mimecast

MAXIMIZING MIMECAST

Protect your organization across email, collaboration, compliance, and human risk

CONTENTS

02 **The Evolving Cybersecurity Landscape:** AI's three-pronged role in protection
Rob Juncker

03 **Behind the data:** The power of human risk management
Masha Sedova

05 **Responding to new threats:** 9 innovations focusing on rapid innovation to stay one step ahead
Marc Amphlett

07 **The inside scoop on insider risk:** How smarter AI and targeted controls are transforming data protection
David Capuano

09 **Empowering employees:** Redefining security culture with personalized training
Masha Sedova

11 **Beyond archiving:** Turning compliance and data governance into valuable insights
Matt Pasternack

THE EVOLVING CYBERSECURITY LANDSCAPE: AI'S THREE-PRONGED ROLE IN PROTECTION

Security teams are overwhelmed: too many alerts, not enough staff, and mounting pressure to keep organizations safe amid constant change. The Mimecast platform is designed to simplify and strengthen security by focusing on both technology and human behavior.

ROB JUNCKER Chief Product Officer, Mimecast

Understanding human risk in a hyper-connected world

Industry thought leaders emphasize that cybersecurity today is as much about people as it is about technology. Forrester, for instance, highlights the importance of tracking and influencing employee behavior – nudging users toward safer actions, adjusting access, and escalating issues when needed. Gartner, meanwhile, underscores the need for solutions that secure not only email but also collaboration tools like Slack and Teams, integrating seamlessly with an organization's existing security ecosystem.

Mimecast's approach addresses both perspectives: a robust platform that detects and intervenes in risky behavior, while also plugging directly into hundreds of existing security tools. The goal is to offer an environment where security is "just add water," focusing on the human element without disrupting established workflows.

AI: A game changer for attackers and defenders

Artificial intelligence has upended both the threat landscape and the defensive strategies required to stay ahead. Attackers now wield AI-powered tools – like WolfGPT and FraudGPT – to create highly personalized, targeted phishing campaigns. The days of crude, generic scams are over; modern attacks are sophisticated, leveraging personal and organizational context to deceive even vigilant users.

Mimecast's own data reveals the scope of this shift. When ChatGPT emerged, AI-generated emails quickly rose to 3% of all messages analyzed in 2024. By 2025, that number soared past 10% and continues to grow. In response, Mimecast developed proprietary engines to detect not just AI-generated content, but the intent behind each message, distinguishing benign automation from malicious manipulation.

Protection from AI, for AI, and by AI

Mimecast frames its new capabilities around three core concepts:

- **Protection from AI:** First, we focus on defending organizations against AI-powered attacks by identifying novel threats before anyone falls victim. Multi-vector threat protection analyzes a variety of signals – sender reputation, behavioral anomalies, and more – to intercept malicious campaigns early, fundamentally changing the industry's traditionally reactive approach.
- **Protection for AI:** As businesses leverage AI for productivity, new risks emerge, such as data leakage to external AI platforms ("shadow AI"). Mimecast proactively blocks the exfiltration of sensitive data, ensuring that organizational "crown jewels" remain secure even as users experiment with generative AI in their workflows.
- **Protection by AI:** Mimecast uses AI within its own defenses, continually evolving its detection engines and automating remediation actions. From real-time user nudges to advanced account takeover protections, AI is woven throughout the platform, enabling faster, more precise responses to emerging threats.

Mimecast's solutions are designed to fit seamlessly into existing security environments, with over 350 integrations with partners. This means organizations can leverage Mimecast's insights and remediation capabilities without disrupting their current workflows. To learn more about the platform and roadmap, contact your Mimecast representative.

BEHIND THE DATA

The power of human risk management

Masha Sedova, Vice President, Human Risk Strategy, Mimecast

As a cybersecurity company securing millions of users, we're constantly delving into data, looking for patterns that will help customers protect themselves from being the subject of the next breach. Our team conducted a data-mining exercise – and we were shocked by the results. We analyzed a data set that had millions of data points detailing the security behaviors exhibited by 300,000 employees across a vast global network of organizations large and small in a wide variety of industries.

The data showed that just 8% of users caused 80% of the security incidents that we were tracking. This was eye-opening. How can so few people be the focal point of so much disruption?

For our team, this small piece of data unlocked a significant opportunity. If we could help our customers identify those 8%, we could change the way they manage risk inside their organizations!

Closing the visibility gap and quantifying human risk

When we think about the user element of our organizations, we understand that every employee is unique, but traditional tools are unable to provide insight on actual behaviors. We knew the applications that were installed on devices and which sites they visited. But we didn't know which employees are targeted, what risky behaviors they engage in, or what data is shared with whom.

Quantifying human risk is similar to the way you would quantify someone's credit score or driver's insurance rates: You take data points and map them to specific behaviors. In security, those behaviors fall into three categories:

1. ***Behavior patterns.*** *Do they make good decisions or bad decisions? Do they open suspicious links? Do they share information over secure channels?*
2. ***Attack factor.*** *How frequently are they in the crosshairs of attackers?*
3. ***Business risk.*** *What role do they play in the organization? What access does their role include? And how do they handle the data they have access to?*

If an organization treats all its employees with a one-size-fits-all training program, it's missing the mark. Organizations need to understand where that risk distribution is and start adapting their policies appropriately.

Who's being attacked – and why

Looking at the attack factor produced another insight from our research. We saw that not everyone gets attacked with the same frequency. Overall, 36% of users were not targeted with phishing attacks in the time that we were analyzing this data. The median phishing rate was about six per year. But there were a small number of employees (4%) that received more than 100 phishing attacks a year.

Who are these people? And why are some getting targeted more often than others?

Turns out, managers are twice as likely to get phished than an individual contributor. We also found that managers received 2.5 times more volume of phishing attacks than individual contributors. The phishing risk also grew as employees gained more experience. Every three years an employee spent in an organization, the phishing rate doubled.

Our research also showed that risk varied by department. Customer service led the pack, with a whopping 22% of employees experiencing at least

one high-risk event. It actually makes sense because these people are out on the front lines: Their job is to engage with customers and make every effort to solve customers' issues. So, they're more apt to open themselves up to risk in an effort to be helpful.

Historically, when security companies thought about quantifying human risk, they focused on developing the right questions to ask and the right ways to simulate a threat environment. What we've learned is that when we look at real data, we can paint a much more robust picture of the actual risks that exist inside organizations. So, we can track behavior events, the kind of insider role that employees have, their attack levels, and their security knowledge.

Once we have this level of visibility, it opens a world of opportunities. Organizations can address the risky behavior directly, by assigning training programs more thoughtfully and with higher precision. They can also provide users with real-time nudges at the time of the risky action rather than weeks later in regularly scheduled training. Beyond empowering the user, admins can also automatically adjust their controls and adjust their access. And when necessary, escalate situations appropriately to HR.

These interventions aren't all created equal. In fact, these interventions layer on top of each other with levels of maturity.

From insight to action

If a leader fires somebody who's repeatedly clicking on links, it's not necessarily going to keep the organization safe. What it will do is create a severe business impact when that person is no longer able to contribute. Training adds a certain amount of protection, and while not the whole solution, it is minimally disruptive in terms of business impact.

The level of attention an organization can apply should increase as risks expand. Most people inside an organization should receive baseline training to help them understand basic security practices. For riskier employees or departments, organizations can consider more aggressive tactics including adding controls, adjusting access, and limiting the ways they move data in the environment. A broader menu of options means organizations aren't limited to the options of either heaping on more training or firing somebody.

Inside the Human Risk Command Center

The Mimecast Human Risk Command Center puts this process into practice. It quantifies human risk by assigning scores for each employee's risk profile, from zero to 10 – zero being no risk, 10 being very risky. For every behavior, an organization can drill in and see insightful data sets about who's doing what.

The Mimecast Human Risk Management platform offers watch lists that can dynamically move users into groups based on risk criteria. Preventative controls can be placed for the most heavily attacked and very high-risk users.

Every employee is different. So why treat them all the same? Adaptive protection means tailoring security to each individual – meeting them where they're at and providing them the right level of support and control.

We also understand that our customers rely on a variety of solutions to protect their entire digital estate, so the Mimecast Human Risk Management Platform offers integrations with leading cybersecurity vendors. This means customers get visibility into human risk in their organization based on data from not just email and security awareness training, but also risk data from endpoint security, DLP solutions, identity and access management systems, and more. For the full list of Human Risk integrations, visit the integrations hub.

The way this looks in practice is that it meets every employee at their risk level, maximizing their productivity while reducing security incidents. So, our low-risk employees, who are doing the right thing and rarely clicking, are getting positive reinforcement. They have basic security controls that minimize friction and maximize their productivity output. Our occasionally risky individuals get nudges and course corrective action to get back on track. With a few reminders and slightly escalated controls, they're back to making good decisions.

And then our high-risk individuals – those who are willfully negligent or occasionally malicious – will have security controls in place to help the organization respond and recover appropriately to that level of risk.

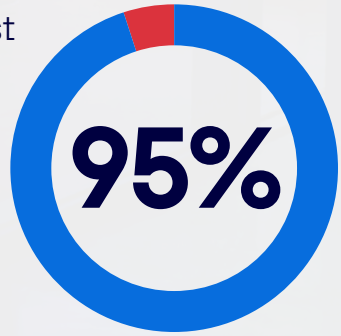
When you understand human risk, you can measure it, manage it, and most importantly, reduce it. That's the power of human risk management.

RESPONDING TO NEW THREATS

9 innovations focusing on rapid best practices to stay one step ahead

Marc Amphlett, Senior Director, Product Management, Mimecast

Our data suggests that while over 95% of malware attacks still come through email, the skyrocketing popularity of collaboration apps is opening up a new attack surface for hackers to exploit. Tools like Slack, Teams and Zoom are frequently used to share sensitive company information. Most are also integrated tightly with cloud email platforms, so a vulnerability in one tool can open a pathway for criminals to move across the enterprise and steal valuable data.



of malware attacks still come through email

As email and collaboration threats evolve, Mimecast is responding by developing next-generation protection to strengthen both of these environments. We're building on more than two decades of email security by adding new capabilities such as account takeover protection, multi-vector threat protection, and URL pre-delivery scanning.

Here is a look at nine new capabilities and best practices to configure and manage your email and collaboration security today. These steps will ensure you're protecting your organization from evolving threats, driving towards resilience, and building a more secure culture along the way.

1. The Human Risk Command Center

If you've already implemented Mimecast email security and collaboration protection, you have access to the Human Risk Command Center. Now is the perfect time to explore this powerful tool. The Human Risk Command Center draws data from all Mimecast products, and even when used just with email security it provides significant immediate value. You can identify your most attacked users, gain insights into the specific risks targeting them – including malware and phishing attempts stopped before reaching their inboxes – and use this information to make smarter decisions about prioritizing protection within your organization.

2. URL Pre-Delivery Scan

Email security is evolving, and Mimecast is leading the charge with a fundamental shift in how we protect your organization from URL-based threats. We've recently released URL Pre-Delivery Scan – a capability that transforms our approach from reactive protection to proactive defense.

When users click suspicious links, they are blocked. The technology works as designed. Yet users keep reporting "suspicious emails" in their inboxes, frustrated that potentially dangerous messages made it through in the first place. This perception gap matters. When employees lose confidence in their email security, they ignore legitimate warnings or develop workarounds that introduce new vulnerabilities.

URL Pre-Delivery Scan brings the full power of Mimecast's multi-step URL inspection pipeline to bear before emails reach any inbox. This targeted approach delivers comprehensive protection without compromising the performance your organization depends on.

3. Account takeover protection

One of the most dangerous threats companies and individuals face is an outright takeover of a corporate account. Once an attacker gains control, they steal money, commit fraud, and gain access to other accounts.

Mimecast has launched account takeover protection, a new feature that spots what's happening in a particular account and gives options for how to circumvent a problem. The Account Takeover module complements existing security layers, detecting signals of compromise to flag suspicious accounts.

Security teams can take proactive actions based on patterns of use, or they can take action in the moment to stop a potential takeover in progress. Depending on the assessment of the threat, they could hold a user's emails, reset the user's password, remove access to their administrative resources, or potentially take away their corporate resources. Using capabilities from across the Mimecast Human Risk Platform, the team can take action based on the person's role, their security history, or other factors that contribute to a risk evaluation.

4. Multi-vector threat protection

The threat landscape has changed dramatically since the days of traditional malware and spam. Attackers have evolved and are aware that they can bypass single point detection. To combat these growing threats, security vendors need to evolve as the threats do. Multi-vector threat protection is new cloud-based detection technology that takes all of the elements from Mimecast's existing scanning layer, correlates them, and puts together a holistic view on whether a message is malicious or not.

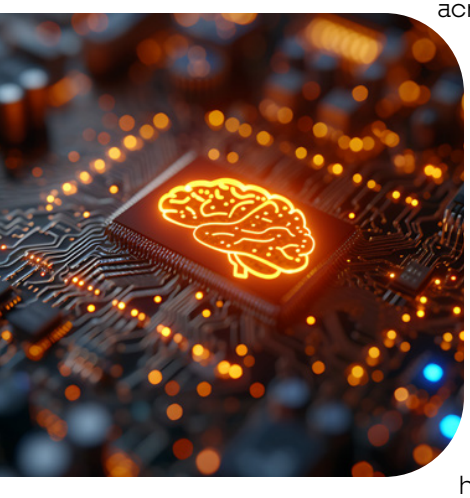
Multi-vector threat protection defends email and collaboration suites against cyber threats such as phishing, impersonation attacks, malware, and AI-generated attacks. It uses a multi-layered approach with features like URL Protect, Attachment Protect,

and Impersonation Protect to stop threats before they impact users, and also includes capabilities for internal threats and data protection. Think of Multi-vector as the conductor at the last stop on a train ride announcing whether a message is safe or not.

An additional benefit it provides is a detailed analysis about decisions involving email threats. It applies multiple indicators, including sender reputation, sending email, suspicious content patterns, and brand impersonation like a Microsoft credential harvesting site. This makes it easy for a helpdesk, CISO or security expert to explain why the multi-vector detection engine flagged a particular message.

5. Mihra AI

In recent years AI has impacted the security industry in many important ways – enhancing detection analysis, automating administrative functions, and powering sophisticated video analytics. Mimecast has introduced a number of AI capabilities into its platform, focusing heavily on human risk management across email and collaboration tools.



Now we're adding new functionality – the ability to interact with email using AI. Using the Mihra AI (Mimecast Intelligent Human Risk Agent) interface, customers will be able to ask the tool to compile a list of risks occurring in their organizations, analyze those risks and explain how those are being targeted. They can ask which accounts they have access to and compile results for a period of time based on certain aspects of risk. Mimecast is delivering a variety of Mihra AI agents that make your work easier and make you more efficient.

6. Human Risk Insights Report

Reviewing the Human Risk Insights Report is essential for any organization aiming to clearly understand and communicate its security posture. Today, the conversation about cyber threats is happening at the highest levels, and security leaders are expected to not only identify risks but also to quantify and contextualize them for stakeholders and board members. With the Human Risk Insights Report, you gain instant visibility into the entire threat landscape your organization faces – including the specific types of attacks targeting your users and how Mimecast is actively blocking threats like phishing and malware. The report drills down even further, offering details on vulnerabilities (CVEs) relevant to your environment and comparing your risk exposure to similar organizations in your industry and region. This empowers you to validate your security investments, demonstrate the value of your protective measures, and make data-driven decisions to further reduce risk.

7. AI-powered similarity modeling

Another recent innovation that Mimecast has rolled out to its Mimecast Email Incident Response (MEIR) customers is the ability to identify related threats through similarity modeling. The feature inside our impersonation protect service uses AI models to detect and block advanced threats by identifying domains that are similar to a customer's internal or trusted domains. It works by checking the "similarity distance" between sender and recipient domains, compiling a Similarity Score based on information in the email body, subject, attachment name and sender. It identifies look-alike domains and ignores communications from domains that have been put on a safe list. This capability enables analysts on the Mimecast team to take action for MEIR customers by automatically warning users or blocking access to the link.

8. Graymail policies

Graymail is another name for bulk email solicitations like newsletters or advertisements that users no longer wish to receive. Mimecast has made updates to its graymail management configurations, including graylisting, which rejects emails from unknown senders but then accepts them later if the sender establishes itself as legitimate. Based on early reports, the upgraded protocols are successfully removing more than 300 emails per user out of their inboxes per month.

9. Evolving our QR code defenses

Many organizations are being disproportionately attacked by phishing attempts using QR codes embedded in PDF documents. For years QR codes typically showed up in normal formats that were easy to spot, but today's attackers have gotten smarter. As vendors have rolled out QR code detection, attackers have evolved, and QR codes now show up as multiple separate images that can be merged together on a screen. In one recent case, an employee received a QR code that was seven levels of images stacked on top of each other to deliver a QR image hidden beneath. Through advances in image detection and with the QR code work we've done allowing us to gain more insight into URLs, Mimecast has sharpened its ability to flag these QR codes and shield customers from damaging incidents.

A future-ready platform

At Mimecast, our commitment to innovation goes beyond catchy product names or hype. We've made a fundamental shift to become an AI-first organization—embedding advanced artificial intelligence across our platform to deliver real protection from AI-driven threats, for your AI initiatives, and now, enabling you to bring your own AI capabilities into the equation. This approach means every Mimecast product moving forward will harness the combined power of our robust security expertise and flexible AI integrations. As we continue to evolve, Mimecast is not only providing the tools to keep pace with emerging threats but also empowering you to leverage AI safely and effectively in your own environment. The result is a future-ready platform designed to protect, adapt, and grow with your organization's needs.

THE INSIDE SCOOP ON INSIDER RISK

How smarter AI and targeted controls are transforming data protection

David Capuano, Vice President, Product Management, Mimecast

Data is the lifeblood of business today – and it's leaving organizations in droves, often unintentionally, but sometimes maliciously. The threats aren't always coming from outside. More are coming from employees who are sitting in offices, logging into systems, and walking out the door when they leave for other jobs.

Whether through mistakes handling data or by outright stealing, insider risk is growing and it's impacting some of the most innovative companies in the world. Insider risk can derail a company's progress, harm its reputation, and cost real money.

So, the question for leaders to ask isn't whether their company is at risk from insiders. Rather, they should be asking themselves: Am I prepared to detect it, to deter it and to defend against it?

Data risks are becoming more frequent. In one recent survey, it was revealed 60% of users in mid-size enterprises admitted to transferring files to personal locations. That's just the number that admitted to moving files in an unauthorized manner. The true amount could be much higher.

Data risks involving insider threats are also impacting more organizations: 1 in 3 data breaches involve insiders. And they're evolving: 86% of security leaders fear employees leak data to GenAI tools.

To protect data from leaking, there are key technology considerations organizations should keep in mind.

Eliminate blind spots

Organizations need unparalleled visibility. They need to see where data is moving in their environment, and you need to do that from a user perspective across endpoints, cloud platforms, and email. That means knowing whether people are uploading content to their personal cloud accounts or GenAI apps, or whether they're sharing company materials over Slack, Teams, or WhatsApp.

Mimecast's technology tracks all those data movements and applies a set of scoring algorithms to help companies make risk-based decisions. Was the act accidental, was it behavior-based or was it malicious? Once organizations develop a picture of that risk, they can apply the appropriate response based on what the risk is.

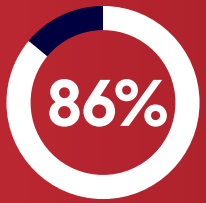
The goal is not to alienate employees, and not to be a mechanism to overwhelm your security analysts. It's really to change cultural behavior and get employees to be stewards of handling data and information.

That's where Incydr, Mimecast's data protection solution, can help. Our mission is to provide organizations a way to proactively manage what's happening from an insider standpoint and prevent accidental data loss by applying the appropriate controls to those users who are not acting maliciously. We want to do it in a way that doesn't disrupt innovation and doesn't overwhelm security teams.

When security teams start with a block-first mentality, it often creates two problems. Employees

DATA RISKS ARE BECOMING MORE FREQUENT

of users in mid-size enterprises admitted to transferring files to personal locations.



of security leaders fear employees leak data to GenAI tools. 1 in 3 data breaches involve insiders.

are clever and they're motivated to get work done, so they find workarounds, which opens the organizations up to new sets of threats. The other issue: Too much brute force blocking can end up keeping employees from accessing tools that they need to perform important tasks.

With Incydr, we can tailor block-and-response strategies based on what the organization sees from a threat standpoint. That can involve setting up targeted notifications or sending micro learning training clips in the moment. Organizations can build controls for low and moderate responses while blocking access to certain browsers or preventing workers from using incognito mode.

Identifying data leaks

Looking at the attack factor produced another insight. Our customers must protect against two principal kinds of employee data leaks. The first is unintentional. One customer described a situation where a well-intentioned finance employee decided to bring her work laptop to the hospital. During her overnight stay, she transferred documents using her personal gmail account and exposed sensitive materials to a public network.

The other variety is intentional. In another incident, an HR employee who had accepted a job at a competitor tried to pilfer a list of employee names and salaries as they prepared to leave the company. This information is valuable. At their new job, the data thief could have leveraged the salary data to poach former colleagues for his new company. But the theft was unsuccessful. Tracking tools detected the transaction, and security prevented the departing employee from leaving with the files.

The never-ending chase for visibility

While it's been said that data is the new oil, at its core it behaves like water. If there is a way for it to leak out of an organization, it will. Hackers continue to get smarter. Corporate information systems get more complicated to operate. And employees take more chances with the data they come into contact with.

To protect against data theft and data leakage, organizations need to see every path data travels – coming in, going out and moving around the organization. Incydr has more than 400 risk indicators inside the product set, and powerful AI helps categorize both known and unknown sources and destinations to help categorize unknown destinations to provide context to users.

Taking action with preventative controls

The times when organizations need to exercise the strictest controls over their data sharing are when employees are getting hired and when they're leaving their jobs. It's critical that organizations spell out clearly what employees' responsibilities are during these times. We're making it easy to get a handle on how data moves by introducing preventative controls that address everything from pop ups to blocking the use of incognito mode. We've augmented those with integrations into Crowdstrike, Okta, Microsoft Entra, and other applications, in case organizations want to take advantage of some of the capability sets that are already in their security stacks.

Companies want to apply uniform controls across their entire organization. We'll be rolling out destination blocking, allowing organizations to prevent data from going to specific sites, and we're also going to introduce a tag base blocking feature. So, if an organization is using sensitivity labels in its environment, and they're associated with a file that's tagged, Incydr will be able to leverage those to prevent that data and content from leaving the borders.

Saving time with agentic AI

It seems that agentic AI has become the topic of conversation in every industry – and it certainly is in security. We're building several agents for the insider threat platform, including an investigation agent that will make it easier for analysts to scale up their threat detection capabilities. The advanced investigation agent will improve analysts' ability to auto-close alerts that look like false positives and escalate alerts that could be live threats based on the quality of the data set.

Despite AI's promise for greater productivity, headlines about AI hallucinations drive home the point that a human analyst has to be part of the process. Keeping analysts tied in helps us refine our feedback loop and continue to auto retrain models to make them smarter based on customers' interactions with the data in the environment.

It's critical that businesses can maintain control of critical data, and Mimecast is helping customers simplify insider risk management so they can focus on what matters most.

EMPOWERING EMPLOYEES

Redefining security culture with personalized training

Masha Sedova, Vice President, Human Risk Strategy, Mimecast

The human element is still the number one reason why security breaches happen. In fact, recent research found that 3 out of every 5 breaches are due to human error – despite years of mandatory training and compliance efforts. Mimecast's Engage platform is tackling this challenge head-on with a bold and innovative approach, shifting away from stale, checkbox training to something truly effective and dynamic. Here's how Mimecast is transforming security awareness and training, turning employees into your organization's greatest security asset.

3 out of every 5 breaches are due to human error

Fresh content for a global workforce

Mimecast knows that engaging, relevant content is key to changing security behaviors. That's why Engage's content library has received a major upgrade. Organizations can now select from a diverse range of styles: from the popular "human error" videos to more mentor-style educational pieces, ensuring every organization finds the tone that fits its culture. But it's not just about style. Mimecast has expanded the range of topics to address modern workplace realities – think guidance on generative AI, personal device security, and safe use of tools like Slack and Google Drive. This ensures your employees are trained on the risks that matter most right now. Recognizing the needs of a global workforce, Mimecast is making this content more accessible than ever. Training materials will be available with subtitles in 27 languages, and many will be dubbed in German, French, and Spanish. Whether your team is in London, São Paulo, or Singapore, everyone gets the same high-quality, relevant training.

Realistic, reliable, and manageable simulated phishing

Phishing simulations are only effective if they land in employees' inboxes and reflect real-world threats. Mimecast has made significant strides in this area. With new direct message delivery, simulated phishing emails now reliably reach intended recipients, eliminating the headaches of domain whitelisting and expanding the range of domains you can use. Mimecast has also supercharged campaign creation and management. You can now run multilingual phishing campaigns using a growing library of 150+ templates (with more added each month), customize landing pages for realistic learning moments, and even send simulated phishing emails with attachments – mirroring the tactics used by real attackers. The campaign manager has been redesigned for easy multigroup sending, better testing, and difficulty ratings to help you tailor simulations as your employees grow more savvy.

Behavioral nudges: Personalized real-time coaching

Changing behavior isn't just about annual training or the occasional phishing test. Mimecast Engage offers "nudges" – real-time, personalized notifications that guide employees when it matters most. If an employee clicks a phishing link, mishandles sensitive data, or downloads malware, Engage detects that risky behavior and sends a tailored nudge right away. Delivered via Slack, Teams, or email, these nudges explain what went wrong and how to improve, with the option to include just-in-time training. Nudges aren't just for mistakes – they also celebrate positive actions, like going months without a security incident or promptly reporting phishing attempts. With an upcoming custom nudge builder, organizations will be able to design nudges for specific risk groups or scenarios. Want to remind your engineering team about a spike in phishing attacks? You can, instantly.

User scorecards: Visibility and accountability for every employee

Mimecast's new user scorecards bring transparency and motivation to the forefront of your security awareness program. Delivered to inboxes on a schedule you control (monthly, quarterly, etc.), scorecards summarize each employee's security performance – highlighting strengths, pinpointing areas for improvement, and providing clear calls to action. These scorecards are fully customizable to match your organization's branding and priorities. Some organizations even tie scorecard performance to incentives like bonuses or use them as the face of the security team's communication efforts. This hyper-personalized approach drives real accountability and empowers every employee to improve.

The future: Adaptive, personalized security experiences

Mimecast is moving security awareness from one-size-fits-all to adaptive, personalized experiences. Employees who consistently demonstrate good security habits get a lighter touch, focusing on efficiency and innovation. Those at higher risk receive more guidance – through nudges, regular scorecards, and, when necessary, security controls tailored to their needs. With these enhancements, Mimecast Engage doesn't just improve security awareness – it transforms it. The platform empowers your workforce, adapts to risk in real time, and helps you measure true behavioral change – not just training completion. Now is the time to make your employees your best digital defenders.

BEYOND ARCHIVING

Turning compliance and data governance into valuable insights

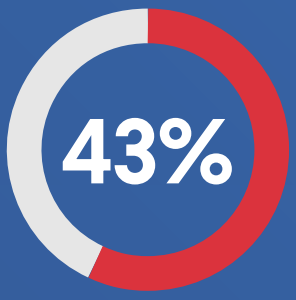
Matt Pasternack, Vice President, Product Management, Mimecast

3 in 5

images that get uploaded into chat systems are software screenshots, oftentimes containing sensitive data.

1 in 13

messages in Slack or Teams are now coming from external users.



of messages are in private locations which security teams don't have access to.

Companies today are facing stiff challenges securing their data in an environment where threats are becoming more complex and governance requirements demand more diligence. Email archiving is evolving to keep pace.

Mimecast's growing fleet of Digital Communication Governance, Compliance & Insights solutions are built with the vision and belief in mind that the most critical risk and insight about a company's employees, its brand, and its customers lives in this rapid real-time data where humans work and communicate.

Evolving data set = new set of risks

This modern data set is different and continuous. It's a heterogeneous environment and it introduces unique human behaviors that never had to be accounted for in the past.

Looking at Mimecast's internal research, for every 166 messages, at least one message contains highly sensitive information such as IP, passwords or company secrets.

- **One in 53 messages are either modified or deleted by end users.**
- **One in 13 messages are now coming from external users in Slack or Teams.**
- **Three in five images that get uploaded into new chat systems are software screenshots, often containing sensitive data.**
- **43% of messages are in private locations which security teams don't have access to.**

In the wrong hands, these messages can create costly risks and additional work for organizations. Over the past year, some major brands have shut off collaboration tools because they were concerned about what their employees were sharing. Others have had to scramble to repair their reputations after having sensitive data exposed. Employees that try to cover their tracks by deleting data in these systems often leave their employers with no native way to restore conversations.

This leaves us with a new issue: Tons of unstructured data and multiple stakeholders that need visibility, access, and control of it.

Speeding "time to context"

Traditionally, E-Discovery has been the main use case for legal teams, but now the market is shifting left as security teams rely more on the use of internal investigation and forensic tools to stay ahead of litigation events.

There's also a push to be more proactive with human risk, to be more resilient. Analyst reports back up this statement. Gartner predicts that by 2029, 30% of enterprises will shift to a proactive employee digital communication governance approach, to improve corporate policy outcomes, and advance business insights, up from less than 10% in 2025.

The median value loss for a company after experiencing a brand or reputational crisis is 30%. But losses from the same types of crises drop to 4% when there is a response within hours of it occurring, 10% when it's within days, and 14% or more when it takes weeks to address it.

The biggest reason companies drag their feet is they lack immediate access and visibility to the context they need to make those responses – what Mimecast describes as time to context. The lack of context typically presents itself in two forms: either not knowing where or what data was involved in the incident or crisis, or not truly knowing why employees took the actions they did.

These systems usually have the answers, but sometimes the answers are impossible to get to in a timely manner. Our mission at Mimecast is to make this data immediately accessible, usable and valuable across the entire enterprise.

For years, we've supported the traditional use cases of cloud archiving, email supervision, sync and recover, and user inbox for email. And now with our latest enhancements, we've layered on AI first, proactive experiences for the future of work.

3 key drivers behind the roadmap

1. Heterogeneous communication environments

Given the urgency to respond to security threats, it's critical to be able to find information quickly. Currently, security teams are left scrambling to interview employees and collect screenshots of conversations – if they even exist anymore. This can take hours, if not days or weeks, sometimes with no solution at the end of the process.

Teams that currently use Mimecast's Search and Discover product to analyze Teams or Slack data and Mimecast Cloud Archive to review email data have had to sift through two separate data sets. Customers have asked to find a way to leverage both engines in a single unified search experience.

Now they can. We've built the integration with customers' existing email archive to work with the powerful capabilities of Search and Discover, allowing them to search all connected data sources from a single AI-powered application experience. Now they can query searches, all provisioned around data access sets, tied to roles, making sure the right user has the right access to data at the start. And they can search across all communication channels based on user profiles, keywords and other criteria.

2. Intentional AI

AI is already playing a role in virtually every technology practice – and Digital Communications Governance and Archiving is no exception. Gartner reports that by 2030, 70% of enterprises using DCGA solutions will adopt AI-driven features and processes – up from 40% in 2025.

The good news is that Mimecast customers are already using AI – they're already in that 70%. The better news: AI will make their lives even easier in the coming years.

One good example of Mimecast's AI capability is the extra context and intelligence the Mimecast Mihra (Mimecast Intelligent Human Risk Agent) AI platform applies to every single message coming through our system. Mihra works behind the scenes, looking at the message, sorting through signals, making the central platform more intelligent.

When an investigation has to be done quickly, AI can save time and headaches. Picture a case where a security team does a search for all communications sent and received by a department that potentially could have been the source of a data leak. Looking across all channels, the number of communications could reach into the tens of thousands. Right away, Mihra brings back a summarization of the search result, letting the team know if it's on the right track.

Using Mimecast's collaboration specific filters and further Mihra analyses, the team can quickly narrow down the applicable communications down to two or three digits, hastening a conclusion to the investigation. Every response that comes through can also be traced back to the actual context that the response was generated from.

3. Improving customer experiences

As the Gartner Magic Quadrant reports, by 2029 85% of DCGA customers will consolidate the supervision of text and audio video-based content to a single solution, which is a major increase from less than 20% in 2025. This is why Mimecast architected and designed our platform the way we did – to be agnostic to data sources while being intentional about their unique experiences.

Our latest innovation involves an expansion into the Google Workspace data sets beyond email. We now support archiving, searching, monitoring and gaining insights from Google Chat. Just like our other integrations, keeping native context is key.

Digital Communications Governance & Archiving has evolved far beyond simple email archiving. Mimecast is working on new capabilities to expand the role we play in the space, helping companies protect and manage their all-important data. Adding new data sources, improving the range of our intentional AI, and providing unified user experiences will give customers the strength and versatility they need to manage threats today and into the future.

mimecast

Want more information? View Mimecast Elevate sessions on demand in the Mimecast Community!

Watch top breakout sessions and workshops from Elevate and dive into AI, Human Risk Management, and cutting-edge cybersecurity.

Log into the Community to see all that is available to you

Mimecast is a global cybersecurity leader redefining how organizations secure human risk. Its AI-powered, API-enabled connected human risk platform is purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform provides enhanced visibility and strategic insight.

By enabling decisive action and empowering businesses to protect their collaborative environments, our technology safeguards critical data and actively engages employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape.

From insider risk to external threats, customers get more with Mimecast. More visibility. More agility. More control. More security.

Mimecast and the Mimecast logo are either registered trademarks or trademarks of Mimecast Services Limited in the United States and/or other countries. All other third-party trademarks and logos contained in this press release are the property of their respective owners.

mimecast.com | ©2025 Mimecast
All Rights Reserved