MIMECAST SECURITY DATASHEET

The industry’s broadest cloud-based service protecting against email-related risks

Email risks are broader than just spam and malware

Today email is a critical business tool, but it can represent significant risk to the organization. Mimecast® aim to provide the broadest possible email risk mitigation and compliance solution as a single service deployed over the Internet. The battle against malware and viruses is constantly evolving, but email is also subject to security threats such as Denial of Service (DoS) attacks, eavesdropping on non-encrypted email, phishing and accidental or malicious data leaks. Litigation and regulatory compliance have also driven the need for retention of email records with legislation such as Sarbanes-Oxley, CPR, FRCP, MiFID, HIPAA, and the Data Protection Act.

Benefits-at-a-glance:

1. Broad protection from email-related risks
A single cloud-based service offering protection from email-related risks, including malware infections, application and OS exploits, spam, phishing, DoS & DDoS attacks, data leaks, outages, social engineering attacks, staff non-productivity due to spam, litigation and compliance.

2. Rapid deployment and immediate effectiveness
Deployed in hours, Mimecast’s reputation harvesting capabilities, minimizes false positives from day one.

3. Constant innovation to match evolving risks
Mimecast security R&D focus on all email-related threats and was the first provider to offer cloud-based data leak prevention for email and one of the first to offer protection via a layer-7 intrusion prevention system.

4. Integration with wider email management systems
Email security should not be deployed on its own – ideally it should be tightly integrated with the entire email environment. For instance, in the event of disciplinary, civil or criminal action, connection to the archive is required to determine the context of a data leak (accidental or malicious).

5. Single policy-focused, not technology-focused administration
As a cloud-based service tightly integrated to Active Directory, Mimecast provides a single view and central point to set and enforce organization-wide security policies, as opposed to setting fragmented policies across point technology systems.

6. Robust Service Level Agreements
The Mimecast service operates at 99.5% spam protection, 100% virus protection and 99.999% uptime guarantee in our online Service Level Agreement.

Key features:

Comprehensive Malware Protection
Along with ARMed SMTP™ and its own proprietary anti-malware technology, Mimecast utilizes multiple commercial anti-malware engines by leading vendors including:

- **Commtouch**: a global network of outbreak detection systems allow them to be the first responder to many malware threats, both known and unknown.
- **Fortinet**: combines signature and heuristic malware detection technologies. The Fortinet approach to detection on-the-wire also allows Mimecast to shut off viral and intrusive transmissions early so that our service grid remains unaffected by malware outbreaks and targeted attacks.
- **AVG Commercial**: an ICSA certified company and market leader in both consumer and business malware protection software with combined intelligence gathered from the millions of commercial and freeware users. Mimecast uses AVG’s commercial signature and heuristic detection technologies to reject malware based on malicious message payloads.
• **Cloudmark**: comprehensive messaging security protecting subscribers and messaging infrastructure from spam, phishing, malware and other harmful content. Cloudmark’s customer base includes over 100 of the world’s largest service providers, including the majority of tier-1 operators in North America, Japan and Europe.

• **Mimecast proprietary anti-malware**: Mimecast’s proprietary anti-malware is based on GPL-licensed anti-malware and intrusion detection toolkits enhanced by Mimecast R&D to work in conjunction with the Mimecast processing grid and the other detection mechanisms.

• **Mimecast’s Dark Traffic Analysis Group (DTAG)** is a specialist team in Mimecast who utilize a network of honeypots that attract and aggregate both spam and malware in the wild. This coupled with community provided intelligence allows Mimecast to provide detection and protection mechanisms against malware easily and effectively using a well-known format applied to a rapidly evolving detection engine.

• **Sandboxing**: ensures that any suspicious executable code is executed in a protected ‘sandbox’ environment that provides a protected virtual environment that will detect the consequences of executing the code.

### Mimecast Advanced Reputation Management (ARMed SMTP™)
Mimecast’s security approach centers on its ARMed SMTP™ mail transfer agent. ARMed SMTP is based on a proprietary Mail Transfer Agent that has been purpose built with the needs of risk management and compliance in mind. The SMTP protocol is implemented in a manner that allows the analysis of anomalies, comparison to shared and individual reputation, detection of malware and the retention and integrity of archiving.

#### Single administration interface
Mimecast was designed ground-up as a single unified email management platform. As a cloud-based service, its single web-based administration interface delivers the granular control you would expect from an on-premise solution. This service empowers IT with the control needed to set policies organization-wide but also the flexibility to personalize granular policies for groups or even individuals. One reporting and easy-to-use web console saves significant time and frees up resources.

#### Protection from Application and OS Vulnerabilities
Malware has advanced beyond the days of viruses and worms, organizations may be subjected to highly targeted, specifically crafted attacks based on the results of careful reconnaissance of the organization’s infrastructure. Mimecast performs application-layer deep packet inspection on all traffic flowing through the Mimecast infrastructure, to protect against exploits that take advantage of vulnerabilities in application and operating systems.

#### Integrated archiving for investigation and evidence
Mimecast is an ideal platform for eDiscovery with its lightning fast search enabling iterative investigation of security and policy breaches. As Mimecast manages and stores the complete email life cycle, it provides evidential quality proof and comprehensive chains-of-custody to back-up disciplinary civil or criminal cases. The archiving platform retains metadata about all transmission, performed searches and policy activity.

#### Connection-based analysis
Mimecast offers state-of-the-art connection-based spam filtering through the use of Mimecast Global Reputation Service.

• **Mimecast’s RFC Conformity Checking**: proactively performs a series of queries on any unknown email servers to ensure they are legitimate (and not a spambot) before accepting any email for delivery.

• **Global Reputation**: Mimecast maintains a reputation database of email servers across the globe; this is comprised of intelligence from the aggregate of Mimecast customers, as well as commercial and non-commercial sources.

• **Local Reputation**: Mimecast offers far more than a ‘one-size-fits-all’ reputation service, by allowing individual groups and even users to utilize a reputation database tailored to their requirements. Mimecast’s Reputation Harvesting capability starts during implementation, and local reputation is effective as soon as it is turned on.
Policy-based encryption, without the hassle
Mimecast provides two separate mechanisms for ensuring encryption in transit: Transport Layer Security (TLS) and Closed Circuit Messaging (CCM). Encryption can be triggered by any form of policy, for instance based on keywords within headers, recipient address or domain or even the content.

- **Mimecast TLS** is completely transparent to the end-user and sends email through an encrypted tunnel to the recipient’s email server.
- **Mimecast CCM** allows for the delivery of email via a secure web-based channel without the hassle of key distribution and management. Perfect for both business-to-business and business-to-consumer communication, CCM provides non-repudiation of receipt and total control. Mimecast also natively supports TLS encryption.

Data leak prevention
Mimecast protects against leaks of confidential or sensitive corporate data, and was the first cloud vendor to offer extensive email Data Leak Prevention (DLP) functionality – a source of almost two-thirds of all data leaks.

- **Keyword / key phrase** detect the presence of a keyword or key phrase within an email body, subject header or attachment text (for instance with a PDF, PowerPoint or Excel document). This is often used to allow users to trigger optional encryption through the use of tagging emails by the inclusion of a phrase like ‘encrypt’ or ‘secure’ in the subject line.
- **Weighted Dictionaries** associate words or phrases with a particular positive or negative score. Each occurrence of a dictionary word or phrase is added to an aggregate score for that dictionary. The total is then compared to a threshold; if the threshold is reached a policy action can be applied.
- **Intelligent Identifiers** look for occurrences of structured data within email – such as credit card numbers, social security numbers or account numbers. Mimecast supplies Intelligent Identifiers for several common data types and users can build their own through the use of regular expressions.
- **File Attachments** compare attached files to a list of known confidentially-tagged files through the use of cryptographic checksums.

Continuous email protection and compliance
Mimecast provides tight integration into an organization’s email server to provide seamless and secure failover and failback with no loss of data or service. In the event of an email server outage, employees can continue to work uninterrupted within Outlook or webmail.

The Mimecast service is deployed on a purpose-built parallel cloud-grid platform that is highly available and protected by multi-layers of security. Mimecast’s online SLA targets a carrier-grade 99.999% uptime.

Effective Protection from DoS Attacks
DoS attacks, especially DDoS attacks conducted from a collection of compromised machines running spam bots under the control of a botherder, represent a threat to an organization’s communications and computing resource. As the Mimecast service is built on a parallel cloud-grid platform, it is able to harness distributed processing power to deal with malicious botnets that use a similar mechanism of tying together the capabilities of multiple machines.

During a DoS attack, Mimecast protects the customer’s computing AND communication resources. In addition, the Mimecast platform uses state-of-the-art Denial of Service mitigation techniques (such as SYN-cookies and behavioral attack detection) to ensure that network and computing resources cannot be overwhelmed by even a large-scale DDoS attack.

About Mimecast:
Mimecast delivers Software-as-a-Service based enterprise email management including archiving, discovery, continuity, security and policy.

By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email.
Protection from social engineering

Mimecast phishing detection capabilities analyze several characteristics of an email to determine whether an email is actually coming from the sender it is purporting to be from. By maintaining a dynamic URL list of known phishing sites, Mimecast is constantly refreshed and updated.

The service also proactively checks any new domain registrations for potential inclusion into the list. Specific phishing attacks are detected using a message fingerprinting technology that detects the phishing attack and all future mutations. The fingerprint database is constantly updated once every 45 seconds.

Protection from zero-day threats

The Mimecast Zero-Hour Adaptive Risk Assessor (ZHARA™) and the commercial anti-malware engine services provide early detection and protection against zero-day malware and spam outbreaks. Mimecast ZHARA provides highly effective zero-day protection against previously unknown threats through deep level anomaly detection and trending across the entire Mimecast customer base.

ZHARA examines suspicious message payloads using our proprietary message component examination system. ZHARA also tracks incoming connection patterns and traffic profiles from mail servers and provides further protection from DDoS attacks. ZHARA threat assessment components then undertake an iterative analysis of each piece of content and makes decisions about the payload.

ZHARA detected threats are analyzed by Mimecast’s team who then produce detection mechanisms for future occurrences.