

Mimecast For Public Sector

Local government departments hold significant amounts of personal and sensitive data as demands for digital public services increase.

Opportunities to enhance and expand digital public services across education, social care, housing, planning and other areas are substantial, however it is vital that local government organizations safeguard personal data against unprecedented cyber threats. Risks from cyberattacks, with email being the main attack vector, have the potential to cripple services and affect day-to-day functioning of public administration at all levels. At the same time, the impact on individuals can be deep and long-lasting.

Government bodies are establishing rules on protecting personal information. Federal and state laws in the United States, new EU General Data Protection Regulations (GDPR) and other country initiatives help reduce the attack surface by changing the way local government organizations collect, store and use personal data. Recent high profile cybersecurity incidents such as ransomware attacks on public infrastructure highlight the vulnerability of public service organizations and the profound impact on citizens. Local authorities must inspire public trust by protecting the personal information they hold while reducing the risk of data breaches and cyberattacks from a variety of sources including criminal hackers, hacktivists, insiders and foreign states.

Why Mimecast:

- 1,000+ local government, public administration and civil service organizations globally trust Mimecast for cyber resilience
- Proven multi-layered security to protect against spear-phishing, ransomware and impersonation attacks that target public sector organizations
- Quick implementation and low administrative burden aligns to public sector budget constraints
- Compliance with international security standards including ISO 22301, 27001 and 27018
- Comprehensive email management for Microsoft Office 365, Exchange and Google G Suite
- Rich APIs extend an existing technology stack and integrate key email data into SIEM and reporting packages
- A single console for email management saves IT administrators time and streamlines trouble shooting
- Email access through Outlook, mobile, web and Mac apps maintain employee productivity when primary email systems are unavailable
- Security awareness training and phish testing platform that changes employee behavior and reduces cyber risk
- Cloud archive with a 7-second search and e-discovery SLA, robust activity logging, and advanced case review tools

Real Customers. Real Solutions.

“Mimecast had the best awareness and control features, including URL protection, plus a cost-to-value that no other vendor could match.”

**—IT Operations Manager and Network Security Engineer,
Kansas City Public Schools**

CHALLENGES FACING THE PUBLIC SECTOR

Data Protection Compliance

Large quantities of personal information and sensitive data are in constant transit across multiple local government departments and affiliated third party providers. Much of this data has the legal requirement of being accessible and transparent for citizens. If not appropriately protected, the risk of cyberattacks and data breaches increases dramatically.

Mimecast: Data Leak Prevention and Secure Messaging tools ensure personal information and sensitive data in emails is encrypted and shared securely both internally and externally.

Cost Effective Security

With many local governments facing funding challenges, cybersecurity spending is lower than it should be, making them vulnerable to ransomware and other advanced attacks. Any cybersecurity incident can have a serious impact on service delivery and efficient functioning of local government departments. Administrators need the ability to quickly prioritize and manage threats.

Mimecast: Targeted Threat Protection inspects inbound, outbound and internal email to defend against ransomware, phishing and impersonation attacks.

Addressing Security Awareness

Human error is the leading cause of security breaches that can cost an organization millions in financial losses, reputation damage and fines. Old training models have proven ineffective to effectively address security awareness and reduce risk. A wide range of employee comfort with information technology and ability to identify threats makes employees in the industry an appealing target.

Mimecast: Awareness training, risk scoring and phish testing improves employee security awareness to reduce cyber risk.

Insider Threats

Local government organizations face threats from three groups of insiders and need to be prepared for each.

- Malicious insiders - purposefully take or misuse confidential data or exploit systems.
- Compromised insiders - email accounts are taken over through external phishing or malware attacks.
- Careless insiders - violate internal security policies and accidentally leak or expose sensitive data.

Mimecast: Internal Email Protect detects and remediates internal threats and prevents the spread of malicious URLs and attachments as well as sensitive information.

Continuity and Cyber Resilience

Getting cyber resilience right has never been more important as public services bear the burden of increasing cyber threats. A sound cyber resilience strategy focuses not just on combating cyberattacks but ensuring public sector staff remain connected during and after an attack to maintain services to citizens. Ensuring data is protected and recoverable after a threat is neutralized is key to business continuity.

Mimecast: Mailbox Continuity ensures uninterrupted access to all live and historic email and calendar information with a 100% service availability SLA.

Improving Web Security

The two most common vectors for cyber attacks are email and web. Email is often the point of compromise, while the web can be used subsequently to download a malicious payload or exfiltrate data. In addition to stopping access to malicious content, IT administrators need to monitor web traffic to block web sites that are out of organization policy or contain questionable content.

Mimecast: Blocks access to malicious websites and enforces.

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.