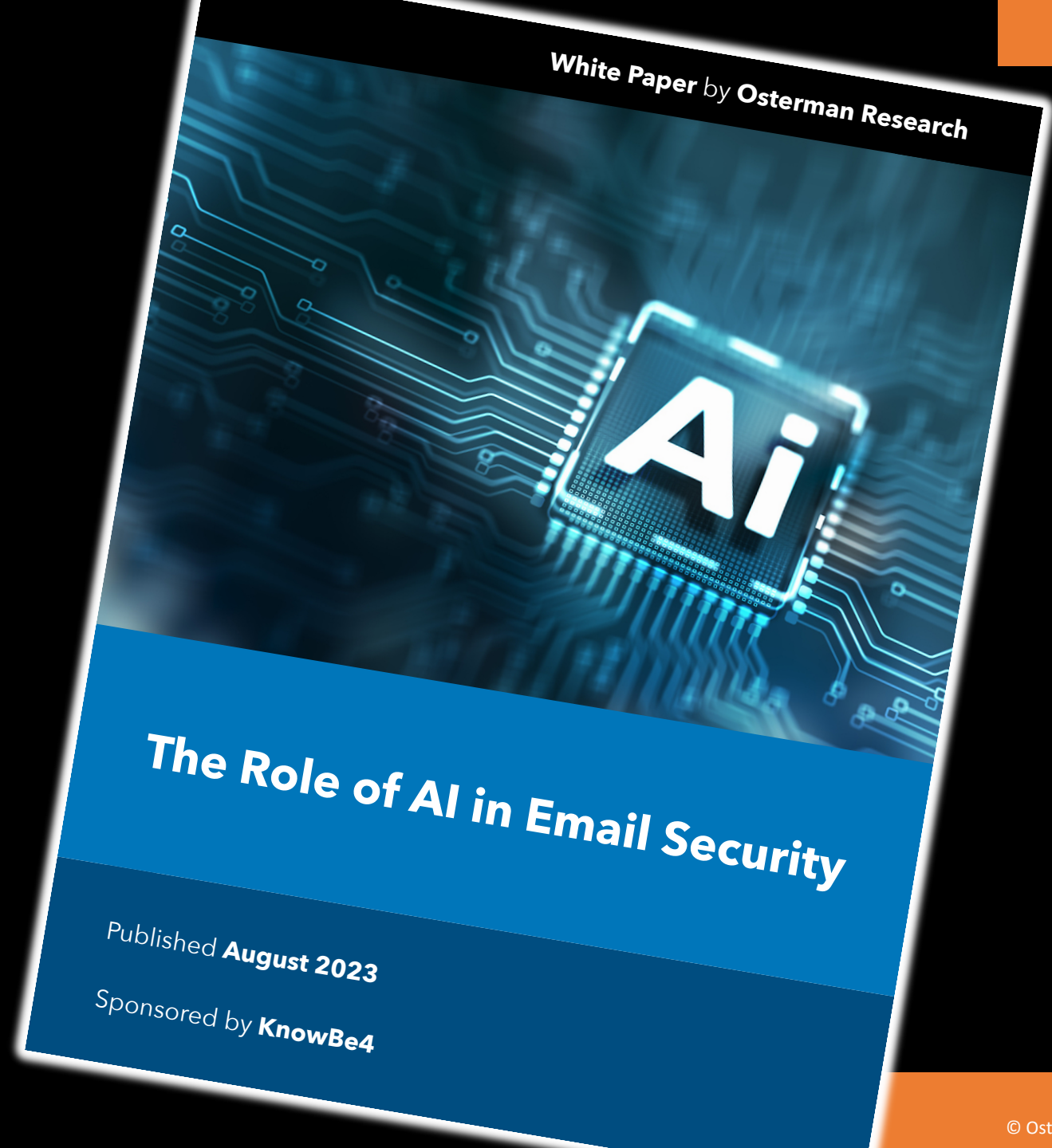
Osterman Research

Michael Sampson

Principal Analyst



Research report



About Osterman Research

Market
research and
consulting

Delivering
insight

Cybersecurity

Information governance

Data protection

Survey design (n=148 in the United States)

Respondents	Firm Size	Industry
IT and security leaders	Firms with at least 1,000 employees	No industry restrictions or exclusions
Know how their organization is using or planning to use AI in email security	Average 3,274	



RESEARCH FINDING

Why AI for
email security?

Cybercriminals are creating new attack methods



Bypass
traditional
detection
methods

Fewer
malicious
signals and
markers

Results in new
forms of spear-
phishing, BEC,
impersonation

Cybercriminals are using AI in email attacks



To create
unique attacks
at scale

To mimic
writing style,
tone, and
mannerisms
(supercharged
impersonation)

To improve
baseline
message
grammar
quality

Vendors are leveraging AI in email security

Profile
behavior of
each sender
and recipient

Detect
anomalous
patterns

Detect emails
written using
AI – and
malicious
intent

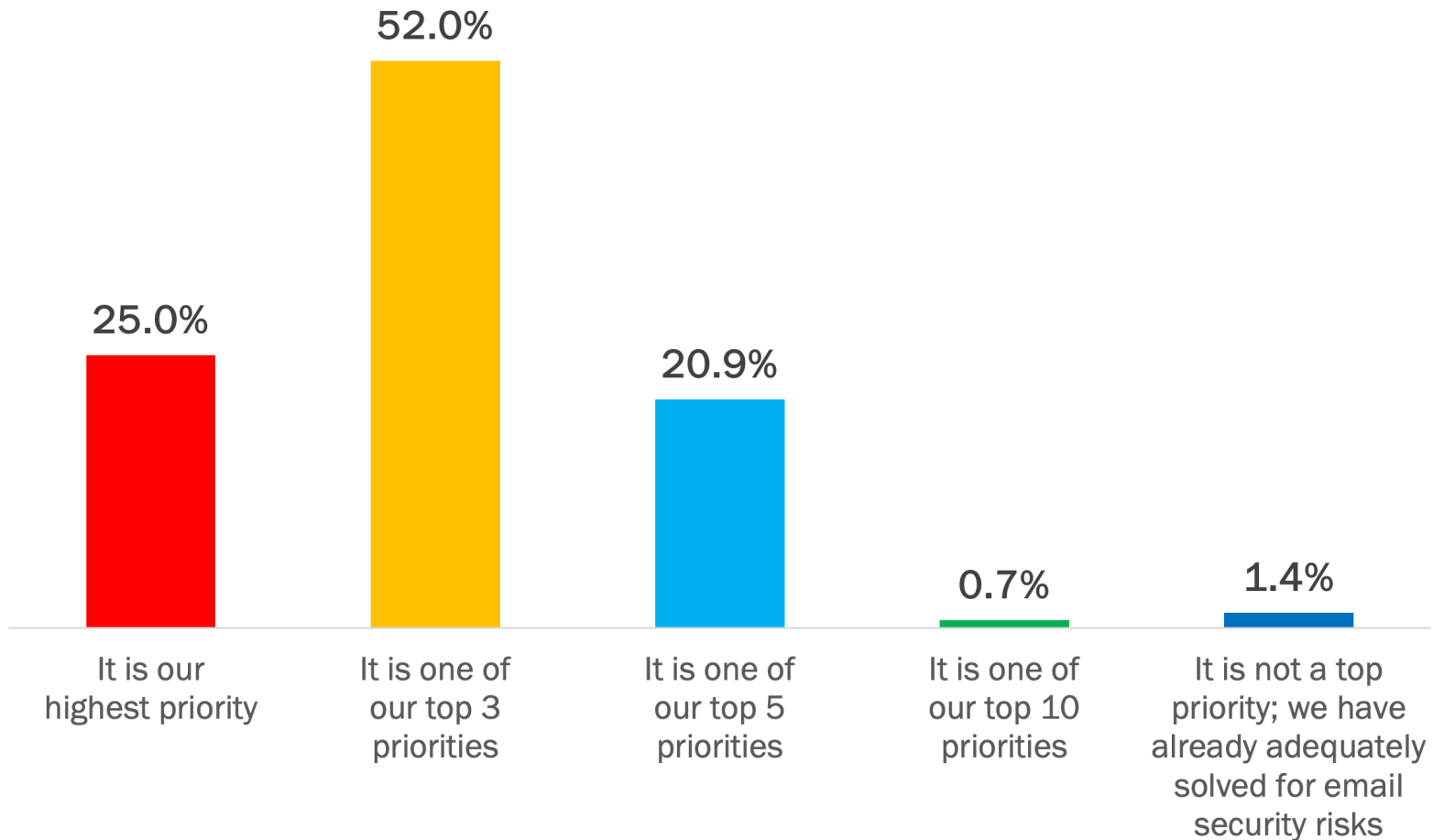
Create
derivative
training data

RESEARCH FINDING

Trends in email and email security

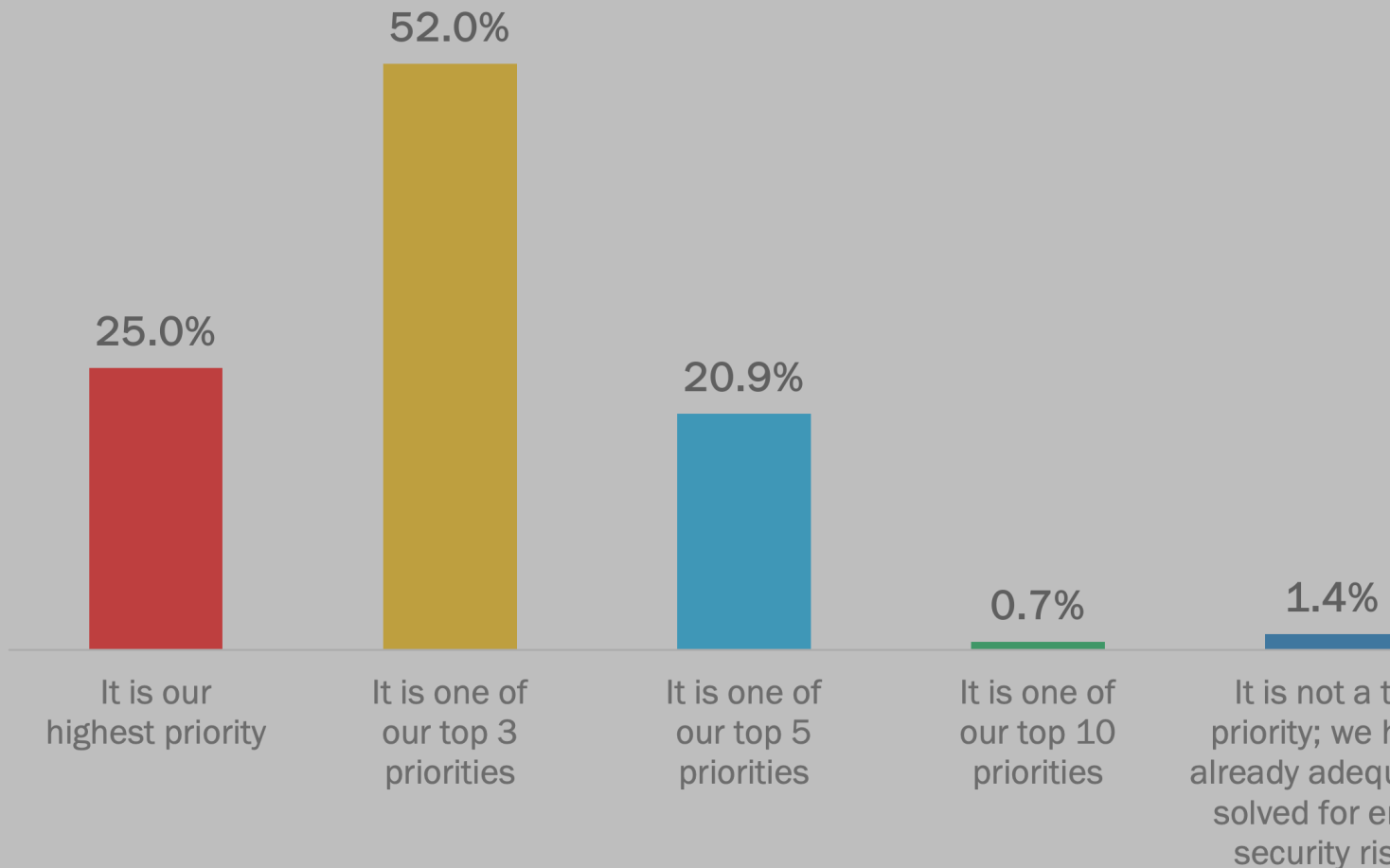
Email security is a very high priority

Percentage of respondents



Email security is a very high priority

Percentage of respondents



Insecure by design

From email to everything else

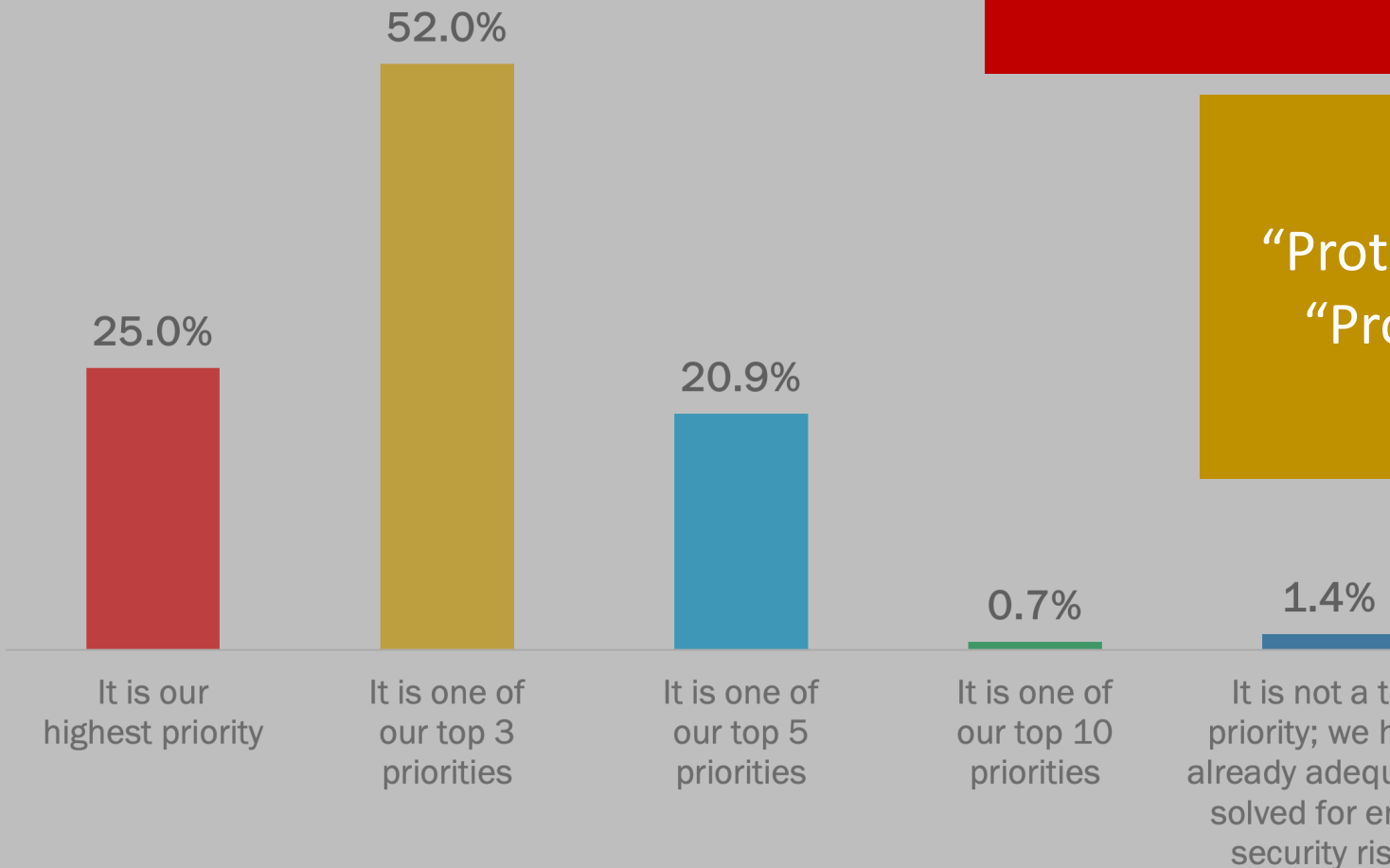
Direct contact to employees

Critical; can't be turned off

Ultimate tool for malicious delegation

Email security is a very

Percentage of respondents



“Safeguarding productivity”
Email is an “increasing threat”
“Stop threats” (social engineering, phishing, ATO)

“Protecting proprietary information”
“Protecting against cyberattacks”

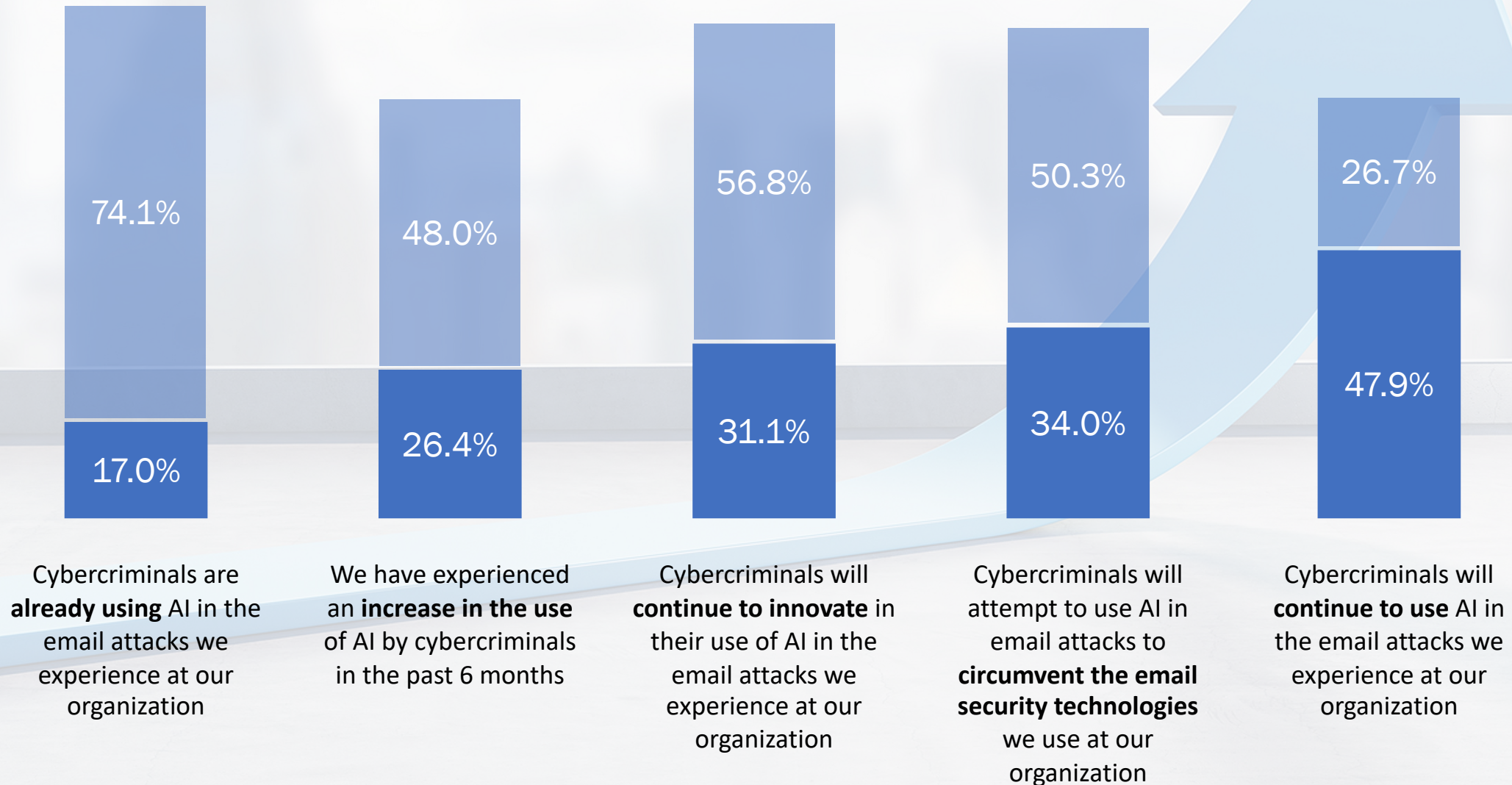
Email is a “vulnerable channel”
“Protected from cyberattacks”
+ “stop data breach”
“More pressing issues”

Agree

Strongly agree

Organizations see cybercriminals using AI

Percentage of respondents indicating “agree” or “strongly agree”

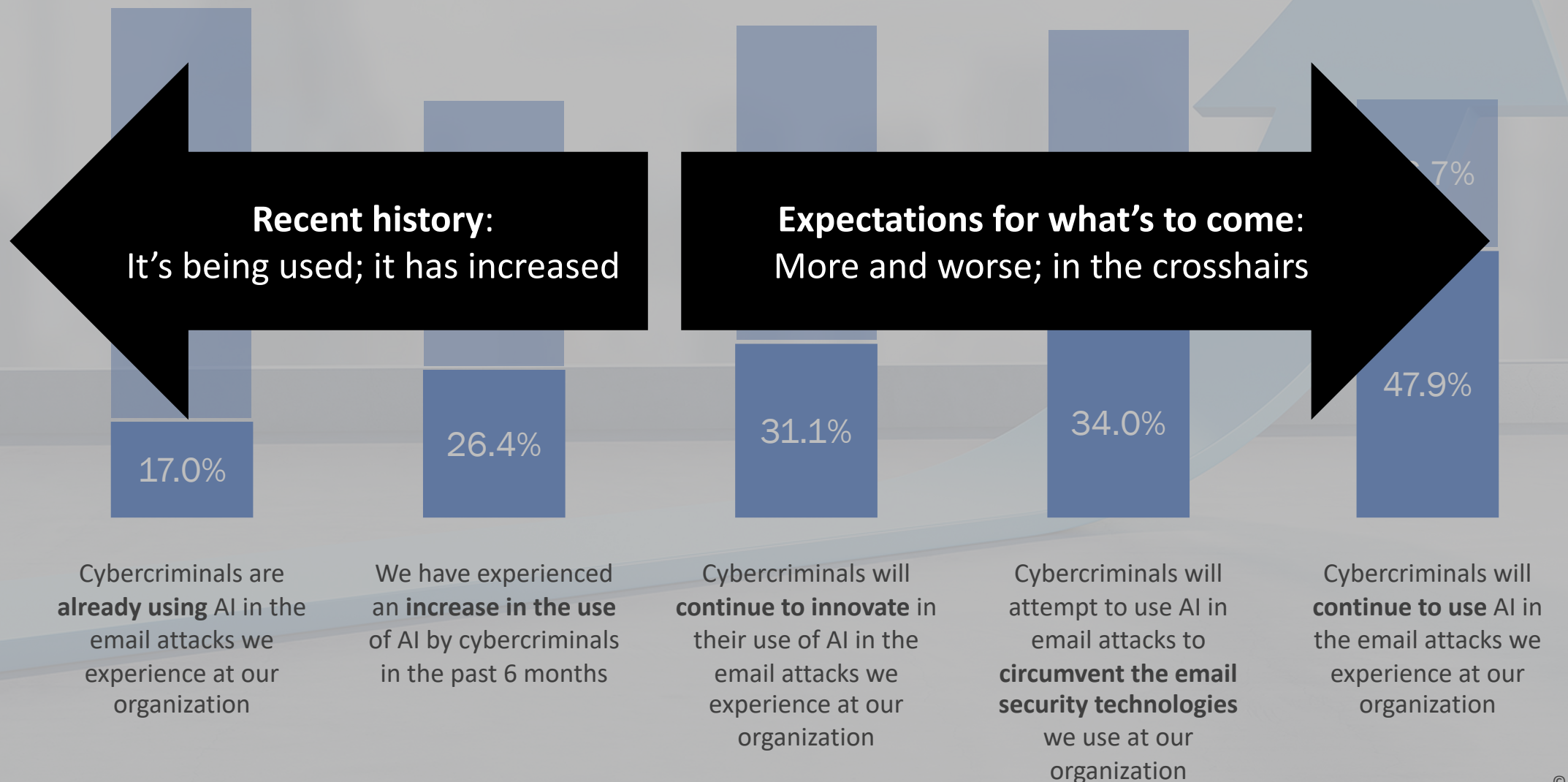


Agree

Strongly agree

Organizations see cybercriminals using AI

Percentage of respondents indicating “agree” or “strongly agree”



Recent history:
It's being used; it has increased

Expectations for what's to come:
More and worse; in the crosshairs

Cybercriminals are **already using** AI in the email attacks we experience at our organization

We have experienced an **increase in the use** of AI by cybercriminals in the past 6 months

Cybercriminals will **continue to innovate** in their use of AI in the email attacks we experience at our organization

Cybercriminals will attempt to use AI in email attacks to **circumvent the email security technologies** we use at our organization

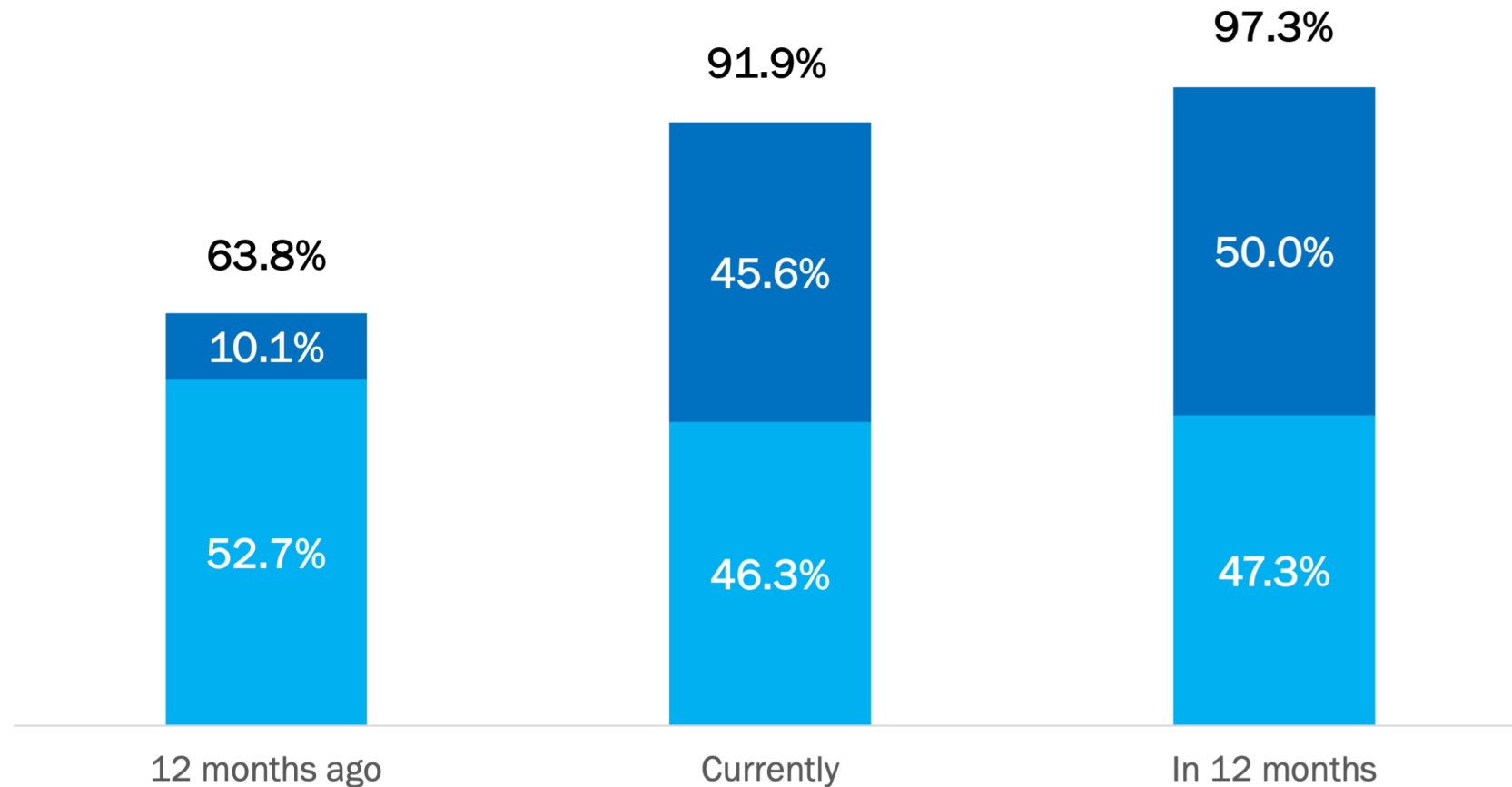
Cybercriminals will **continue to use** AI in the email attacks we experience at our organization

Extremely

Moderately

AI-enabled protections more important

Percentage of respondents indicating “moderately” or “extremely important”

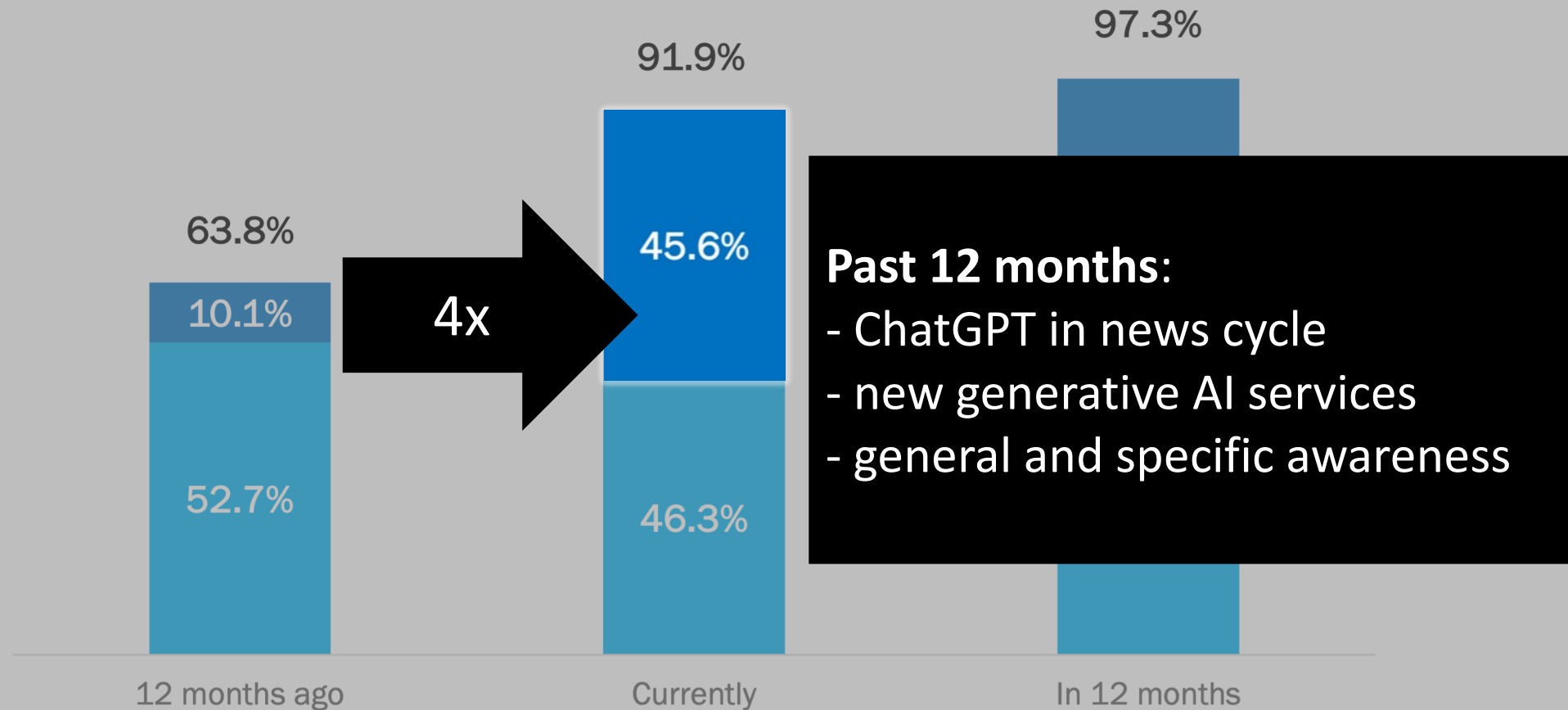


Extremely

Moderately

AI-enabled protections more important

Percentage of respondents indicating “moderately” or “extremely important”

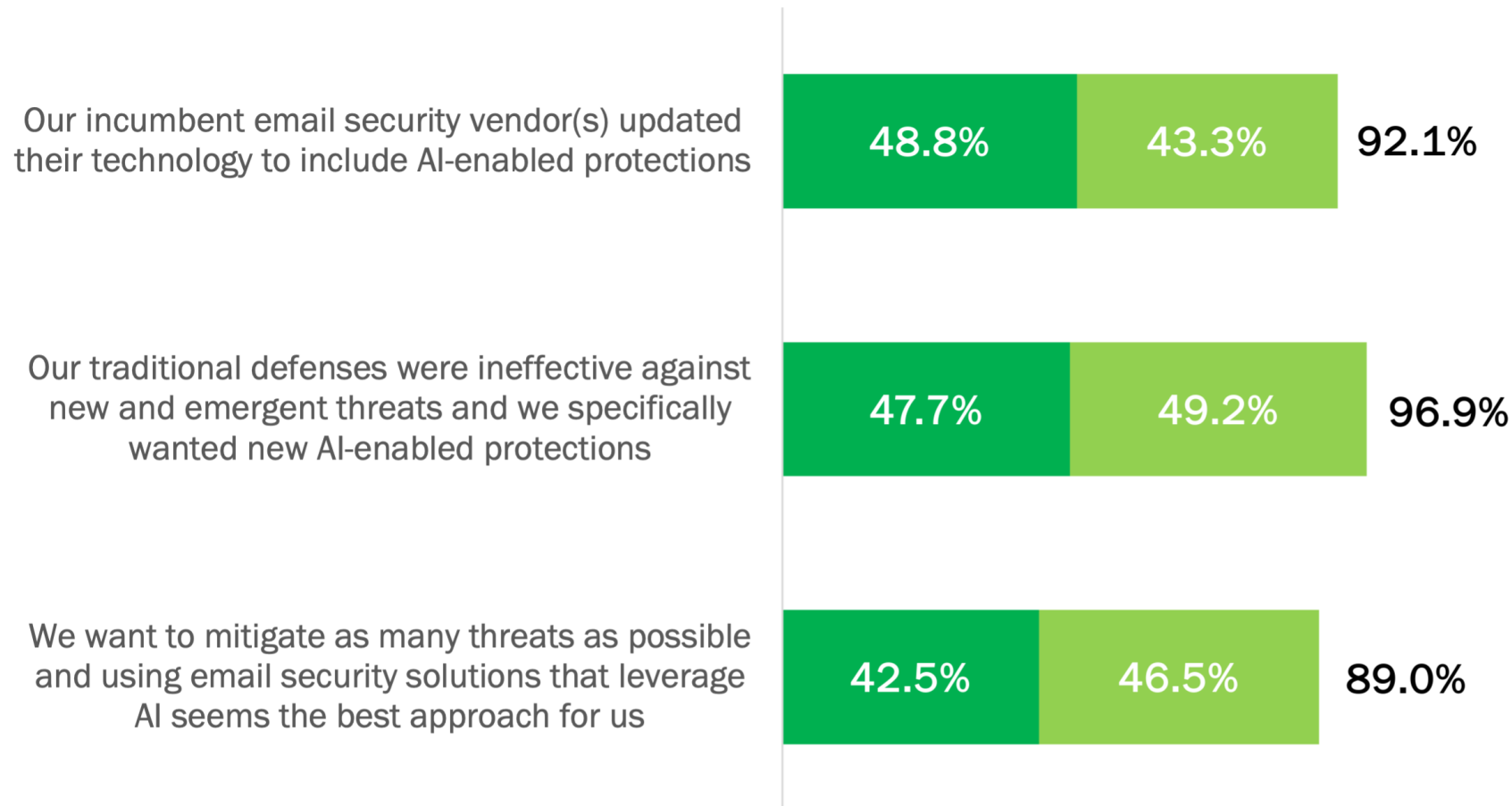


Extremely

Moderately

Email security vendors embracing AI

Percentage of respondents indicating “moderately” or “extremely important”

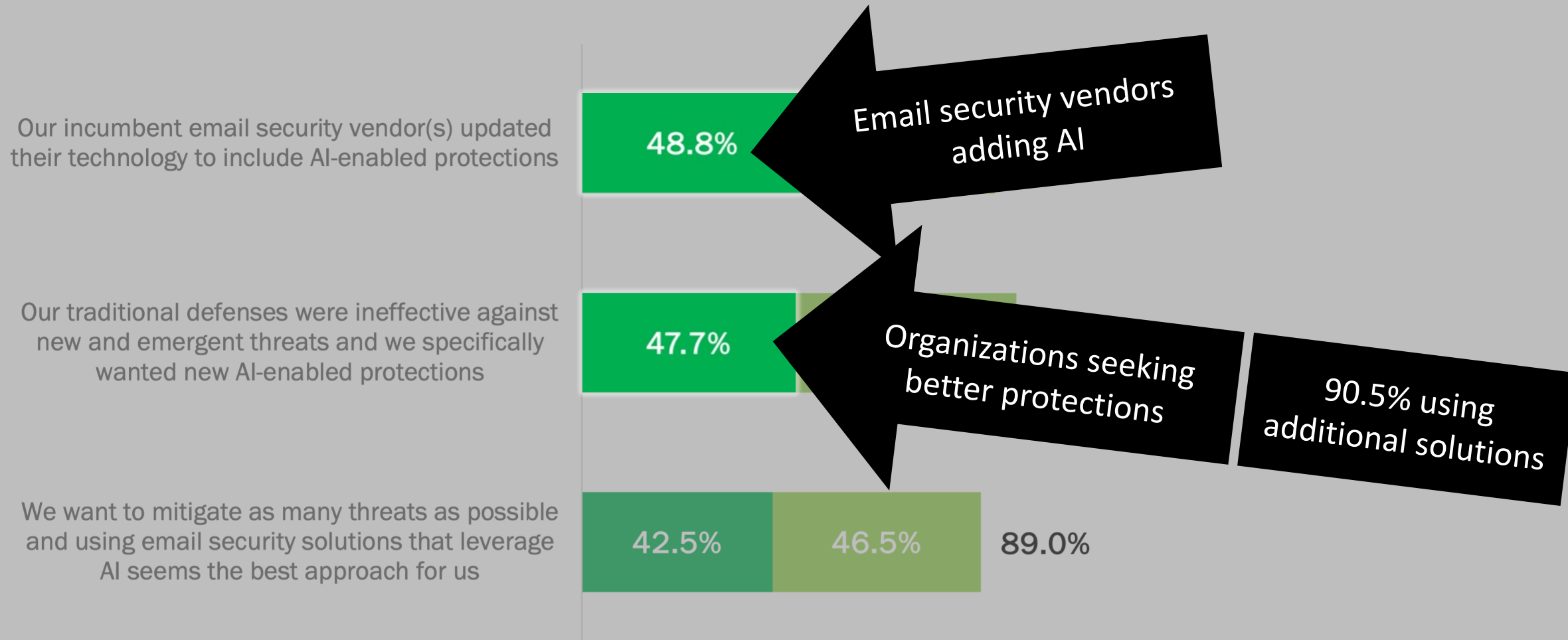


Extremely

Moderately

Email security vendors embracing AI

Percentage of respondents indicating “moderately” or “extremely important”



RESEARCH FINDING

Assessing current usage of AI for email security

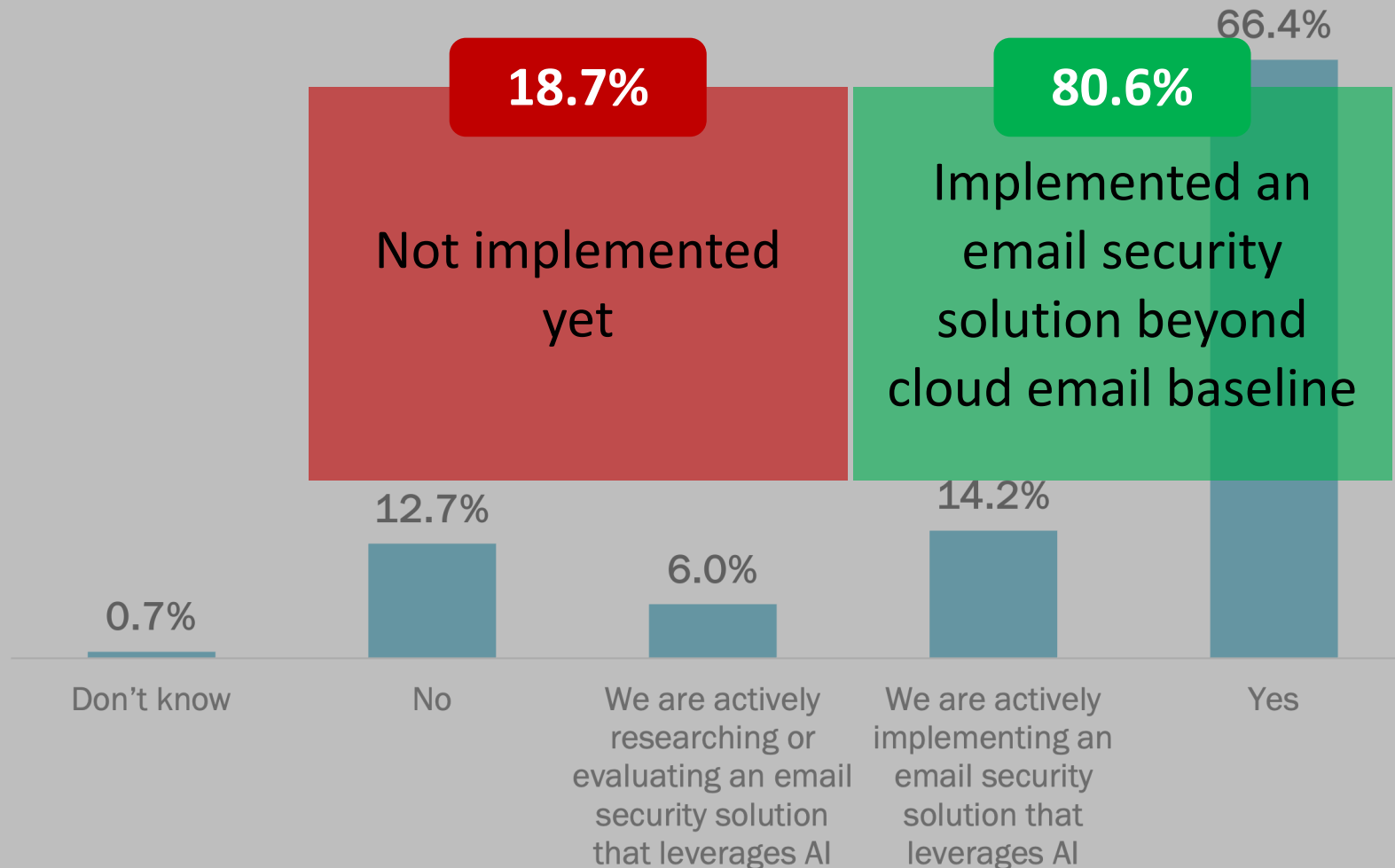
Most organizations already using AI

Percentage of respondents



Most organizations already using AI

Percentage of respondents

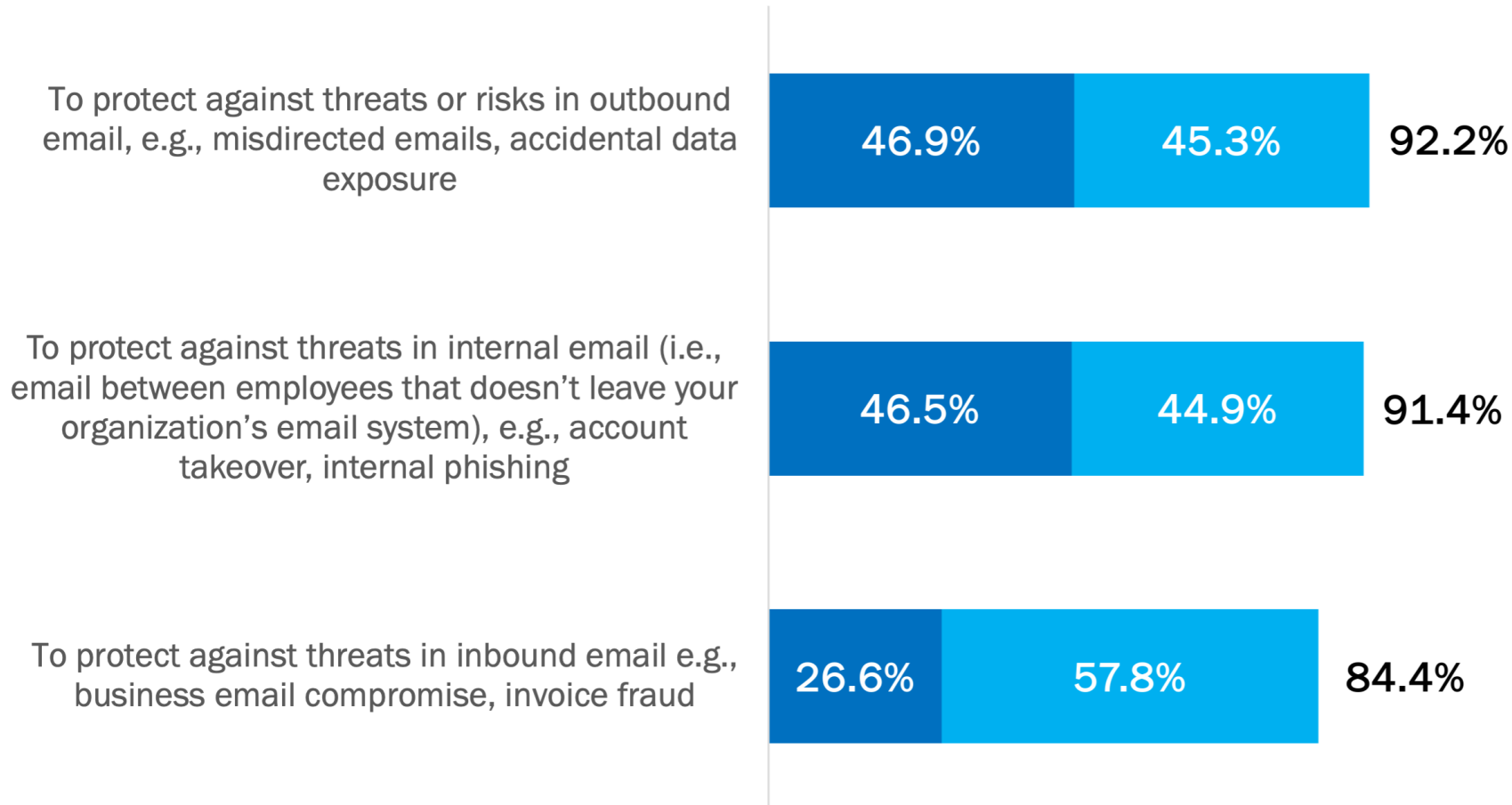


Extremely

Moderately

AI used to protect against various threats

Percentage of respondents indicating “moderately” or “extremely important”



Extremely

Moderately

AI used to protect against various threats

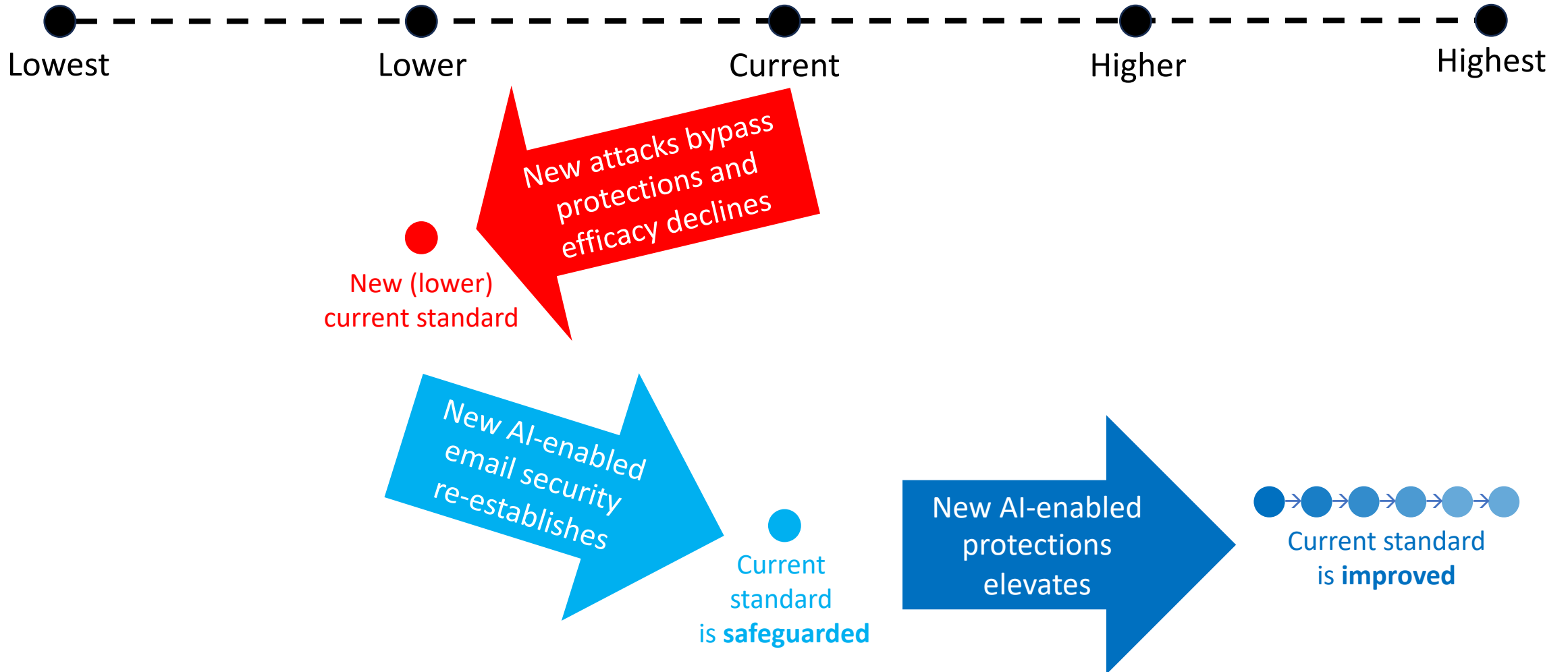
Percentage of respondents indicating “moderately” or “extremely important”



Strange prioritization;
organizations can't ignore
the threat conveyed by
inbound email

AI safeguarding and improving detection efficacy

Detection efficacy

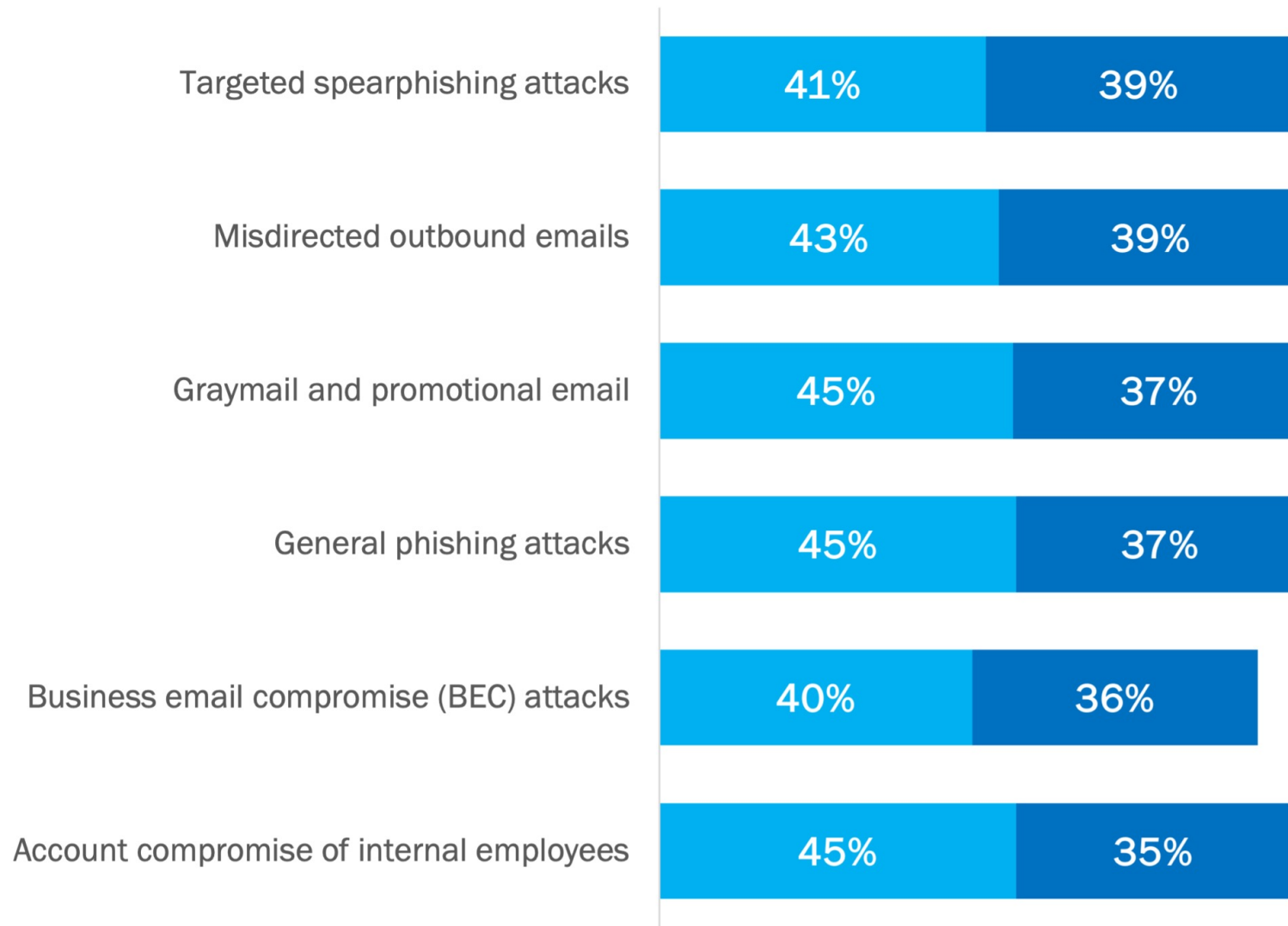


Safeguarded

Improved

AI safeguarding and improving detection efficacy

Percentage of respondents



Some organizations don't realize they are already being protected by AI



Relying
on email
provider only
... who uses AI

Already using
the tools ... but
priority focus
is elsewhere

Most intend
to embrace
additional
tools over next
24 months



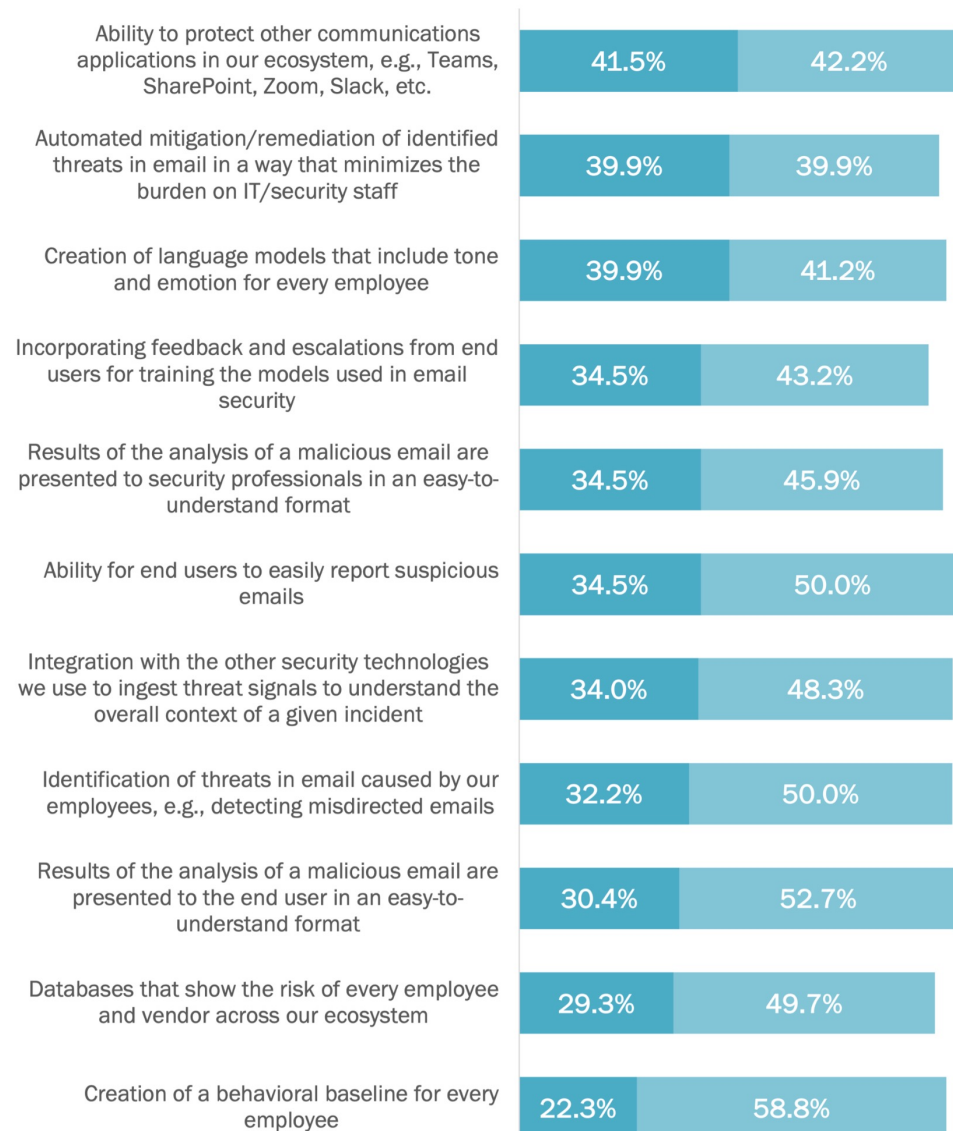
RESEARCH FINDING

Shopping list for AI in email security

Extremely

Moderately

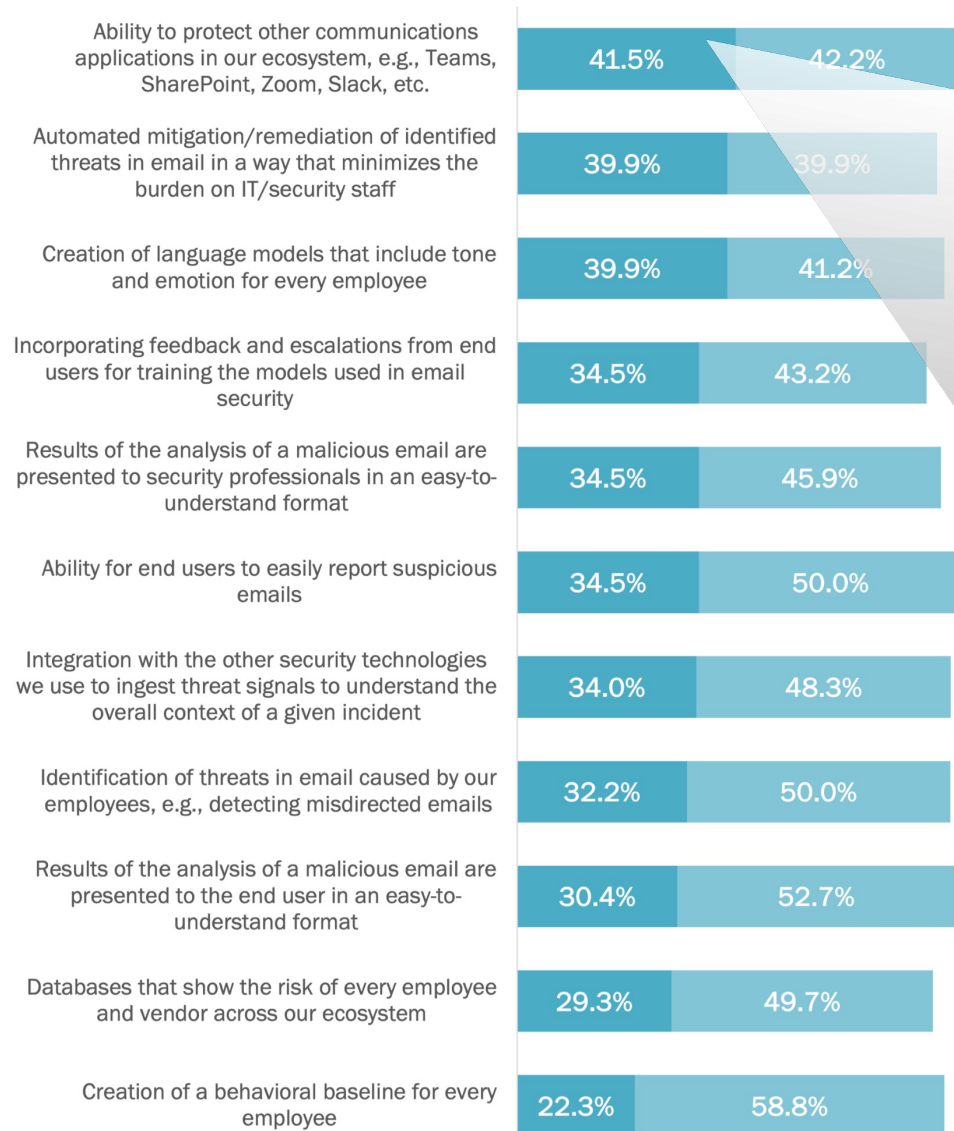
Shopping list – ranking 11 purchase factors



Extremely

Moderately

Shopping list – ranking 11 purchase factors



#1 – Protecting more than just email

Email = essential

Email only = insufficient

Employees working in tools beyond email; protect all

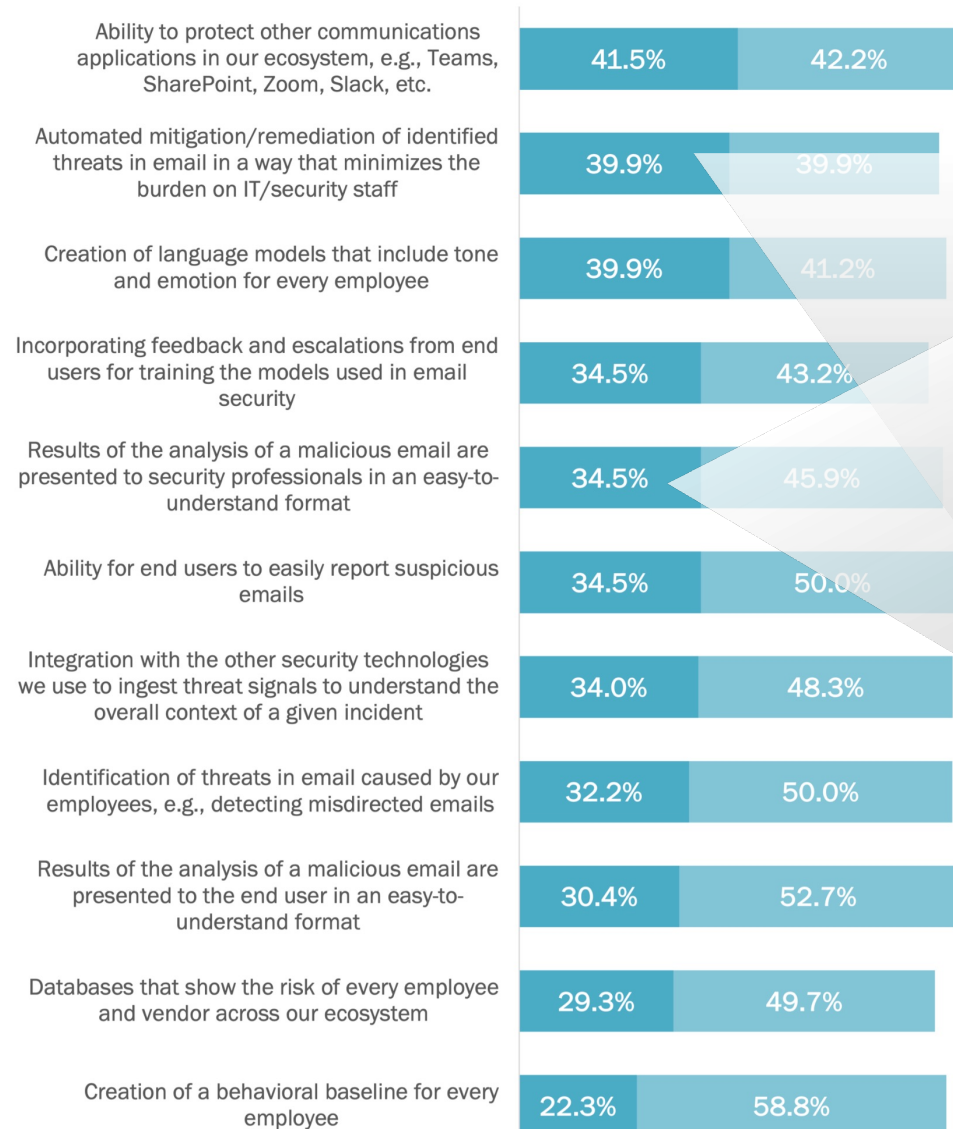
Ability to protect other communications applications in our ecosystem

extremely
41.5%

Extremely

Moderately

Shopping list – ranking 11 purchase factors



#2 – Simplifying security processes for IT/security

Empowering → simplification
Automated plus informed

Automated mitigation / remediation of identified threats in email in a way that minimizes burden on IT/security staff

extremely
39.9%

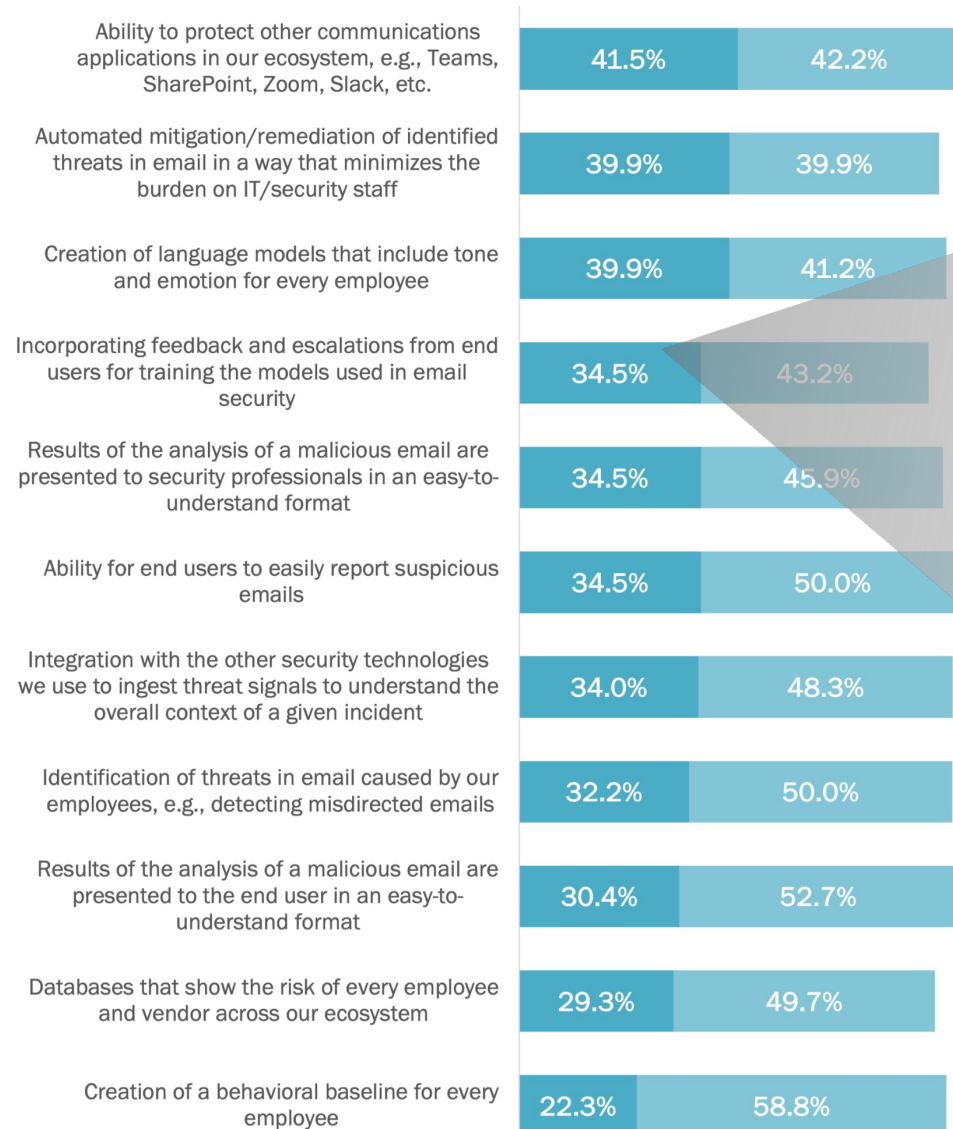
Results of the analysis of a malicious email are presented to security professionals in an easy-to-understand format

extremely
34.5%

Extremely

Moderately

Shopping list – ranking 11 purchase factors



#4 – Train ML models on organizational context

Use employee feedback to train ML models on organizational context

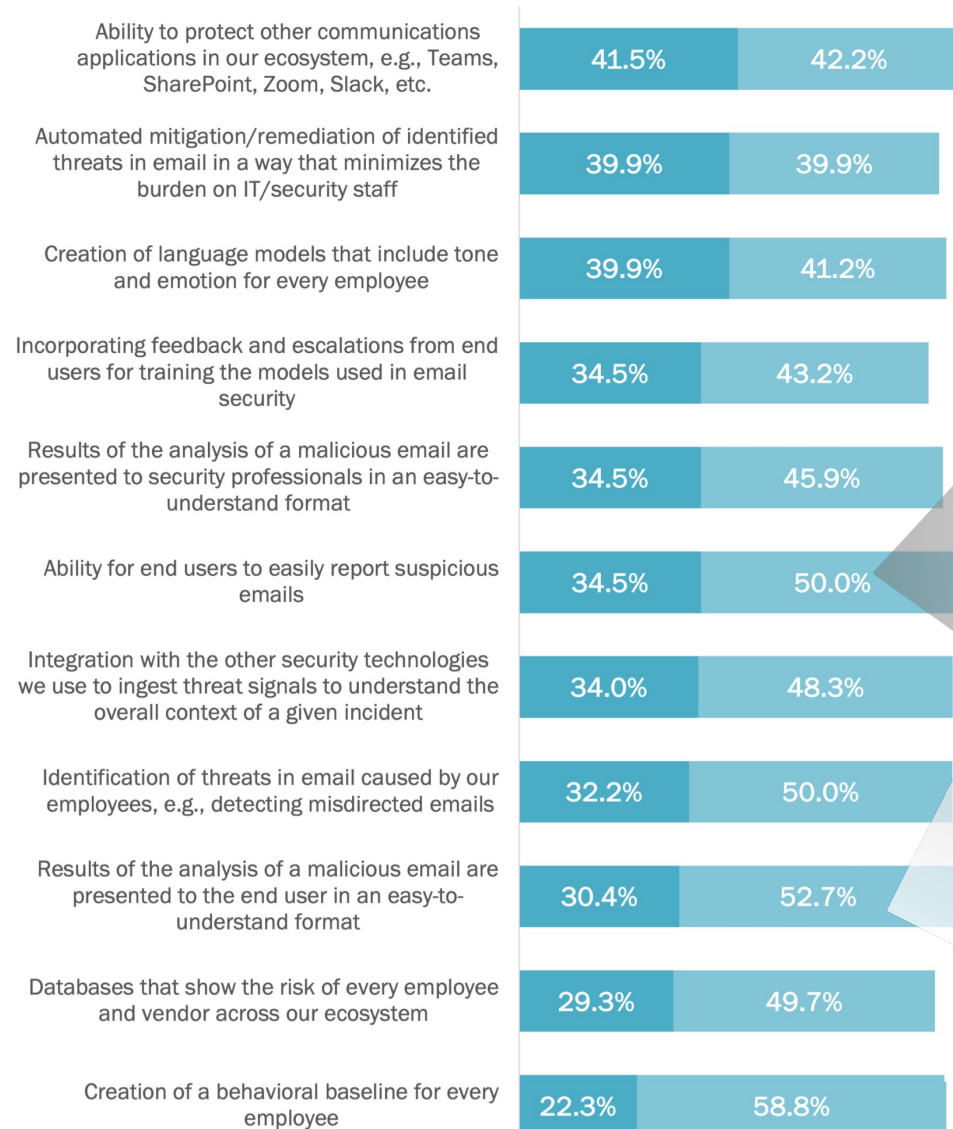
Incorporating feedback and escalations from end users for training the models used in email security

extremely
34.5%

Extremely

Moderately

Shopping list – ranking 11 purchase factors



#1 and #3 overall – Enlist employees in fight against email threats

Employee involvement is critical

Ability for end users to easily report suspicious emails

extremely and moderately

84.5%

Results of the analysis of a malicious email are presented to the end user in an easy-to-understand format

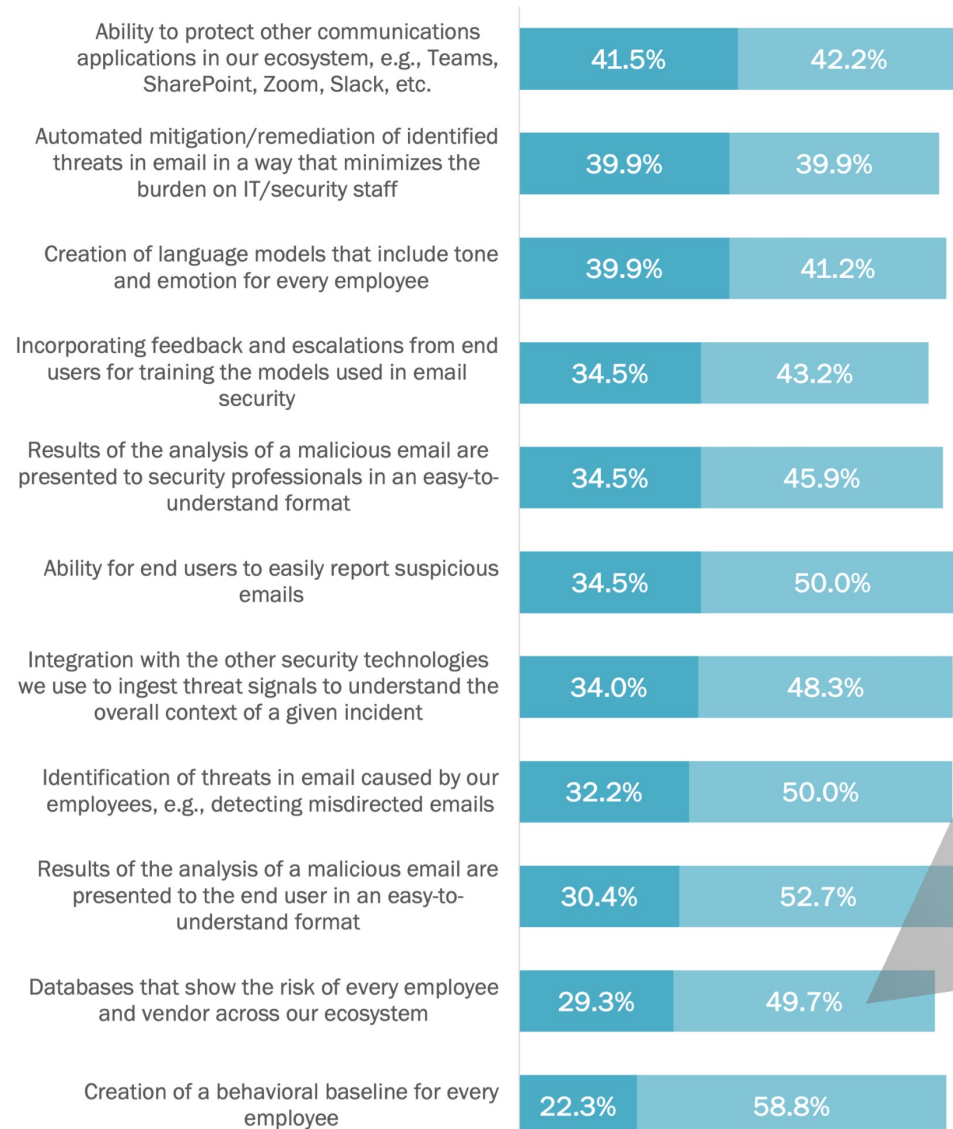
extremely and moderately

83.1%

Extremely

Moderately

Shopping list – ranking 11 purchase factors



Underlying technical wizardry assumed

Detection relies on these capabilities

Databases that show the risk of every employee and vendor across our ecosystem


extremely
29.3%

Creation of a behavioral baseline for every employee

extremely
22.3%


RESEARCH FINDING

Best practices in using AI for email security

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large black sign in front of his chest. He is looking directly at the camera with a neutral expression. The background is a plain, light gray wall.


If you can't see new
threat methods in
email, fix visibility

1

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large white sign. He is looking directly at the camera with a neutral expression. The background is plain white.


Technology plus
process plus people
is still the order
of the day

2

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large black sign. The sign has white text on it. The background is a plain, light grey color.

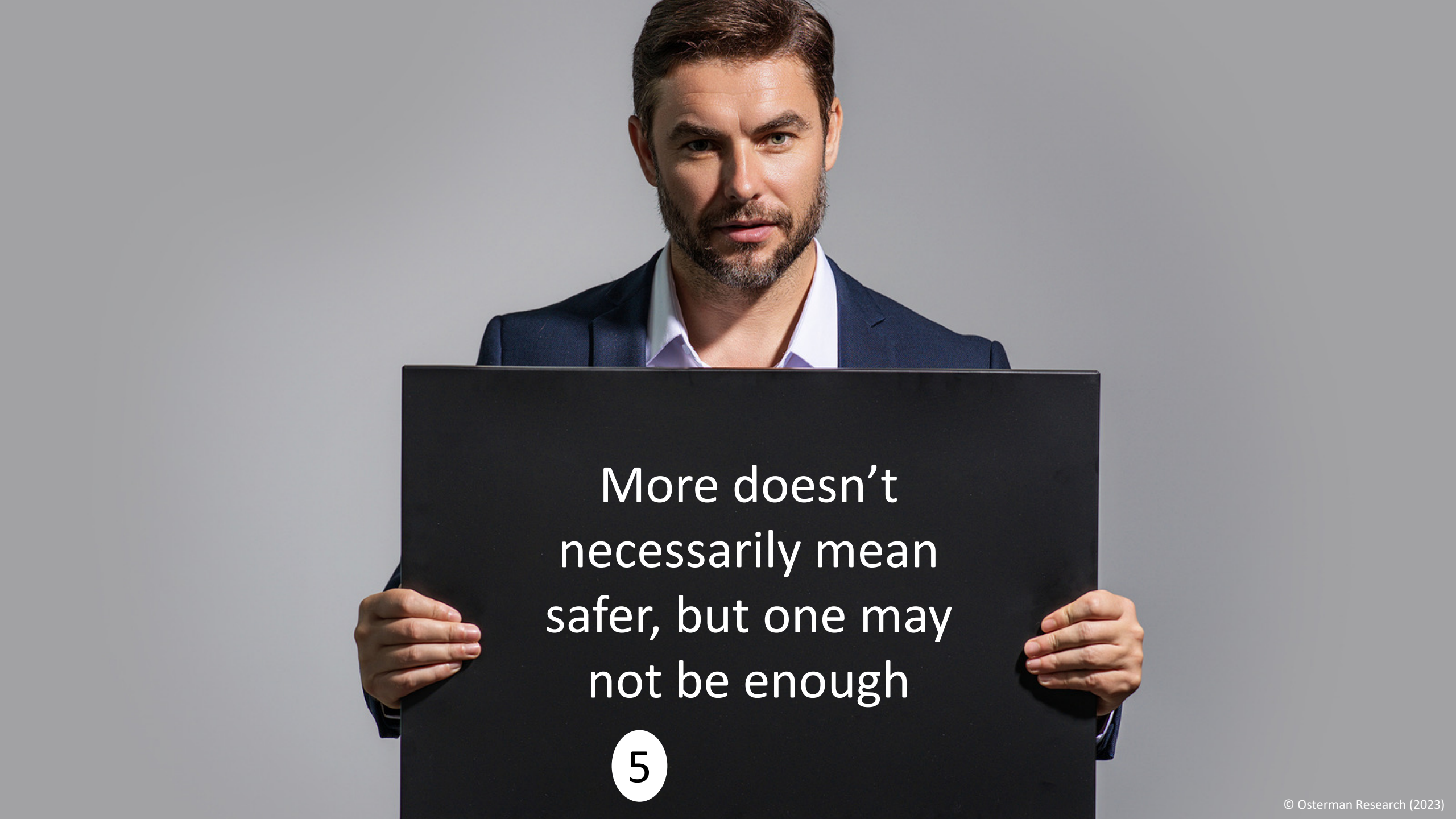
Take signals for
detecting attacks in
email from more than
just email

3

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large white sign in front of his chest. He is looking directly at the camera with a neutral expression. The background is plain white.


AI does not
eliminate the need
for cybersecurity
expertise

4

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large black sign in front of his chest. The sign contains white text. The background is a plain, light grey wall.

More doesn't
necessarily mean
safer, but one may
not be enough

5

A man with a beard and short brown hair, wearing a dark blue suit jacket over a light purple shirt, is holding a large white sign in front of his chest. He is looking directly at the camera with a neutral expression. The background is plain white.

Protect more
than just email

6

CONCLUSION

AI in email security is already essential ... and inevitable

Conclusions

Email attacks have shifted – with new attack methods

AI is essential to detect, disrupt, and stop current and emerging attack methods

Almost all organizations are embracing additive email security solutions

How PhishER Plus Works

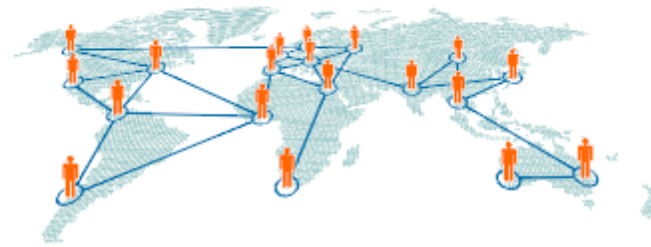


Triple-Validated Human-Curated Phishing Threat Intelligence



Human-Reported

10+ million **Phish Alert Button** users identify and report real-world, active phishing and social engineering attacks to PhishER.



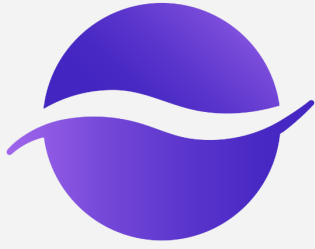
Human-Analyzed

PhishER administrators analyze and review user-reported messages, add them to their private Blocklist and create PhishRIP queries, which is then used in aggregate by PhishER Plus.



Human-Vetted

KnowBe4's Threat Research Lab is a dedicated team of researchers that collect, analyze, and validate identified email threats before adding entries to the Global Blocklist threat feed.



OSTERMAN RESEARCH

delivering insight

Michael Sampson

Principal Analyst

michael.sampson@ostermanresearch.com

Michael Osterman

Founder and Senior Advisor

michael@ostermanresearch.com



Osterman Research



1 206 929 3195 x101



info@ostermanresearch.com



www.ostermanresearch.com



[@OstermanRsch](https://twitter.com/OstermanRsch)

