Solution Brief

mimecast

Mimecast for Healthcare

We take care of security so you can take care of your patients

Healthcare organizations face unique cybersecurity challenges that have been exacerbated by an unprecedented global health crisis. IT and security staffing gaps and budgetary constraints have collided with a dramatic rise in the volume and sophistication of cyberattacks to create a new level of risk. Now more than ever, healthcare organizations need security solutions that mitigate risk, reduce complexity, and let them focus on what matters most – caring for patients.

> **"Mimecast quickly became what I believe to be one of the best technology investments we have made so far."**
>
> *- Mediclinic*

Why Mimecast

- Trusted by over 2000 healthcare organizations
- Best-in-class email security that delivers a fast time to value, while also helping drive ROI for other security investments
- Comprehensive protection, including archiving, continuity, and awareness training
- Single, unified platform that's easy to use and administer
- Award-winning customer service
- Robust library of pre-built API integrations
- Deep partnership with complementary security providers

An industry under attack

Healthcare providers face the same attack types that threaten most organizations. However, because the data healthcare providers hold is both sensitive and highly valuable, the industry is aggressively targeted. According to Mimecast's 2021 State of Email Security for Healthcare report, cyberattacks targeting healthcare organizations rose by 55% in 2020, resulting in PHI compromise for over 26 million Americans. There are a number of attack types that are particularly prevalent.

- **Ransomware**
  In Mimecast's most recent State of Email Security report, 50% of the healthcare organizations surveyed experienced a successful ransomware attack in 2020. The cost of ransomware attacks to the US healthcare industry in 2020 alone is estimated to be $21B. Because downtime isn't an option for healthcare providers, the likelihood of attackers receiving payment is high. As a result, organizations like FIN12 and others have been aggressively targeting the industry.
- **Payment fraud**
  Because healthcare organizations process such a high volume of financial transactions and must navigate complex insurance requirements and reimbursement structures, they are prime targets for payment fraud. Unsuspecting employees are hit with often highly personalized attacks designed to lure them into transferring funds to malicious actors.
- **Brand spoofing**
  Brand spoofing has become a growing problem for healthcare organizations, particularly during the pandemic. Mimecast's State of Email Security for Healthcare report showed that 67% of healthcare organizations had their brand spoofed or impersonated in 2020, exposing staff and patients to dangerous threats and misinformation during a time of crisis.
- **Data breaches**
  Securely storing patient data and complying with the complex regulations that govern it is a mandatory requirement for every healthcare organization. Cybercriminals understand how valuable healthcare data is and are highly incentivized to exploit it. However, that's not the only way that PHI can be exposed. HIPAA and HITECH have strict patient data requirements and auditing that are difficult to keep up with, factors that increase the risk of employee mistakes.

Competing priorities, growing challenges

To keep their organizations secure, healthcare security leaders must navigate a changing, complex, and sometimes competing set of priorities. Nothing is of higher priority than mitigating the risk of threats that can cripple operations – from ransomware to zero-day attacks. However, doing so is only getting more challenging. Budgetary constraints and uncertainty have been exacerbated by the pandemic, which required massive investments in resources and equipment while delaying elective procedures that can be a critical source of funding. At the same time, the difficulty of finding and retaining skilled staff for already lean IT and security teams requires getting a lot done with limited resources.

Simplified security designed to address complex needs

Mimecast helps healthcare organizations reduce risk and increase resiliency by providing best-in-class email security, combined with complementary security and data governance solutions that let you manage a broader set of needs with a single, integrated platform. These solutions are designed to help you:

- **Protect against the most sophisticated email-based attacks**
  The top attack vector demands the best possible protection. Mimecast is up to the task of keeping healthcare organizations secure in an increasingly hostile threat landscape.

- **Keep email communications flowing**
  Outages and attacks happen; things don't always go as planned. With Mimecast, you can ensure critical email communications keep flowing no matter what might come your way.

- **Shut down brand spoofing**
  Brand protection solutions give you full visibility into and control over who's sending emails on your behalf, while also allowing you to identify and quickly take down impersonations of your brand online.

- **Support end-user productivity**
  Mimecast protects clinicians and staff without getting in their way. End-user self-service tools – like SLA-backed email search and apps for mobile and web – can also make navigating email a little easier and less time-consuming.

- **Reduce the risk of human error**
  Mimecast's award-winning awareness training is designed to help end users detect and avoid attacks, while also educating them on healthcare-specific topics like HIPAA. Dynamic email warning banners, powered by AI and automatically updated across devices, also alert users to risk and crowd-source intelligence to make everyone safer.

- **Simplify compliance and data governance**
  Industry-leading archiving and data forensics solutions simplify the application of policies, ensure data is never lost, and dramatically reduce the time required to respond to legal requests.

- **Decrease the burden on staff**
  Mimecast's managed services for Email Incident Response and Awareness Training can reduce the burden on staff and put critical functions into the hands of dedicated, expert resources.

- **Reduce complexity and automate tasks**
  Mimecast's extensive library of API connections makes integrating with other systems (like Crowdstrike, Netskope, Splunk, and others) fast and easy, while supporting the automation of time-consuming, manual tasks.

The Mimecast Solution

Best-in-class email security	Protect against phishing, ransomware, impersonation, malicious URLs, weaponized attachments, and internal compromise
Email continuity	Keep email communications flowing, no matter what
Archiving and data governance	Ensure data is never lost, simplify compliance, and reduce the time and costs associated with e-discovery searches
Brand impersonation protection	Provide visibility into and control over emails sent from owned domains and quickly remediate digital brand spoofing
Awareness Training	Arm staff with the knowledge to detect and avoid cyberattacks with training modules that can be delivered through Mimecast or an existing LMS and with inline education that keeps them alert and engaged
Secure Messaging	Give staff a user-friendly way to safely email sensitive information
Data loss prevention	Prevent the accidental or intentional leakage of sensitive data
Robust API library	Easily ingest email data into other systems and automate tasks
AI-powered email warning banners	Alert users to potential threats with AI-powered warning banners that update risk levels in real-time across all devices
Staff augmentation	Reduce the burden on staff by out-sourcing key functions like administering awareness training programs and investigating emails reported as malicious by end-users

Mimecast is proud to help over 2000 healthcare organizations globally focus on their core mission of providing the best possible patient care. To learn more about why 40,000+ customers trust Mimecast to keep them secure, visit mimecast.com.

Cleveland Clinic LIFEPOINT HEALTH

> **“If we didn’t have Mimecast blocking such a volume of unwanted email, we would now be a lot busier reacting to issues than we are.”**
>
> *- South West London And St George’s Mental Health NHS Trust*

*https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-on-healthcare-organizations-cost-nearly-21b-last-year-study-finds.html