FORRESTER®

Take Control Of Email Security With Human Layer Security Protection

Human Layer Security Is The Missing Link For Enterprise Email Security Stacks

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY TESSIAN, OCTOBER 2021

Table of Contents

Project Director:
Brett Chase, Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

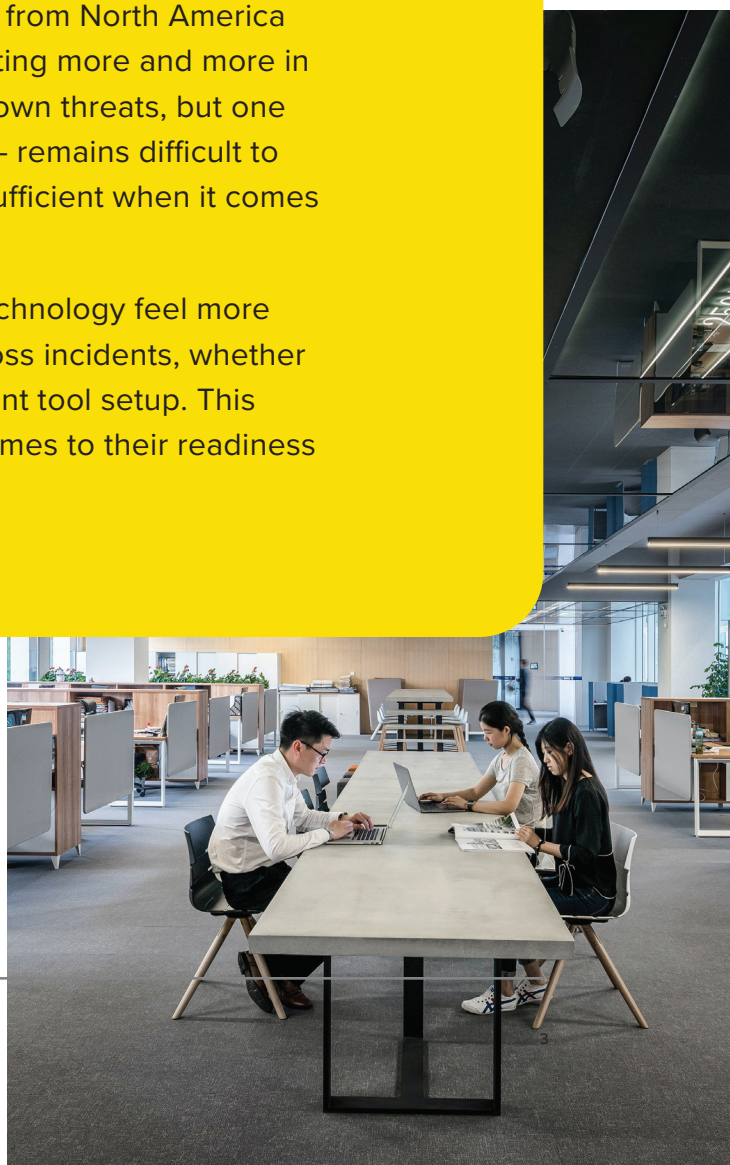
Executive Summary

If data is the lifeblood of a successful business, email systems are the veins through which it travels. Email is every bit as crucial an environment to protect as the network and databases because, once compromised, there can be lasting, costly, and damaging effects. Unfortunately, organizations aren't doing enough to protect this vital business organ and continue to fall victim to malicious attacks, data loss, and exposure stemming from human error. Preventative measures can proactively reduce these threats.

Human layer security is the missing link for today's enterprise email security stacks. It provides much needed protection to mitigate human-based security vulnerabilities and prevent human-centric data breaches via email.

Tessian commissioned Forrester Consulting to evaluate the current state and trends of email security. Forrester conducted an online survey with 317 security and risk leaders in different industries from North America and Europe. The survey found that firms are investing more and more in email security technologies to reduce costly unknown threats, but one of the most critical vulnerabilities — human error — remains difficult to prevent. Current email security postures are not sufficient when it comes to comprehensive email protection.

Organizations that deploy human layer security technology feel more prepared to face email security threats and data loss incidents, whether accidental, negligent, or malicious, with their current tool setup. This demonstrates a higher level of maturity when it comes to their readiness to prevent these damaging threats.



Key Findings

To err is human. Human errors involving email are unavoidable, but how a firm reacts to human errors makes a significant difference in its preparedness for an attack. While organizations understand the dire consequences of threats like accidental sensitive data loss and business email compromise and invest in security solutions, they don't sufficiently address human risk.

Expect the same porous results with your current email security tech stack. Firms leverage many technology solutions and processes to help them manage email security and data loss issues. But many lean on built-in security controls and legacy technologies that are insufficient against human-related threats over email. This is in part because they see human error as uncontrollable — but it's not.

Control the uncontrollable with human layer security. Security and risk leaders look to stay one step ahead of the ever-changing threat landscape as their organizations move toward an uncertain future. Some firms are doing so with human layer security. Human layer security technology leverages machine learning and artificial intelligence (ML/AI) capabilities and uses behavioral intelligence to mitigate human-centric security vulnerabilities, so organizations can stop data breaches before they happen via email. This improves customer trust and employee experience, leading to greater protection and increased revenue. Human layer security solutions are necessary to achieve the full value of existing security tech stacks in a way that empowers employees while achieving maximum protection.

Security And Risk Leaders Seek To Improve Email Security

Email is a communications mainstay due to its ubiquitous nature. It is also a potential source for data breaches — intentional and unintentional. Traditional security solutions, such as secure email gateways (SEGs), legacy data loss prevention (DLP) software, and built-in email security controls, have inherent limitations and fail to solve for risks. According to Forrester Research, global security decision-makers reported that 31% of their organizations' external data breaches involved phishing attacks in 2021.[1] To assess the current state of email security further, we surveyed 317 security and risk leaders and found that:

- **Firms are pursuing improvements.** Security organizations are laser focused on enhancing data loss prevention capabilities, improving email security strategies, and reducing human error risks, as they should be. Accidental data loss and business email compromise are the most common cybersecurity incidents. Nearly half of respondents reported that their organizations experienced these incidents in the past year even though traditional security solutions are deployed in these organizations. Additionally, employee mistakes caused roughly a third of incidents related to phishing attacks, accidental data loss, and noncompliance. Our survey found that, depending on the company size, organizations experienced between one and 50 employee-related email security incidents per month on average with nearly 40% reporting at least 10 or more incidents per month. As a result, organizations spent up to 600 hours per month resolving employee-related email security incidents. Interestingly, larger enterprises with 20,000 plus employees reported experiencing more accidental data loss, sensitive data exfiltration, intellectual property theft/insider threat, and data breaches (see Figure 1).

Figure 1

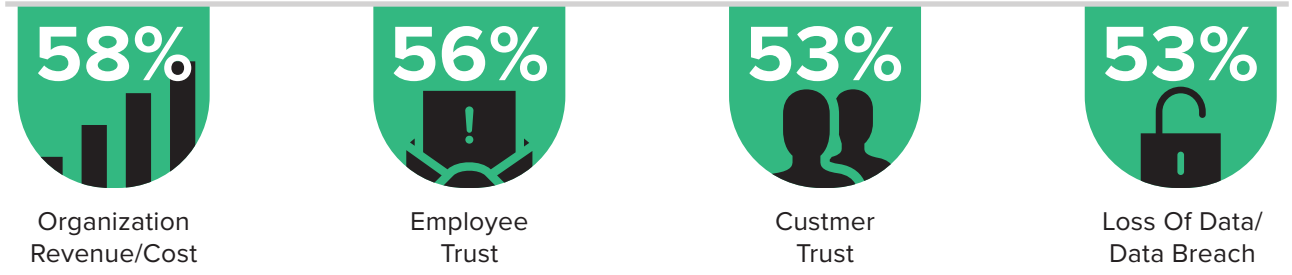
Percentage Of Employee-Related Email Security Incidents By Company Size

Base: 290 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity and experienced employee-related email incidents
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

- **Doing nothing is not an option.** Addressing these vulnerabilities was among the top priorities for surveyed security and risk leaders over the next 12 months because email-related security incidents can have a lasting impact on organizational revenue/cost, employee trust, and customer trust (see Figure 2).

Figure 2

Email Security Incidents Impact These Areas Of Business



Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

Traditional Approaches Are Fraught With Weaknesses

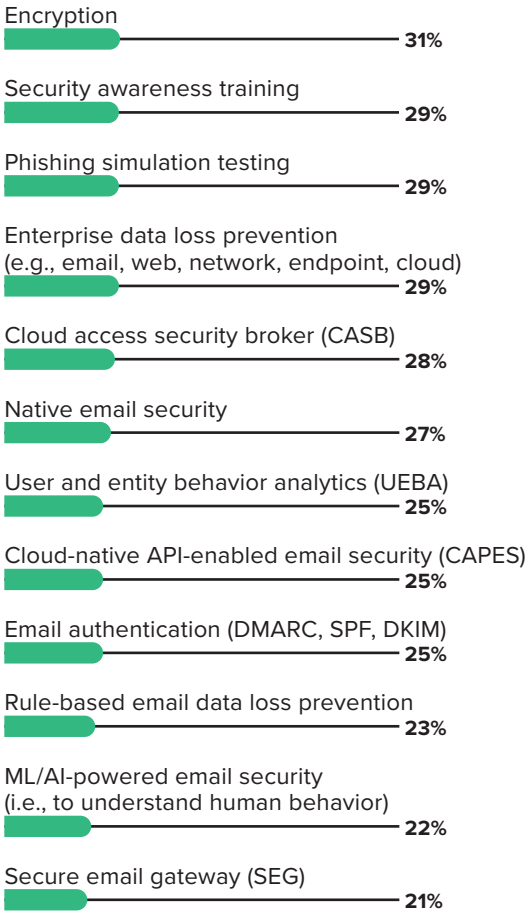
Security and risk leaders seek security improvements even though most feel their organizations have go-to resources for preventing human error risks over email. These resources included traditional security solutions (see Figure 3). They also included reactive methods, such as deploying sandboxes to analyze inbound threats and leveraging security ops teams to triage incidents (see Figure 4).

EMPLOYEE BEHAVIOR — INTENTIONAL OR UNINTENTIONAL — IS WEAKENING EMAIL SECURITY

- 61% of security and risk leaders believed that an employee's actions will cause their organizations' next data breach.
- 63% of security and risk leaders believed hybrid work environments will make human-activated threats more prevalent due to an increase in difficulty communicating in real time and an inability to ask for support when needed. Security and risk leaders also reported their organizations have less visibility into employee behavior and that data may be compromised more easily as employees move in and out of different networks.
- 48% of security and risk leaders said human error-caused security incidents will increase in the next year.
- Employee mistakes cause roughly a third of security incidents in organizations.
- Accidental data loss was the leading cybersecurity incident in the past year.

Figure 3

Technologies Used To Prevent Security And Data Loss Risks From Employee-Related Email Incidents

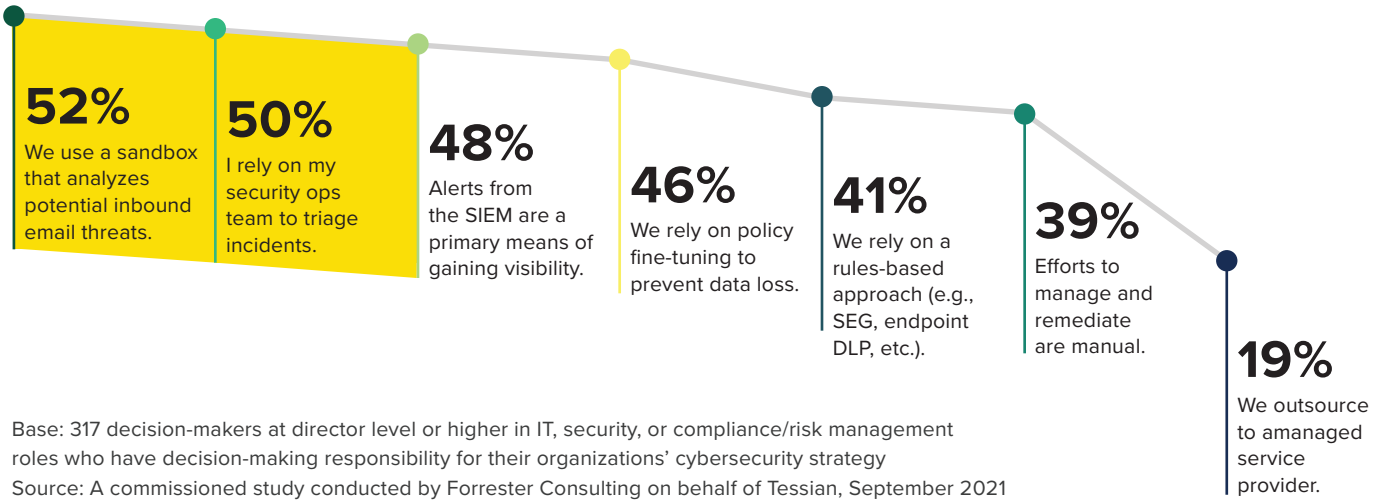


Base: 317 decision-makers at director level or higher in IT, security, or compliance/ risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

Figure 4

"What security methods do you currently rely on to manage and remediate potential inbound threats and outbound data loss caused by human error?"

(Select all that apply.)



Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

A TECHNOLOGY-CENTRIC SECURITY APPROACH LEAVES OUT HUMAN ELEMENT

Despite email security efforts, security controls are ineffective and porous. Two-thirds of security and risk leaders said email is the most susceptible to security incidents caused by human error. Over 75% of respondents reported that 20% or more of email security incidents get past their organizations' existing security controls. Roughly one-quarter reported that 21% or more of their organizations' employees have failed a phishing test in the past year (see Figure 5).

Overall, maximum phishing failure rates hover around 50%, and these mistakes can have dire consequences. According to Forrester Research, the phishing email itself is usually just the beginning of an attack and opens the door to others like credential phishing which leads to credential theft.[2]

Traditional security solutions have inherent limitations when it comes to solving for risks posed by people.

A Forrester survey reported that 44% of global security decision-makers who experienced a breach in the past 12 months listed authentication credentials as a type of data potentially compromised by that breach.[3]

Over a third of survey respondents reported their organizations' spent excessive time and unnecessary effort on triaging, investigating, and resolving incidents with traditional email security solutions. These lapses in email security are due, in part, because many respondents' organizations (45%) reported relying on independent phishing simulations for security awareness training vs. real-time (or in-the-moment) employee education that prevents risky behaviors in the context of real emails. As a result, security and risk leaders felt they have little control over the risks employees pose. Nearly three-quarters believed human-activated threats are the most challenging to prevent; one-third reported their organizations lack visibility into threats and risky behaviors.

As such, security and risk leaders remained concerned about defending their organizations against risks, such as accidental data loss and phishing attacks, demonstrating how traditional security solutions have inherent limitations when it comes to solving for risks people pose.

Figure 5

Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

Gain Control With Human Layer Security For Email

A holistic email security strategy must not only include tools and technologies, but human-centric solutions and processes as well. To achieve this level of maturity, many of the surveyed leaders reported their organizations are taking steps to improve the security of their human layer (see Figure 6).

Figure 6

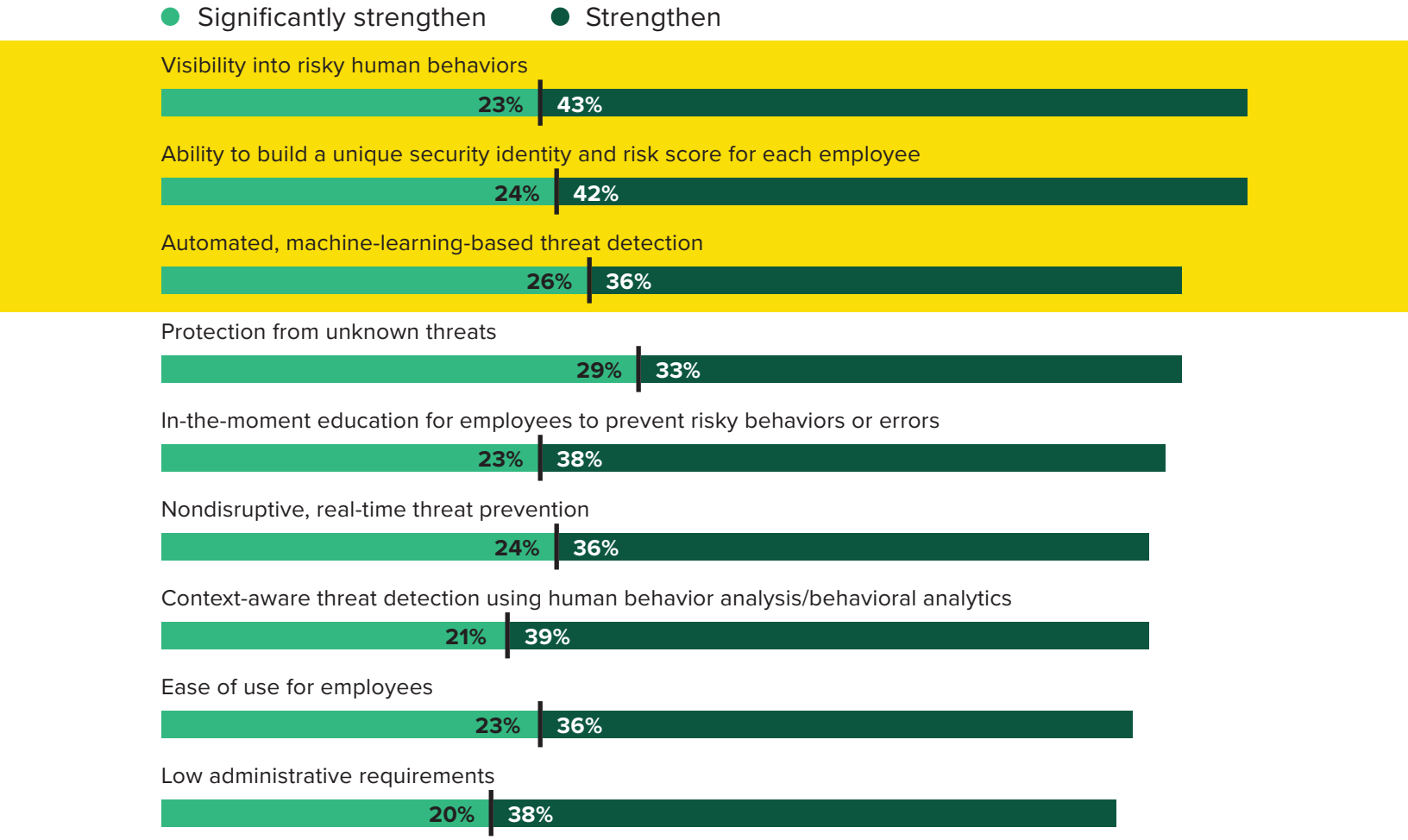
Steps Taken To Improve Security And Prevent Security Incidents

Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

To improve their email security and data loss prevention posture, security and risk leaders reported specifically seeking solutions that allow their organizations to gain visibility into risky human behaviors and build unique security identity and risk scores for each employee. They then want to use this information to feed automated, ML-based threat detection systems to predict and protect against unknown threats (see Figure 7). Firms can take advantage of their own insights-rich email data and leverage machine learning capabilities, which are core to a human layer security solution, to predict and prevent risky behavior, build valuable intelligence, and take a human-layered approach to email security.

Figure 7

"To what extent would each of the following functional capabilities impact your organization's email security and data loss prevention and minimize future risk?"



Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

Human layer security technology allows organizations to stop data breaches before they happen via email. This tech uses ML and AI, along with behavioral intelligence, to mitigate human-centric security vulnerabilities.

Security and risk management leaders that reported using human layer security technology applied more of an employee-focused mindset when it comes to security. Security and risk management leaders have a heightened awareness of the risks that their employees can cause and, as a result, understand that lower friction leads to greater security. For example, over two-thirds of human layer security technology users believed the easier their functional security capabilities are for their employees, the better their firms can fight against future risks and data loss.

We found that the security and risk leaders that took a more human-layer approach to their organizations' email security strategy feel more prepared to face security and data loss incidents with their current tech stack than those who haven't. They believe their organizations' email security posture is extremely effective at alerting the organization to potential attacks and threats from users' risky behaviors or poor security decisions. Meanwhile, those who don't take a human layer approach felt less control over business disruptions (see Figure 8). Human layer security solutions are necessary to achieve the full value of existing security tech stacks in a way that empowers employees while achieving maximum protection.

Figure 8

Are Current Email Security Setups Effective?

Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

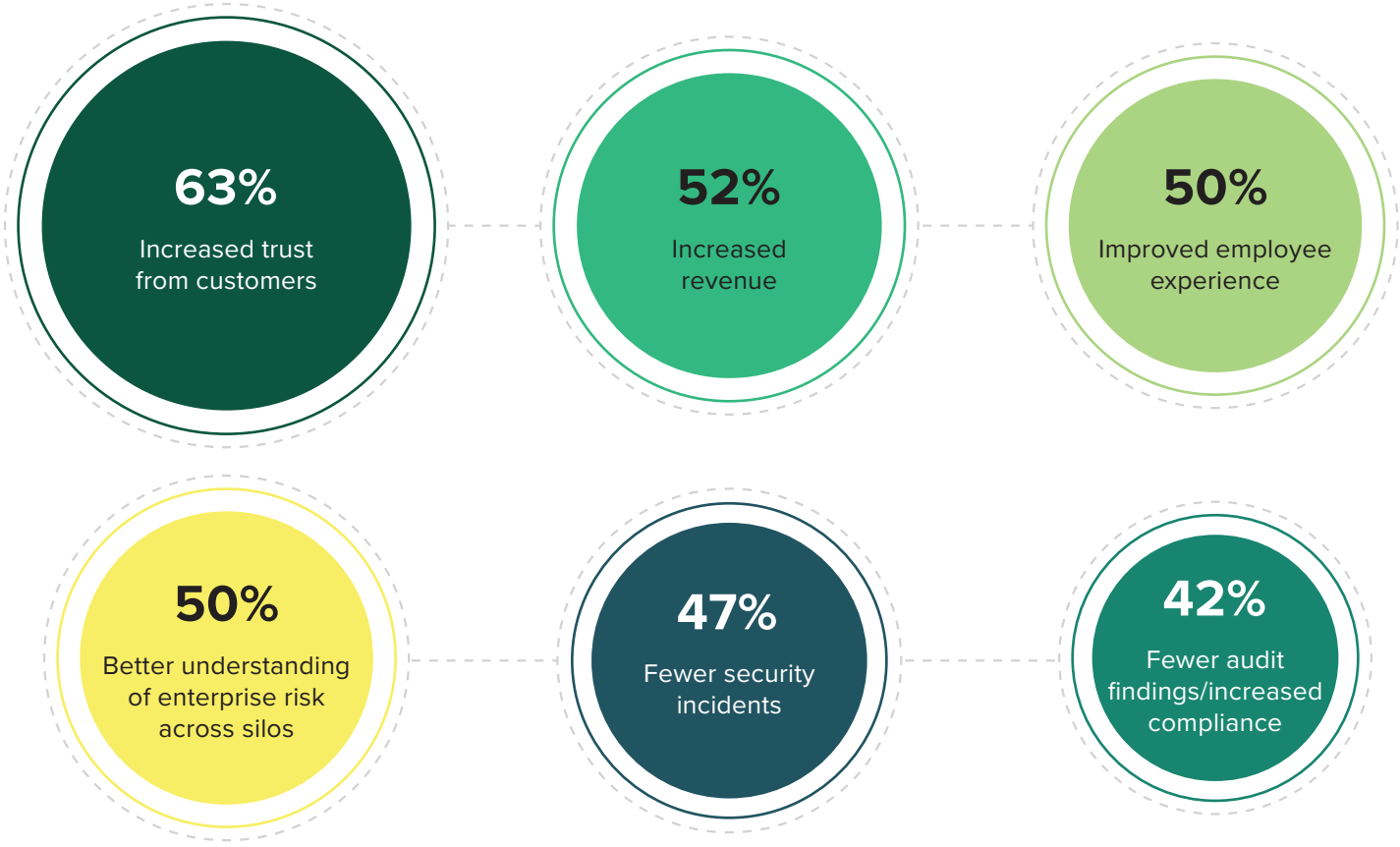
There's significant upside to an enhanced email security posture. Email security improvements will not only help firms avoid costly human activated security threats, but security and risk leaders expect they will also increase customer trust, increase revenue, improve employee experience, and provide a better understanding of enterprise risk across team silos (see Figure 9).

Human layer security sets organizations up for email security success with a focus on in-the-moment security coaching and preventative technology.

Figure 9

"What benefits would you expect to experience from improved email security and data loss prevention capabilities?"

(Select all that apply.)



Base: 317 decision-makers at director level or higher in IT, security, or compliance/risk management roles who have decision-making responsibility for their organizations' cybersecurity strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Tessian, September 2021

Key Recommendations

For many business professionals, email is the first thing they look at in the morning and the last thing they see at night. It is a vital component to everything in business from daily workflows to annual strategy planning. Unfortunately, email security and data loss prevention tech stacks and strategies are incomplete as threats like phishing, business email compromise (BEC), accidental data loss, and insider threats still plague most firms today. Additionally, these threats will likely get worse in the future. This demonstrates the current business need to embrace more modern security approaches like a human layer security platform that takes a behavioral approach and understands context to detect known and unknown threats and provide greater peace of mind.

Forrester's in-depth global survey of security and risk decision-makers yielded several important recommendations:

Assess current capabilities.

Work with your teams and those in the organization on the front lines of employee experience (e.g., tech support, help desk, project managers, product managers) to understand how workers complete tasks and communicate and how effectively current solutions safeguard data in those actions. These workflows should uncover areas that are vulnerable to human error and where to focus additional training and resources.

Invest in email security technology wisely.

Defense in depth is often conflated with expense in depth and the perception that an environment is more secure than it is. This check-the-box approach does not replace a thoughtful review of the related processes and controls that must also be in place to ensure an email security technology solution is working as intended and reducing risk to the organization. Consider automation and machine-learning technology, which can help you stay one step ahead of constantly evolving social engineering attacks and predict threats from employee actions by understanding human behavior. Additionally, automation can significantly reduce resource hours for security teams spent in triage and investigation and lower ongoing administration.

Put people first when it comes to email security.

Organizations that focus on human layer security outcomes are best positioned to select and deploy the most effective balance of security technology solutions. As these security incidents arise, consider providing contextual in-the-moment coaching that improves your employees' security awareness level and helps them make the right decision in real time. This approach provides the advantage of applying advanced human layer security technology in an integrated and complementary manner with traditional security solutions, resulting in greater overall protection and, for employees, the perception of empowerment and confidence instead of roadblocks and confusion.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 317 security strategy decision-makers at organizations in the United States and the United Kingdom to evaluate their email security posture. Survey participants included decision-makers in IT, security, and compliance/risk management. Questions provided to the participants asked current email security setup, challenges firms experience with their email security, and future-state aspirations. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in August 2021 and was completed in September 2021.

Appendix B: Demographics

COUNTRY	
United States	**51%**
United Kingdom	**49%**

ROLE	
IT technology/infrastructure leader	**24%**
Information security leader	**13%**
Data protection/data integrity leader	**11%**
Governance, risk, and compliance leader	**9%**
CISO/CIO/CSO	**9%**
Security operations and control leader	**9%**
Data protections officer	**8%**
Identity and access management leader	**6%**
Security awareness and training leader	**5%**
Chief technology officer	**5%**
Chief risk officer	**3%**

COMPANY SIZE	
500 to 999 employees	**9%**
1,000 to 4,999 employees	**40%**
5,000 to 19,999 employees	**32%**
20,000 or more employees	**19%**

SECURITY TOOLS/PROTOCOLS	
Data loss prevention	**100%**
Email security	**100%**
Firewalls	**83%**
Mobile device management	**79%**
Endpoint protection	**79%**
Antivirus	**60%**
VPNs	**42%**

Appendix B: Demographics (continued)

INDUSTRY	
Healthcare	**16%**
Technology and/or tech services	**16%**
Professional services	**16%**
Manufacturing and materials	**17%**
Financial services and/or insurance	**17%**
Other	**17%**

DEPARTMENT	
IT/security	**60%**
Compliance/risk management	**40%**

LEVEL OF RESPONSIBILITY	
Final decision-maker for security and risk management strategy	**57%**
Part of a team making security and risk strategy decisions	**34%**
Influences decisions related to security and risk management strategy	**9%**

RESPONDENT LEVEL	
Director	**46%**
Vice president	**33%**
C-level executive	**20%**

Note: Percentages may not total 100 because of rounding.

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

“The Forrester Wave™: Enterprise Email Security, Q2 2021,” Forrester Research, Inc., May 6, 2021.

“Now Tech: Enterprise Email Security Providers, Q3 2020,” Forrester Research, Inc. July 14, 2020.

Appendix D: Endnotes

[1] Source: Forrester Analytics Business Technographics® Security Survey, 2021.
[2] Source: “Best Practices: Phishing Prevention,” Forrester Research, Inc., September 30, 2019.
[3] Source: Forrester Analytics Business Technographics® Security Survey, 2021.


FORRESTER®