

# Veolia cleans up e-mail for 5000 users in 38 countries with IronMail

## VEOLIA

### AT-A-GLANCE

**Industry:** Waste Management

**Location:** France

**Business Needs:** Centralise anti-virus protection, eliminate spam and block phishing attacks

**Solution:** Secure Computing IronMail messaging security appliance with TrustedSource sender reputation system

#### Results

- ◆ Protects more than 5000 mailboxes from spam and viruses
- ◆ Ensures compliance with international legislation such as the Sarbanes Oxley Act
- ◆ Reduces administration resources required to run messaging system and security
- ◆ Significant reduction in e-mail volume removes the need to increase the number of mail servers

**“Secure Computing was the only provider to offer us an “all-in-one” and “best-of-breed” solution that was quick and easy to implement. The main server, based in the head office, requires virtually zero maintenance.”**

**Didier Prou, IT Operations Manager, Veolia Environmental Services**

*Veolia delivers secure e-mail and anti-virus protection throughout their worldwide operations with IronMail from Secure Computing*

Veolia Environnement is a world leader in environmental services. With more than 250,000 employees and revenues of over €25 billion, the company has operations all around the world and provides tailored solutions to meet the needs of industrial and municipal customers in four complementary segments: water management, waste management, energy management and passenger transportation.

The waste management division, Veolia Environmental Services, has operations on every continent, is the only operator which can provide services across the waste management sector. The company operates in 38 countries and provides waste management and logistics services, including collection, wastewater management, cleaning and flow control, and treatment and recovery of waste.

With operations in multiple countries Veolia Environmental Services depends on e-mail and the web to run its business efficiently. It is essential to the company that they can minimise the impact of spam and threats such as viruses that can be communicated via e-mail.

#### Business Challenge

Veolia Environmental Services had two key requirements concerning their messaging system: firstly to implement the same domain name as Veolia Environnement (the parent company), and secondly to bring the system into compliance with international regulations, such as the Sarbanes-Oxley Act.

Veolia Environmental Services was looking for a package that could centralise its gateway anti-virus solution between the head office and the different divisions out in the provinces, while providing an industry standard anti-spam and SMTP routing solution which could quickly deal with phishing problems. The company was also seeking to procure high-performance, easy-to-deploy tools that would require almost no maintenance.

#### Why Veolia selected Secure Computing

The IronMail global solution from Secure Computing provides anti-spam, anti-virus and content filtering protection, and ultimately anti-phishing features. The Secure Computing solution guarantees security for all users via a dedicated server and a security appliance. With this solution in place, Veolia needs only one person dedicated to the messaging system.

The IronMail solution provides unified policy enforcement at the e-mail gateway to address all e-mail threats, including viruses, hackers, worms, intruders, spam and libelous content. It also provides webmail protection that enables e-mail users secure access to their e-mail any time, from anywhere in the world.

According to Didier Prou, IT Operations Manager at Veolia Environmental Services, “Secure Computing was the only provider to offer us an “all-in-one” and “best-of-breed” solution that was quick and easy to implement. The main server, based in the head office, requires virtually zero maintenance.”

#### Results

The Secure Computing solution guarantees security for more than 5 000 mailboxes. With this solution in place, Veolia needs only one person dedicated to the management of their messaging system.

According to Olivier Bousquet of Secure Computing, “The IronMail appliance has actually been designed from the outset as a “plug-in and forget” solution. We believe that our customers do not need to become experts, just users. In addition, the depth of information from the performance metrics can be used instantly to check the messaging system's security level. Our cutting-edge SMTP routing functions have enabled us to meet the complex environmental and geographical constraints faced by the Veolia Group, as well as remaining poised to address any future developments in their messaging security requirements.”

## About Secure Computing

Secure Computing® is a global leader in Enterprise Gateway Security, and has been securing the connections between people and information for over 20 years. Specializing in delivering Enterprise-class solutions that secure Web, email, and network connectivity, Secure Computing is proud to be the global security solutions provider to some of the most mission-critical network environments in the world.

Our more than 19,000 customers, supported by a worldwide network of partners, include the majority of the Dow Jones Global 50 and the most prominent organizations in banking, financial services, healthcare, telecommunications, manufacturing, public utilities, and federal and local governments. With over 900 employees, the Company is headquartered in San Jose, California, and has offices worldwide.

## Secure Computing Corporation

Corporate Headquarters:  
4810 Harwood Road  
San Jose, CA 95124 (USA)

Tel: +1.800.379.4944  
Tel: +1.408.979.6100  
Fax: +1.408.979.9501

European Headquarters:  
Tel: +44.0.870.460.4766  
Fax: +44.0.870.460.4767

Asia/Pacific Headquarters:  
Tel: +852.2520.2420  
Fax: +852.2587.1333

Japan Headquarters:  
Tel: +81.3.5339.6310  
Fax: +81.3.4496.4537

Secure Computing takes precautions to ensure the accuracy of the information contained in this publication and is not liable for any errors. The information in this publication is subject to change without notice.

Copyright © 2006. All Rights Reserved. Secure Computing, the Secure Computing logo, IronMail, TrustedSource are trademarks of Secure Computing. All other trademarks are held by their respective companies.

## Secure Computing IronMail

IronMail protects enterprise email systems from inbound threats: spam, viruses; or hackers trying to take down or take over the e-mail system. IronMail protects enterprise email systems from outbound threats: regulatory compliance violations, corporate policy violations, or theft (“leakage”) of confidential information or intellectual property. IronMail protects enterprise email systems from threats that haven’t even been identified yet.

### Key Benefits and Functionality to Stop Inbound Threats

#### Anti-Spam

Utilizing Secure Computing’s best-in-class TrustedSource Reputation Service, along with an award-winning “cocktail” of multiple detection algorithms, IronMail delivers the most accurate, effective, scalable and easy-to-manage anti-spam protection available.

#### Zero Day Anti-Virus

Given the severity of today's virus threats, enterprises can't afford the time it takes signature-based anti-virus software to respond to an attack. IronMail's Zero Day Virus Protection takes anti-virus protection to the next level by leveraging global threat intelligence from the TrustedSource reputation service to close the window of vulnerability that occurs between when an attack first emerges and when a signature is available – protecting your network from threats that don't yet exist.

#### Anti-Phishing

Phishers use spam to perpetrate fraud and identity theft. The best protection against phishing is to prevent these fraudulent emails from ever getting to an employee's inbox. In other words, the best anti-phishing defense is your anti-spam defense. And IronMail, with the TrustedSource Reputation System, is the industry's best anti-spam solution.

### Email Firewall and Intrusion Prevention

IronMail protects enterprises from every known e-mail attack technique, as well as those that have yet to be discovered. Denial-of-service, directory harvest attacks, port scans and other attacks are blocked by the purpose-built, hardened IronMail appliance and never have a chance to reach the network.

### Key Benefits and Functionality to Stop Outbound Threats

#### Compliance

Patient information; your customer list; this quarter's financial results. Organisations must protect critical content from “leaking” as well as prove they are complying with regulatory and other company policies. IronMail provides industry-leading e-mail scanning, content analysis and rules-based enforcement tools to ensure control of sensitive content and compliance with policy.

#### Policy-based Encryption

Encrypting emails containing sensitive information is a “best practice” that has historically been too hard to implement due to incompatible technologies; confused end users; and the complexity of translating policy into rules and action. IronMail solves these problems with an integrated, interoperable, policy-based encryption solution that ensures email compliance with no end-user interaction.