clearswift

RUAG Cyber Security

ISSA Central Maryland December 2017 Monthly Meeting

Gene Stromecki

Sales Executive / Account Manager

Eugene.Stromecki@clearswift.com

Scott Messick

Pre-Sales Engineer

Scott.Messick@clearswift.com

We're Moving to Office 365" - Enhance Security in Office 365

Overview

Volusia County Schools is the public school district for Volusia County in Florida. The district operates over 80 schools with over 63,000 students and 7,300 teachers and administrators.

A business decision in 2017 motivated by the need to reduce business costs prompted Volusia County Schools to migrate from an on premise infrastructure to Microsoft Office 365 and Microsoft Azure cloud services. Volusia's IT department, however, understood the security functionality limitations with Office 365 and wanted to retain the same level of protection the Clearswift SECURE Email Gateway (SEG) had provided for their on premise system.

Alex Kennedy, Assistant Director of Business & Data Operations, Volusia County Schools said, "The functionality of the Clearswift SECURE Email Gateway and its web-based interface have always been key strong points for us. The solution's integration with Office 365 was a real bonus. We now have peace of mind that our new cloud email platform has the same level of protection that we had become accustomed to."

The Challenge

Basic Security Functionality in Microsoft Office 365

Email remains one of the most common digital collaboration tools for organizations globally and the threat landscape has subsequently evolved. Today, advanced security and data loss prevention features are needed to combat information borne threats across email – from within and outside the organization. However, Microsoft Office 365 only has basic security features built in such as anti-spam, anti-malware and URL scanning. In addition, any anomalies the platform detects and deems as a threat are 'blocked' which the IT department then has to deal with. For large organizations, the administrative time dealing with 'stop and block' solutions, or worse still, security threats that penetrate a network because they can't be captured with basic security functionality, can be time consuming and costly.

clearswift
RUAG Cyber Security

Agenda

- Case Study
- Ransomware, Spear Phishing and Human Error
- Targeted Attacks Using Web Sites and Social Networking
- How to Protect
- Summary

Ransomware in Perspective – 2016

600%

Growth in ransomware attacks against businesses

97%

Of phishing emails contain ransomware

30%

Of malware attacks are zero-day exploits with increased use of evasion techniques

$1 billion

Cost to businesses

Source: "Malware Year in Review 2016", PhishMe and "Internet Security Report – Q4 2016", WatchGuard

clearswift
RUAG Cyber Security

Spear Phishing in Perspective – 2016

91%

Breaches that begin with spear phishing

146 days

Average time to identify a breach

82 days

Average time to contain a breach

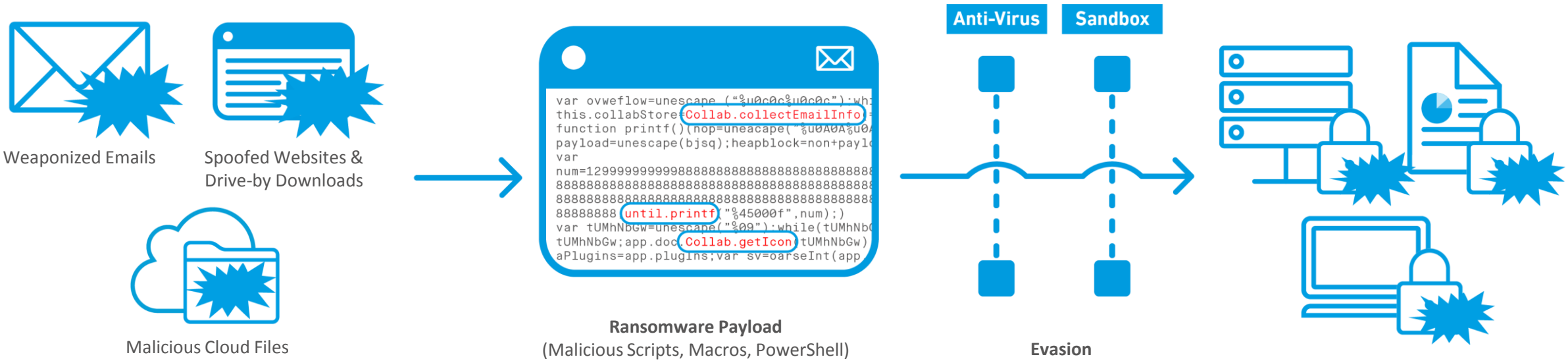
$4 million

Average cost of a data breach

Source: "Malware Review Q3 2016", PhishMe

Delivery Methods and Evasiveness

- Delivery methods constantly evolving
- Ransomware designed to bypass traditional SPAM, anti-virus and sandboxing technologies



clearswift
RUAG Cyber Security

Ransomware In Action: Cerber Example

Cerber arrives as password protected Word document attached to email

User opens Word document and enables editing

Word macro script executes, runs PowerShell script

Cerber automatically downloaded from Internet and installed

Cerber encrypts files

Ransom request displayed

clearswift
RUAG Cyber Security

Ransomware

Problem

- Lincolnshire County Council attacked via email with CryptoLocker ransomware that encrypted data
- Attacker initially asked for $500 in Bitcoin, with threat to escalate

Result

- Council's computer systems closed for four days
- Services including libraries and online booking systems affected
- "People can only use pens and paper, we've gone back a few years."

Lincolnshire County Council's computer systems have been closed for four days after being hit by computer malware demanding a £1m ransom.

clearswift
RUAG Cyber Security

Spear Phishing

Problem

- US Nuclear Regulatory Commission (NRC) hacked three times in as many years
  - Employee's personal email account used to send PDF attachment containing malicious active content
  - Employees targeted with email linking to Microsoft OneDrive document hosting malware
  - Emails sent to employees with link to Google spreadsheet

Result

- Confidential records of US nuclear power industry compromised
- Clean up costs

clearswift
RUAG Cyber Security

Spear Phishing: Social Media

Problem

- Chief Design Engineer at construction equipment manufacturer responds to approach on LinkedIn about potential recruitment opportunities
- Opens email with malicious attachment that installs spyware
- Spyware uses password protected compressed files over HTTP to bypass DLP policies

Result

- Primary competitor launches identical piece of large construction equipment
- Other projects in danger of similar compromise
- Loss of competitive edge and business

Business Email Compromise (BEC) – Phishing

Problem

- Government cybersecurity contractor Defense Point Security LLC employee fooled by email masquerading as memo from CEO requesting people's IRS W-2 forms
- Included social security numbers, income figures, work and home addresses, and other personal data
- No outbound DLP controls to block this type of data

Result

- Affects anyone employed by Defense Point Security in 2016
- Scammers can file false tax records impersonating employees and funnel refunds into perpetrators' bank accounts

17 MAR 17 Govt. Cybersecurity Contractor Hit in W-2 Phishing Scam

Just a friendly reminder that phishing scams which spoof the boss and request W-2 tax data on employees are intensifying as tax time nears. The latest victim shows that even cybersecurity experts can fall prey to these increasingly sophisticated attacks.

On Thursday, March 16, the CEO of **Defense Point Security, LLC** — a Virginia company that bills itself as "the choice provider of cyber security services to the federal government" — told all employees that their W-2 tax data was handed directly to fraudsters after someone inside the company got caught in a phisher's net.

Alexandria, Va.-based Defense Point Security (recently acquired by management consulting giant **Accenture**) informed current and former employees this week via email that all of the data from their annual W-2 tax forms — including name, Social Security Number, address, compensation, tax withholding amounts — were snared by a targeted spear phishing email.

clearswift
RUAG Cyber Security

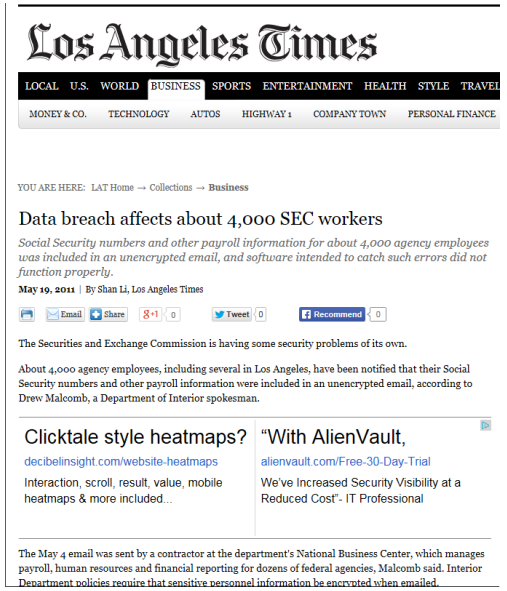
Encryption: Human Error

Problem

- 4,000 Security and Exchange Commission (SEC) workers affected by data breach
- Contractor sent unencrypted email containing employees' Social Security numbers and payroll information
- Staff had access to unsecured email accounts

Result

- Damage to reputation
- Affected employees offered 60 days of free credit monitoring
- Loss of employee trust



Los Angeles Times

LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH STYLE TRAVEL

MONEY & CO. TECHNOLOGY AUTOS HIGHWAY 1 COMPANY TOWN PERSONAL FINANCE

YOU ARE HERE: LAT Home → Collections → Business

Data breach affects about 4,000 SEC workers

Social Security numbers and other payroll information for about 4,000 agency employees was included in an unencrypted email, and software intended to catch such errors did not function properly.

May 19, 2011 | By Shan Li, Los Angeles Times

Email Share 8+1 0 Tweet 0 Recommend 0

The Securities and Exchange Commission is having some security problems of its own.

About 4,000 agency employees, including several in Los Angeles, have been notified that their Social Security numbers and other payroll information were included in an unencrypted email, according to Drew Malcomb, a Department of Interior spokesman.

The May 4 email was sent by a contractor at the department's National Business Center, which manages payroll, human resources and financial reporting for dozens of federal agencies, Malcomb said. Interior Department policies require that sensitive personnel information be encrypted when emailed.

clearswift
RUAG Cyber Security

Data Loss: Human Error

Problem

- Medical clinic sends HIV newsletter with recipients in the CC field
- Names and email addresses of 780 people revealed

Result

- Investigation into Chelsea and Westminster NHS Trust handling of confidential medical information
- Fine from Information Commissioner's Office (ICO)
- Legal action by victims
- Wider inquiry into NHS handling of confidential medical information


BBC Sign in News Sport Weather iPlayer TV

NEWS

Home UK World Business Politics Tech Science Health Education

England Regions London

London clinic leaks HIV status of patients

2 September 2015 | London

Dr Alan McOwan: "Not everybody on the list is HIV positive"

A London sexual health centre mistakenly leaked the details of nearly 800 patients who have attended HIV clinics, bosses have admitted.

The 56 Dean Street clinic in Soho sent out the names and email addresses of 780 people when a newsletter was issued to clinic patients.

Patients were supposed to be blind-copied into the email but instead details were sent as a group email.

clearswift
RUAG Cyber Security

Data Loss: Boeing

Problem

- Boeing employee emailed a spreadsheet full of employee personal data to his spouse
- Spreadsheet sent to provide formatting template
- Also contained personal information of 36,000 Boeing employees, including Social Security numbers and dates of birth in hidden columns

Result

- Boeing offer two year Experian subscription to employees
- Damage to reputation due to not using own DLP solutions

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Blundering Boeing bod blabbed spreadsheet of 36,000 coworkers' personal details in email

Its own security software could have stopped data exposure

22 Feb 2017 at 19:43, Thomas Claburn

Global aerospace firm Boeing earlier this month sent a notification to Washington State Attorney General Bob Ferguson, as required by law, about a company employee who mistakenly emailed a spreadsheet full of employee personal data to his spouse in November, 2016.

The spreadsheet, sent to provide the employee's spouse with a formatting template, contained the personal information of roughly 36,000 other Boeing employees, including Social Security numbers and dates of birth, in hidden columns. Some 7,288 of the affected

clearswift
RUAG Cyber Security

Data Loss: We Trust Our Employees

Problem

- Six employees of large manufacturing company Liebherr download thousands of design documents to USB drives
- Included virtually every type of drawing, design and other document necessary to build a mining truck business, design a manufacturing facility and design a series of mining trucks to compete with Liebherr
- Passed files to Chinese competitor

Result

- Competitor offered their truck at lower cost
- Loss of competitive edge and business
- Each Liebherr truck costs $4 to 5 million

clearswift
RUAG Cyber Security

Compliance

Problem

- Various compliance regulations (e.g. GDPR, HIPAA, PCI, etc.) require protection of sensitive data
- Employees not aware of latest requirements
- Security seen as a barrier to just doing their job

Result

- Legal fines
- Damage to reputation
- Loss of business

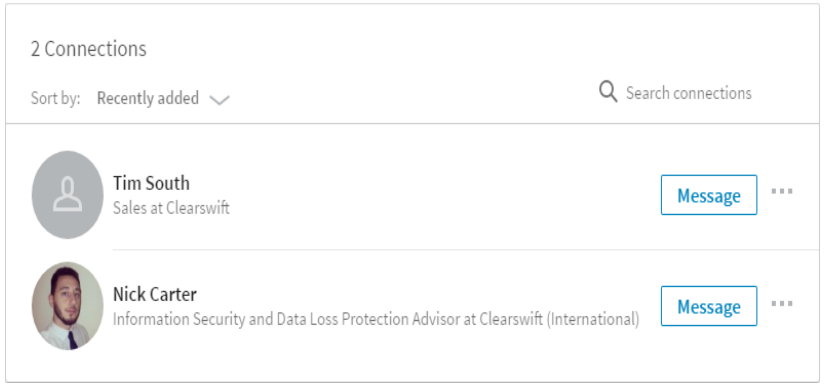
“If you think compliance is expensive, try non-compliance.”

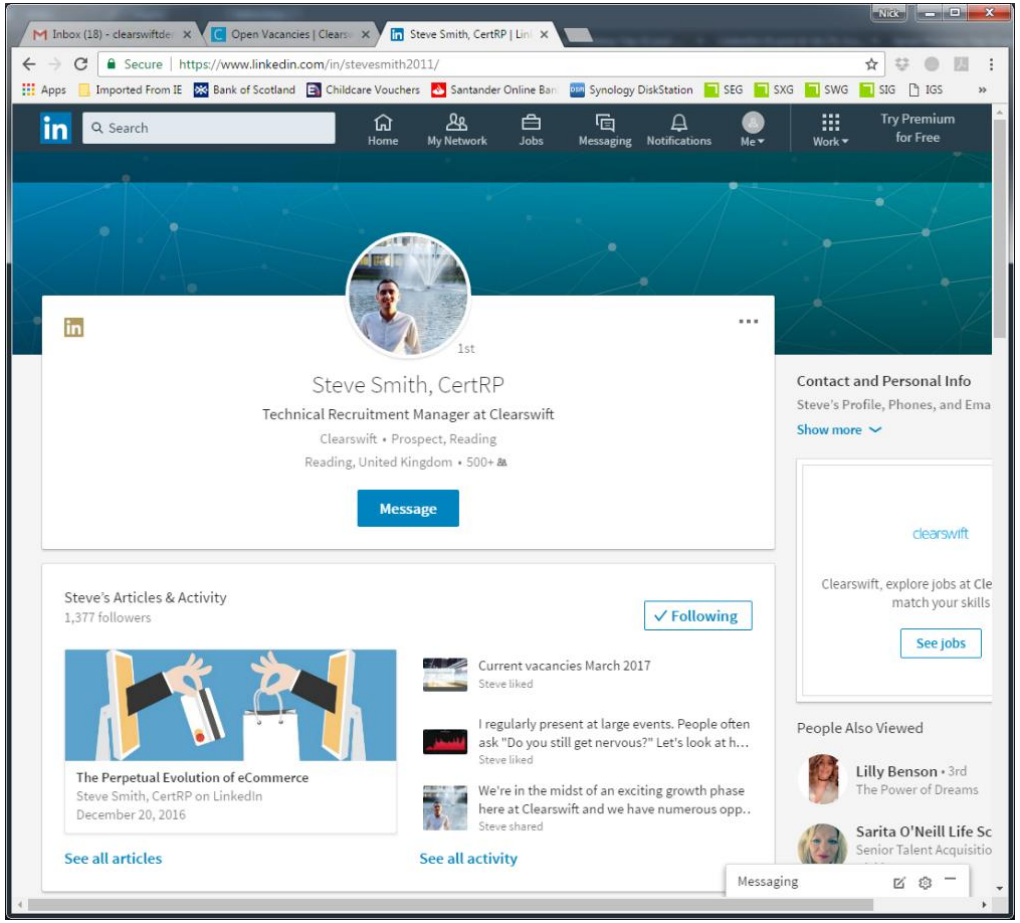
Former Deputy U.S. Attorney General Paul McNulty

clearswift
RUAG Cyber Security

Example Clearswift

- Check LinkedIn for job roles at target organization
  - Target Sales people to build mutual connections
  - Focus on roles that have access to sensitive data
  - Focus on roles that are likely to open a document (e.g. HR, Finance, etc.)
  - Look at other connections they have
  - Check other social media for useful information (e.g. where they have worked, when they are on holiday, etc.)

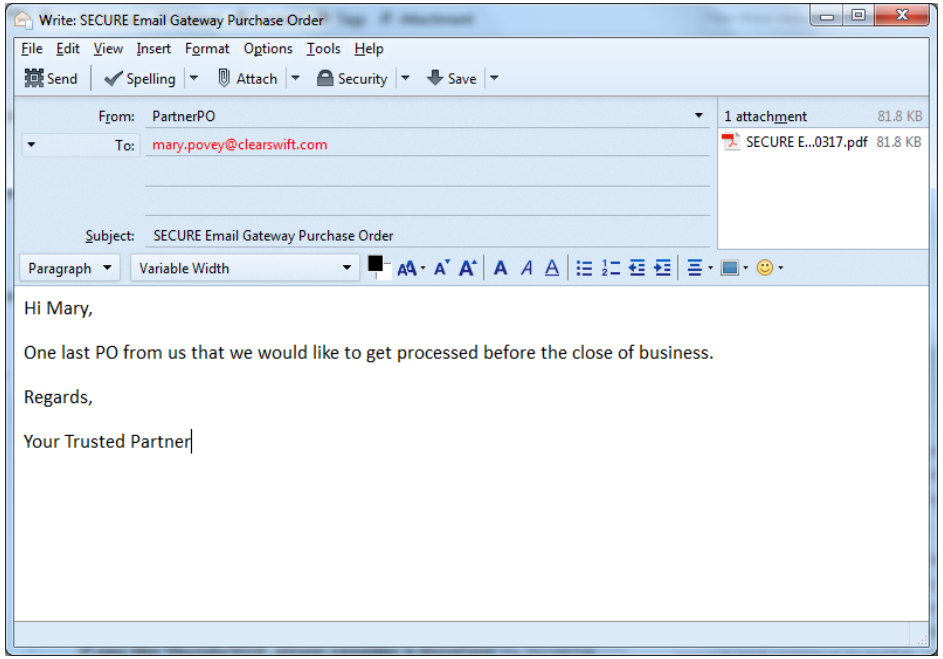


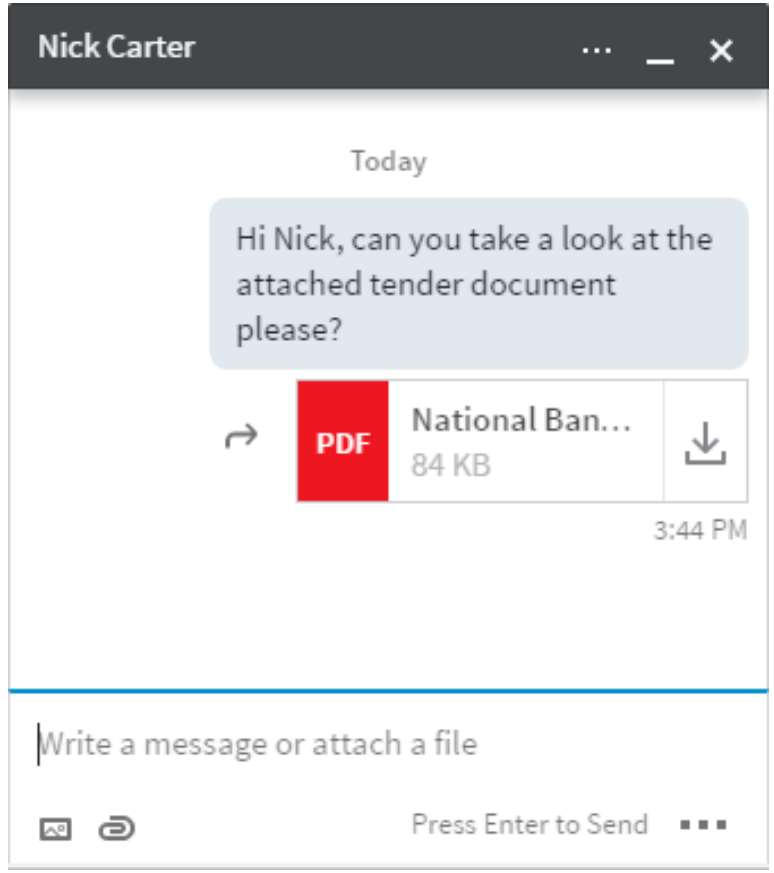


clearswift
RUAG Cyber Security

Example Clearswift

- Check website for customers or partners
  - Spoof PO from partner with payload
  - Spoof RFI from prospect with payload

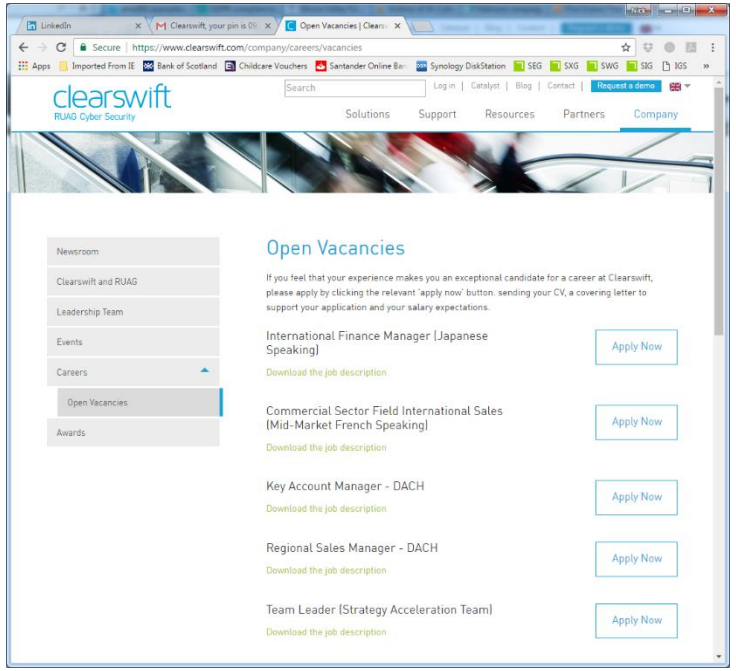


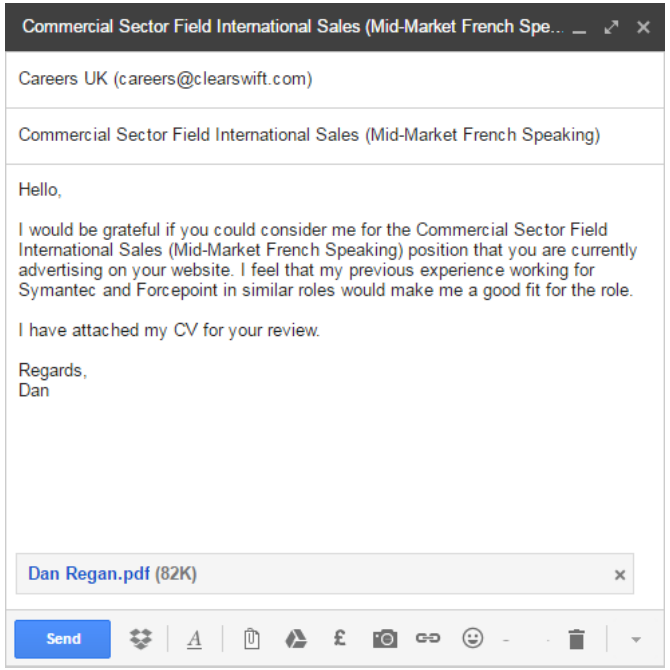


clearswift
RUAG Cyber Security

Example Clearswift

- Check website for vacancies
  - Send CV with payload
- Check website for documents with metadata
  - Spoof message from author to reviewer(s) with payload





clearswift
RUAG Cyber Security

Protection from Ransomware, Spear Phising and Human Error

Solution

- SECURE Email Gateway and ARgon for Email
  - Block by source
  - Dual Anti-Virus
  - Deep Content Analysis
  - Structural Validation
  - Message Sanitization
  - Structural Sanitization
- SECURE Web and ICAP Gateways
  - Block by source
  - Dual Anti-Virus
  - Deep Content Analysis
  - Structural Validation
  - Structural Sanitization

SECURE Email Gateway

ARgon for Email

SECURE Web Gateway

SECURE ICAP Gateway

clearswift
RUAG Cyber Security

Clearswift Unique: Adaptive Data Loss Prevention

Adaptive Data Loss Prevention

Adaptive Redaction: Data Redaction

Overwrites critical information to prevent breach
Communication is not blocked

Adaptive Redaction: Structural Sanitization

Removes active content (e.g. scripts, code, etc.)
Information is left intact in original file format

Adaptive Redaction: Message Sanitization

Removes malicious URL's from email messages

Adaptive Redaction: Document Sanitization

Strips out hidden information (e.g. change tracking, properties, comments, etc.)

Encryption

Secures data in transit
Automated to avoid delays and mistakes

Modifying content to *reduce disruption* to business

- o -

Automatically & consistently remove content which breaks policy, but leave the rest alone

- o -

No 'stop & block' associated with traditional DLP

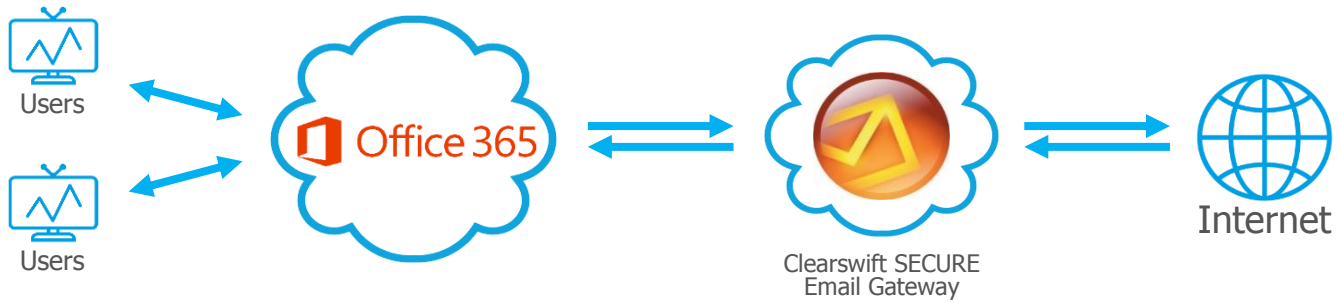
- o -

Security & compliance (incl. GDPR)

Summary

- Microsoft O365 good solution although feature GAPS exist between Microsoft and 3rd Party Security Email Gateway products
- Enhance Microsoft Office 365 Email Security with Clearswift
- Instant risk mitigation from Advanced Persistent Threats (APT's)
- Protect critical information, reduce DLP false positives and enable secure continuous collaboration
- Incorporate business requirements
- Rule Granularity
- Managed, hosted and on premise deployment options

Alex Kennedy, Assistant Director of Business & Data Operations, Volusia County Schools said, "The functionality of the Clearswift SECURE Email Gateway and its web-based interface have always been key strong points for us. The solution's integration with Office 365 was a real bonus. We now have peace of mind that our new cloud email platform has the same level of protection that we had become accustomed to."



clearswift
RUAG Cyber Security