Government Email is Changing: Here’s How to Secure Your Journey to New Infrastructure

If you work in a government department or local authority there are major changes coming to the way you’ll manage and use email. Specifically, the Government Secure Internet (gsi) family of email domains and underlying email infrastructure are being phased out in 2019. The government claims this legacy set-up has become “costly, restrictive and cumbersome to maintain” and that migrating away will grant “more flexibility and commercial control to departments and local authorities.”

Many public sector IT managers are trying to understand the next steps. What options are on the table in terms of new messaging services to migrate to, and how do you ensure the appropriate security controls are applied?

To help manage this major upheaval, Trend Micro has produced a special white paper. It contains official advice from central government and the National Cyber Security Centre (NCSC) which should outline what your options are and what levels of security are required. Many IT managers will be looking to take advantage of this policy change to migrate to cloud productivity suites, in which case we have additional information on how to stay secure during the journey.

What’s Happening?

For more than 20 years, “.gsi” has been a part of government email addresses, but Whitehall now believes they are too restrictive. After March 2019 public sector organisations will instead need to use their own domain: ie gov.uk, gov.scot, llyw.cymru, gov.wales. The government has claimed the migration away from .gsi will help to ensure security in the modern digital age, although this will require more effort on the part of public sector IT managers.

A local government perspective

At a local government level, this also means an end to the current GCX network which allows councils to share data securely with central government departments. The hope is that local authorities will use the opportunity to simplify their email infrastructure from multiple gcx, gov.uk and other accounts to a single email account.

There are three main options available going forward:

Option 1: Cloud/on-premise email solutions (secured to the government standard). These might include Office 365 and Google G-Suite, or locally configured Microsoft Exchange etc.

Option 2: Cloud (portal) based email encryption solutions. From providers including Cisco, Trend Micro and Egress.

Option 3: Supplementary email solutions. In addition to their core email solutions, some councils may want to add other platforms like NHSmail to enable the use of shared calendars and instant messaging.

Security Requirements

It’s up to the individual local authority to choose the best option(s) for their organisation. But whatever platform they choose, strict security standards must be met. That government standard has been explained in more detail by the NCSC here.

In short, it mandates that all organisations should:

1) Ensure their email service is capable of sending and receiving email using Transport Layer Security (TLS). For a more specific set of recommendations, see this section on configuring TLS to protect email in transit.

2) Configure the following anti-spoofing controls on their domain:
   • Domain-based Message Authentication, Reporting and Conformance (DMARC)
   • Sender Policy Framework (SPF)
   • Domain-Keys Identified Mail (DKIM)

Other security controls – There are additional security controls that should be considered in addition, focusing on new and emerging threats as well as regulatory compliancy.

• Data Leakage Prevention, working with GSC (Data Protection and GDPR),
• Next generation and day zero antispam and anti-phishing covering Phishing treats and advanced BEC protection with writing style machine learning.
• Zero day malware, advanced threat detection / prevention with integrated custom Sandboxing.

Journey to the cloud

Many public sector IT managers will want to take advantage of these major changes to migrate to cloud-based platforms that could help drive broader cost and IT efficiencies and improve productivity. Office 365 does have the built-in capabilities to help you comply with NCSC guidelines for secure e-mail. But in many cases this journey to the cloud may take some time, during which there might be hybrid environments to secure. Many councils are only in the planning or pilot stages, for example.

With the March 2019 deadline fast approaching, it pays to find a single vendor that can handle both on-premise and cloud security. Consolidating in this way will save money, drive operational efficiencies and ensure there are no security gaps for attackers to exploit.
Fortunately, Trend Micro has mature e-mail and O365 e-mail/collaboration security solutions, designed with flexibility and security in mind.

**Advanced Next Generation cloud, on premise or hybrid protection.**

**InterScan™ Messaging Security** provides the most comprehensive protection against both traditional and targeted attacks. Using the correlated intelligence from Trend Micro™ Smart Protection Network™ and optional sandbox execution analysis, it blocks spam, phishing, and advanced persistent threats (APTs). The included hybrid SaaS deployment option combines a powerful gateway virtual appliance with a SaaS pre-filter that stops majority of threats and spam in the cloud—closer to their source. This hybrid solution delivers the best of both worlds: the privacy and control of an on-premises appliance with an in-the-cloud pre-filter for resource efficiency and proactive protection. The Data Privacy and Encryption Module solves the toughest regulatory compliance and data protection challenges by securing outbound data.

Trend Micro offers integrated security with two Cloud products in one: Trend Micro **Hosted Email Security** and Trend Micro **Cloud App Security**.

**Hosted Email Security** is a no-maintenance secure email gateway service that delivers continuously updated protection to stop phishing, fraud, ransomware, spam, and advanced targeted attacks before they reach your network. It protects Microsoft® Exchange™, Microsoft® Office 365™, Google Gmail, and other hosted and on-premises email solutions, meeting NCSC guidelines around encrypting e-mails with TLS 1.2 and the anti-spoofing guidance with DMARC, SPF etc.

Although built-in Office 365 security is good, it only scans for known threats, when the truth is that 90% of today’s malware is unknown to traditional AV techniques. That’s why countless public sector organisations have already contacted Trend Micro to enhance their O365 security and secure their journey to the cloud.

**Cloud App Security** provides state-of-the-art threat and data protection for Office 365 and cloud sharing environments. It protects incoming and internal Office 365 email from advanced malware and other threats, and enforces compliance on other cloud file-sharing services, including Box, Dropbox, Google Drive, SharePoint® Online, and OneDrive® for Business. Powered by the Smart Protection Network, Trend Micro’s industry-leading cloud intelligence platform, it offers pre-execution machine learning, document exploit detection and behaviour analysis to spot ransomware, Business Email Compromise (BEC) and other advanced threats.

The over-arching Smart Protection for Office 365 is designed and licensed to be flexible and co-exists to allow for that journey from on-premise e-mail security to cloud based infrastructure — all in the one license.

---

**Smart Protection for Office 365**

![Diagram](image)

```
* also includes integration with

- Box
- Dropbox
- Google Drive
```

---

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo and Deep Security are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. (SB05_18052018US)