SOLUTION BRIEF

Security Heroes Unite: Mastering Human Risk Together

Become the Hero with the Human Risk Command Center

Your security team faces two interconnected challenges that make effective human risk management nearly impossible. First, you're trapped by the rigid, one-size-fits-all policies that quickly become outdated and cannot keep pace with the dynamic nature of user behavior and evolving threats that exploit human vulnerabilities. These inflexible approaches leave you constantly playing catch-up with sophisticated attackers who adapt their tactics faster than your security measures can respond.The second challenge cuts even deeper as you lack the ability to measure what truly matters. Traditional security awareness programs track completion rates rather than behavioral risk reduction, making it impossible to demonstrate real-world effectiveness or justify program investments.

This measurement gap means you cannot identify which interventions change risky behaviors and which fail to move the needle. Without this visibility your security investments remain unjustified, your high-risk users remain unidentified, and your organization remains vulnerable to the very threats your training programs were designed to prevent.

The fundamental problem extends beyond having the right tools. You need visibility into user behavior patterns, the ability to correlate training participation with actual security improvements, and adaptive policies that respond to emerging threat patterns in real time. Without these capabilities, your security team remains reactive, always one step behind both your riskiest users and the attackers targeting them.

Key Benefits

- **Measure organizational risk**
  Uncover your full spectrum of potential risk
- **Empower your workforce**
  Make employees part of the solution
- **Protect your organization**
  Secure the tools where work happens

Your Dynamic Defense Solution

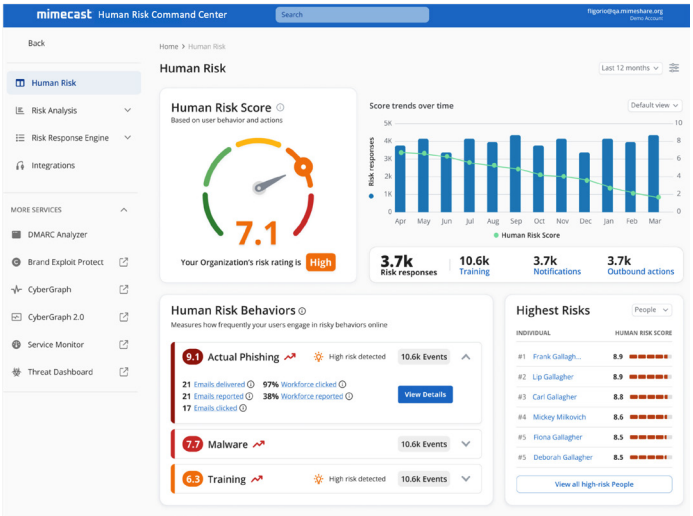
Mimecast's Human Risk Management (HRM) platform enhances risk visibility across your organization through various integrations. It collects data from email security, EDR solutions, IAM platforms, DLP tools, and training completion metrics.

The Human Risk Command Center centralizes the management of human risk, allowing security teams to identify and address vulnerabilities before incidents occur. By analyzing patterns like phishing susceptibility and risky behaviors, the platform provides insights into effective interventions that can reduce human risk.

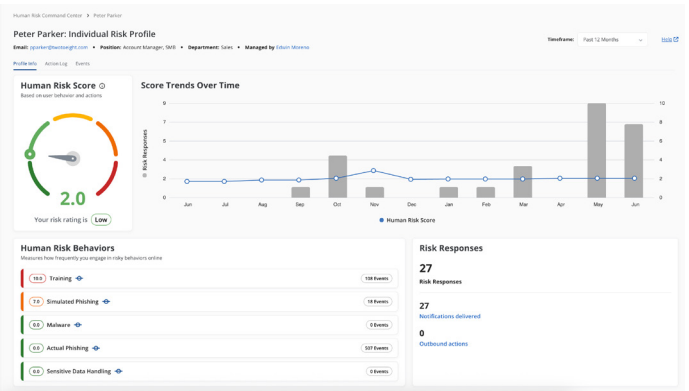
This approach uses behavioral correlation analytics to connect interventions with measurable security improvements, demonstrating which strategies effectively change behavior and mitigate risk.

Workflow

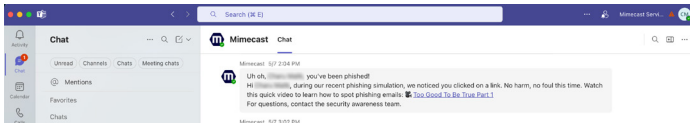
The power of the HRM platform lies in how the different products work together to mitigate human risk and adapt controls. When risky behavior is detected across Mimecast or any integrated tool, the HRM platform responds with targeted interventions or adjusts policies for the affected users – not everyone in the organization.



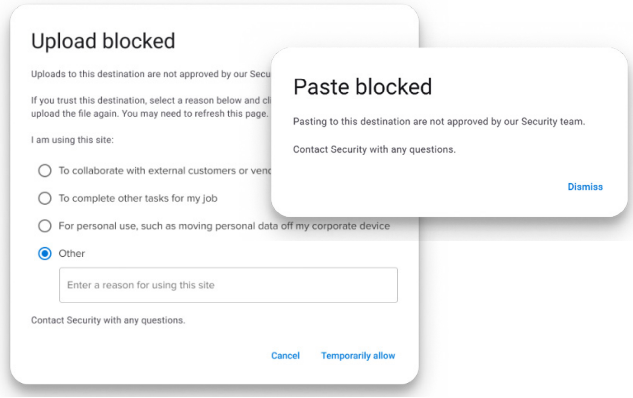
For example, users who continually click on phishing links and mishandle sensitive data are automatically placed into dynamic profile groups with tailored security measures addressing their specific risk patterns. This could include removing the ability to edit documents received via email or placing outgoing messages on hold to key supply chain partners.



Mimecast Engage behavioral nudges deliver just-in-time, context-aware feedback directly to users relating to their sensitive data mishandling. These configurable nudges provide immediate guidance across the tools where they're most likely to see it – email, Slack or Microsoft Teams – without disrupting their workflow, allowing you to engage them more effectively.



Mimecast's email security and Incydr synchronize the dynamic profile groups and watchlists, creating a bidirectional data flow. This ensures that any user added to the profile group in email security is immediately included in an Incydr watchlist. Preventative controls on the watchlist, like custom end user messaging and requiring justification for data movement, help mitigate risks. Should the risky actions of the user continue, adaptive policies can be applied like real time blocking, containing the endpoint, or disabling the user's account.



Use Cases That Drive Results

Executive Phishing Protection

Executives represent high-value targets for phishing attacks, yet they often lack the technical expertise to identify advanced threats. The Human Risk Command Center continuously monitors email patterns and automatically adjusts risk scores based on targeting attempts and behavioral responses. When an executive demonstrates phishing susceptibility or faces increased targeting, they're placed in a 'Very High Attack Factor' group that triggers enhanced protection measures. Adaptive email policies provide additional scrutiny for phishing links, while blocking unsupported browsers and applications from launching on the endpoint through Incydr.

Managing Repeated Offenders

Some users consistently engage in risky behaviors despite training efforts. The Human Risk Command Center automatically identifies repeat policy violators and places them in a 'Very High-Risk users' group that adapts to their behavior patterns. These users receive escalating security controls and enhanced monitoring that correspond to their specific risk areas rather than generic training interventions. Adaptive policies within email security removes their ability to edit attachments received via email. Within Incydr they receive micro training, warning message, or block access to cloud file shares. As a last resort, their endpoint can be quarantined for investigation while reaching out to the user directly.

Sensitive Data Protection

Improper handling of sensitive data continues to be a leading cause of breaches and compliance violations. Through Incydr and other integrations, the Human Risk Command Center obtains data handling events related to policy violations. When these events are viewed in conjunction with other risky behavior, users are placed within the 'Very High-Risk users' group. These groups sync back to Incydr, adding users to watchlists. When concerning behavior is detected, preventative controls activate immediately, providing just-in-time guidance that explains the risk and required actions. Through Engage behavioral nudges deliver just-in-time, context-aware feedback directly to users relating to their sensitive data mishandling

Become the Hero of Your Security Story

Your organization has the opportunity to transform from reactive to proactive defense through dynamic, measurable human risk management. Mimecast's HRM platform achieves measurable reductions in human risk through risk correlation amplified by your security ecosystem visibility, preventative controls, and adaptive policies. This transformation shifts your security posture from to evolve as dynamically as the threats you face, turning your workforce into active defense participants who adapt alongside emerging attack patterns.

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage 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, with Mimecast customers get more. More visibility. More insight. More agility. More security.