carahsoft | mimecast

Mimecast for State and Local Government: Elevating Email Security

Protecting your organization and citizens

The challenge state and local government entities face

State and local government entities play a crucial role in safeguarding sensitive data, including citizen information, intellectual property, and valuable research data. Given the diverse network of personnel, such as staff, officials, and contractors, these entities become attractive targets for advanced email attacks. The repercussions can include significant financial losses and damage to reputation. To counter these evolving threats and secure the integrity of government data, Mimecast provides an AI-driven email security platform. This technology serves as a robust defense, shielding state and local government institutions from a wide range of potential attacks.

Mimecast Protects

1,000+

Public Sector customers

2.25M

Public Sector users

1.3B

Emails inspected daily

Sophisticated, targeted threats

Ransomware Attacks

Ransomware attacks cost 28.6% more for critical infrastructure organizations, including education and public sector, than other industries.[1]

Phishing & Social Engineering

According to Verizon's Data Breach Investigations Report, 44% of social engineering attacks are phishing, meaning phishing is still a top threat facing all users.[2]

Vendor Risks

The US Government Accountability Office (GAO) reported that it can take up to 9 months to recover from a cyber-attack, resulting in monetary loss and downtime.[3]

1 IBM Security Cost of a Data Breach Report 2023 | 2 Verizon 2023 Data Breach Investigations Report | 3 GAO Highlights, Critical Infrastructure Protection

Addressing the Challenge with Mimecast Email Security

Modern educational institutions require advanced defenses against evolving threats. Mimecast's cloud-native solution seamlessly integrates with Microsoft 365 and Google Workspace within minutes, utilizing thousands of signals across identity, behavior, and content to distinguish legitimate messages from perilous threats.

Secure your educational organization with Mimecast's advanced email security platform. Safeguard valuable student and faculty data, protect intellectual property, and defend your reputation against the rising tide of sophisticated email attacks. By partnering with Mimecast, you ensure the continuity of learning and the safeguarding of critical resources.

The Mimecast Advantage

Proactive Detection:

Mimecast's AI driven approach recognizes anomalies in messages, instantly identifying and neutralizing threats targeting your faculty and staff.

Rapid Remediation:

Swift action ensures that threats are addressed promptly, mitigating the risk of data breaches, IP theft, and financial losses.

Enhanced Visibility:

Mimecast's email security solution dashboards offer a singular source of visibility into email threats, investigations, and trends.

Seamless Integration:

Mimecast integrates seamlessly with existing security layers, SIEM, SOAR, and other SOC solutions, streamlining your security workflows.

> "Mimecast is invaluable because it protects usfrom so many potentially costly and/or bad situations that could negatively impact city services or force us to revert to legacy processes."
>
> \- Shane McDaniel Director of IT, City of Seguin

Mimecast Email Security empowers state and local government with a unified platform that fortifies your email communication landscape across six essential protection domains. Seamlessly integrating with diverse email infrastructures and a wide array of IT security solutions, Mimecast delivers industry-leading protection and automated insights, simplifying management and fostering heightened confidence in your communication's security.

Key Benefits to Mimecast

Defensive Mastery: Safeguard both internal (East-West) and external (North-South) email traffic, ensuring uninterrupted communication across your entire ecosystem.

Impersonation Resilience: Advanced algorithms thwart intricate impersonation attempts providing unyielding protection against malicious deception.

Link & Attachment Vigilance: Proactively neutralize threats by blocking malicious URLs and sub-links, while meticulously inspecting attachments to neutralize malware.

Supply Chain Confidence: Identify and neutralize threats targeting suppliers, building a formidable defense against supply chain attacks that can disrupt critical services.

Domain Integrity: Prevent domain spoofing, ensuring that emails received are genuinely from trusted sources, bolstering brand trust and reputation.

Automated Intelligence & Reporting: Seamlessly share data across all products, enhancing threat insight and actionable reporting for swift, effective investigations.

Prevent Domain Spoofing: Mimecast's DMARC management empowers you to prevent domain spoofing and unauthorized email use, enhancing brand reputation.

Enanced Email Authentication: Implement strict authentication policies to verify the legitimacy of incoming emails, mitigating phishing attempts.

Integrate with Confidence:: Trust Mimecast Email Security to fortify your educational institution's email communication landscape. Experience industry-leading protection, streamlined management, and automated insights that empower your sector.

Contact us to discover how Mimecast Email Security enhances email security for state and local government.