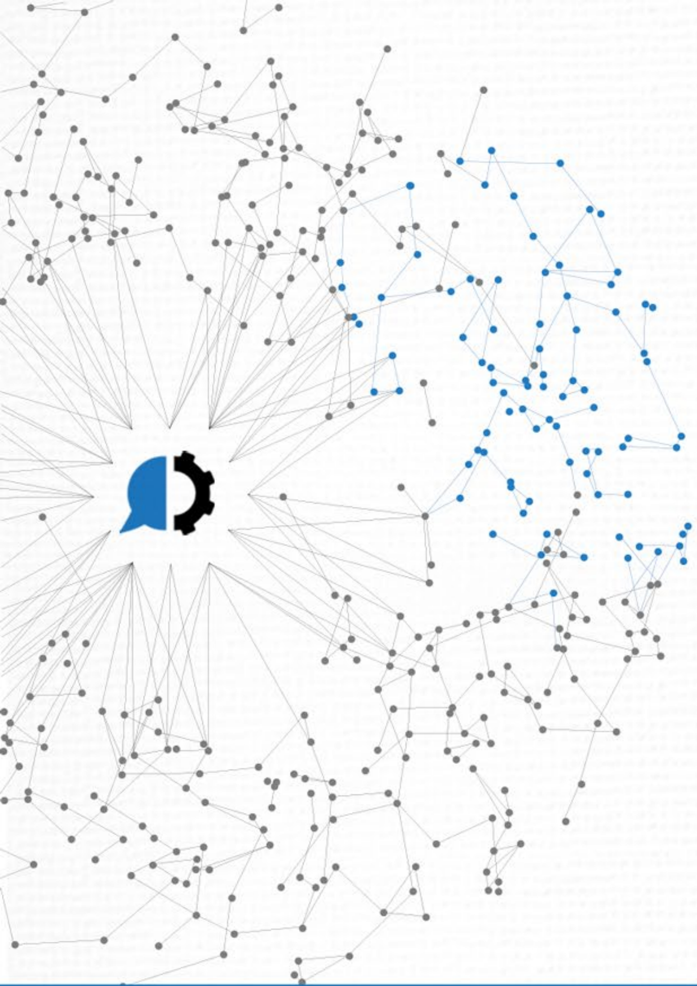


Manage, Sanitise and Secure Your File Transfers

www.helpsystems.com

Today’s Presenters

Ray Sutton

Technical Solutions Consultant

HelpSystems

Kym Welsby

Regional Director, APAC

HelpSystems

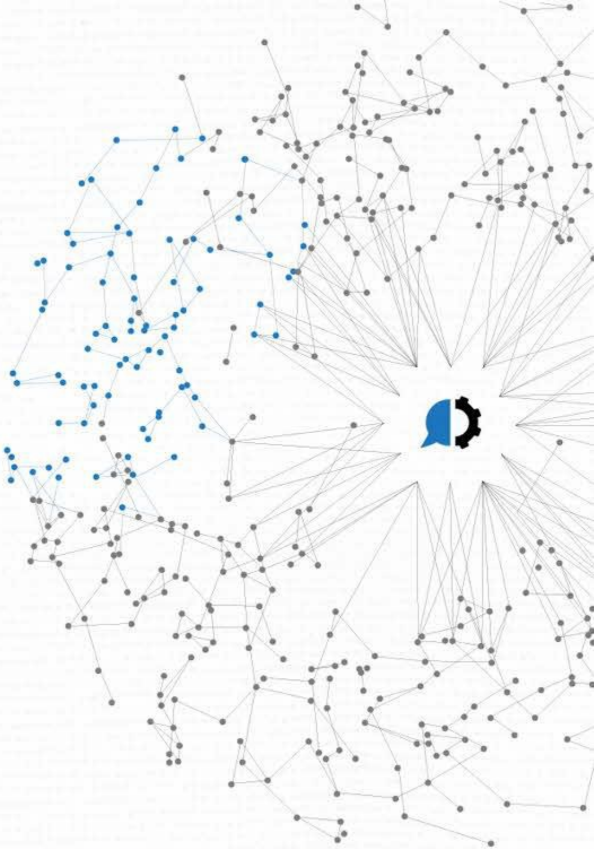
Simon Kuenstner

MFT Subject Matter Expert

Generic Systems

Agenda

1. 2019 data security statistics
2. Common security challenges when transferring files
3. Why encryption isn't enough
4. Use cases
5. Demo
6. Q&A



UP NEXT

2019 Data Security Statistics

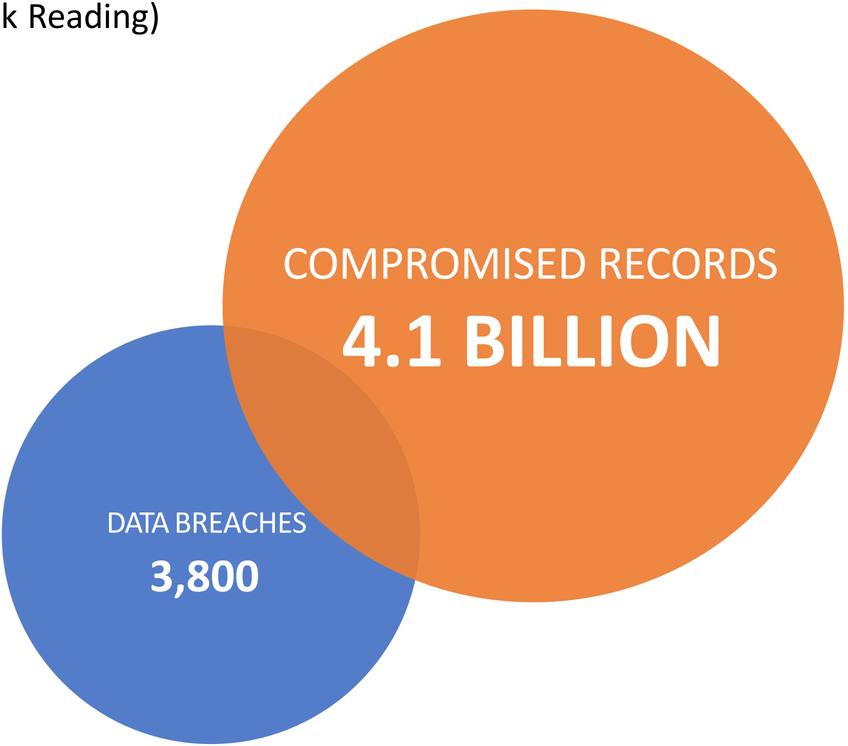
Trended as “worst year on record” for data breaches (Dark Reading)

COMPROMISED RECORDS ARE ON THE RISE

In the first half of 2019, 4.1 billion records were publicly reported as compromised as part of more than 3,800 data breaches – **a 54% increase** over data breaches reported in the first half of 2018. (Norton)

WHAT DATA WAS MOST EXPOSED?

Email (contained in 70% of exposed records) and **passwords** (contained in 60% of records exposed) were at the top of the pile. (Forbes)



COMPROMISED RECORDS

4.1 BILLION

DATA BREACHES

3,800

2019 Data Security Statistics

$41,000

The average pay-out for cybercriminals targeting individuals and businesses increased to over $41,000 in Q3 of 2019, a growth of 13.1% over the previous quarter. (Data Breach Today)

50%

Research by the Everest Group revealed that 50% of technology spend in organizations is "shadow IT" systems, software, or applications used regularly without knowledge by the executive or IT teams.

82%

82% of teams told Nexplane in a recent survey that they've pushed back against IT's attempts to implement a vetting process for collaboration tools.

More than just Emotet

2,000%

Growth in ransomware attacks in 2 years

Stealth for Destruction

Stealth for information harvesting

24 - 47%

Of malware attacks missed by traditional anti-virus

Source: “The New Mafia: Gangs and Vigilantes”, Malwarebytes, “Internet Security Report Quarter 3, 2017”, WatchGuard and “Bootkit Ransomware Baddy Hops Down BadRabbit Hole in Japan”, The Register

Australia's biggest cyber threat – active content!

- Australia’s three most significant national cyber security incidents of the last 12 months have all been triggered by a user simply opening a word document received by email.
- Malicious code evaded anti-virus engines.
- **All** files received from external sources, even trusted partners, can have malicious code embedded – in text, images, and more.
- Note: Recent exposure of nearly 55K drivers licenses by NSW found in an open cloud storage environment.

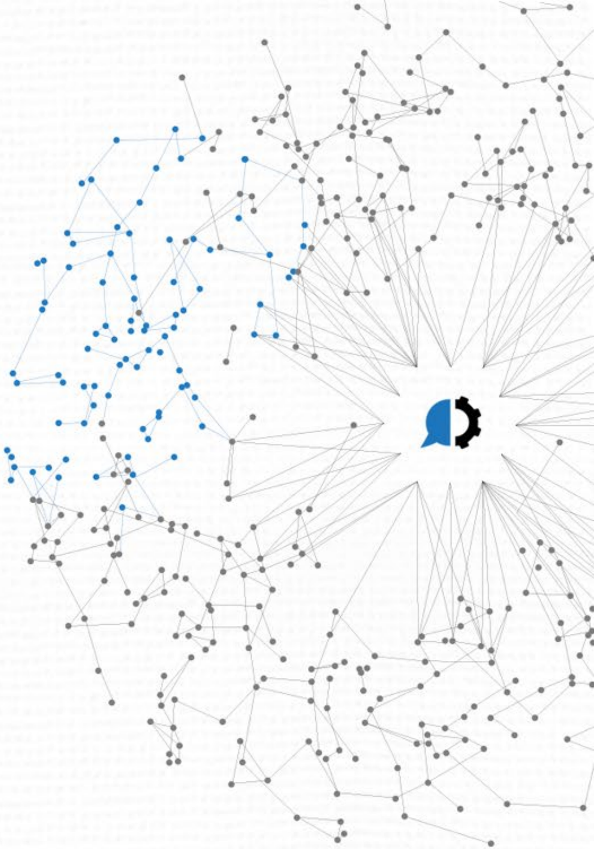
Australian National University

TOLL

VICTORIA State Government | Health and Human Services

NSW GOVERNMENT

Common security challenges when transferring files



UP NEXT

4 Common File Transfer Challenges

#1
Old technology is being used, such as FTP, PC tools, or scripts.

#2
Processes are time-consuming and inefficient.

#3
No error alerts or audit logs to meet compliance rules.

#4
Employees are still sending files unchecked.

5 Common File Transfer Challenges

#1
Old technology is being used, such as FTP, PC tools, or sc

#2
Processes are time-consuming and fficient.

#5
Covid-19. with people working from home this is causing major data challenges for companies.

#3
No error alerts or au logs to meet compliance rules.

#4
Employees are still sending files unchecked.

Why isn’t encryption enough?

Even if it is secure…

- Viruses, malware, and advanced persistent threats should NOT be allowed to be transmitted at all.

Even if it is secure…

- You need to know what is being transmitted.

Even if it is secure…

- The ability to audit who is sending what is a requirement for many organizations.

Best Practices for Secure and Sanitised File Transfers

1. Use secure protocols like SFTP to exchange files with trading partners (do not use standard FTP!).
2. Encrypt files in transit and at rest.
3. Set up batch workflows to automatically process files.
4. Generate detailed audit trails.
5. Use a managed file transfer (MFT) solution to simplify and protect file transfers from a centralized interface.
6. Automatically modify content to reduce disruption to business: Sensitive Data Redaction, Document and Structural Sanitization
7. Employ anti-steganography and OCR technology to remove content from images.

Why HelpSystems?

HelpSystems helps you mount a triple-threat defense of managing, sanitising, and securing your file transfer with a singular, dashboard-friendly solution. Our solution can be deployed on-premise, in the cloud, or in a hybrid environment to secure and streamline the exchange of data between systems, employees, customers, and trading partners.

Secure File Transfer

Move files with extensive security controls to meet compliance requirements.

Automated Workflows

Eliminate the need for custom programs/scripts, single-function tools, or manual processes.

Content Inspection

Deep, rich content analytics ensure sensitive data is not transmitted.

Threat Protection

Ability to inspect content for viruses and malware.

Use Case #1

How it works…

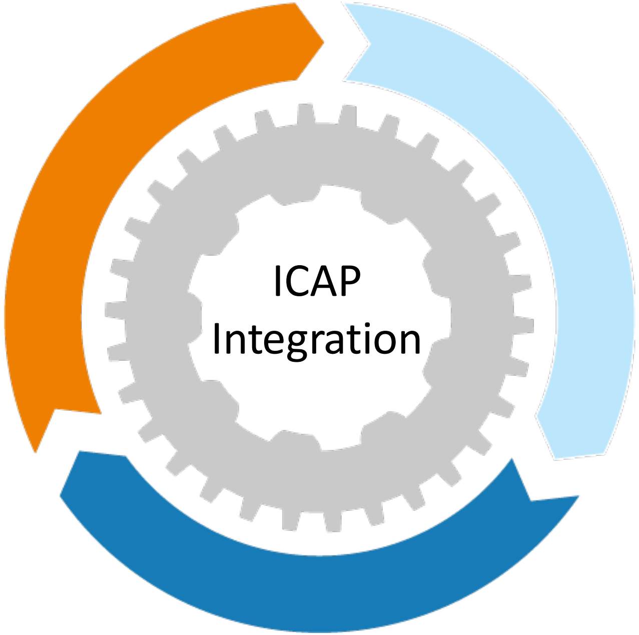
1 Customers upload PDF forms to a company's web portal.

2 Managed File Transfer solution encrypts the channel for secure (private) transmission

3 ICAP checks for viruses, validates that it is a PDF and checks for any active content.

4 If the content *can* be sanitized, the transmission is allowed and continues.

5 If the content *cannot* be sanitized or is not a PDF, the transmission is blocked and notification sent.



Use Case #2

How it works…

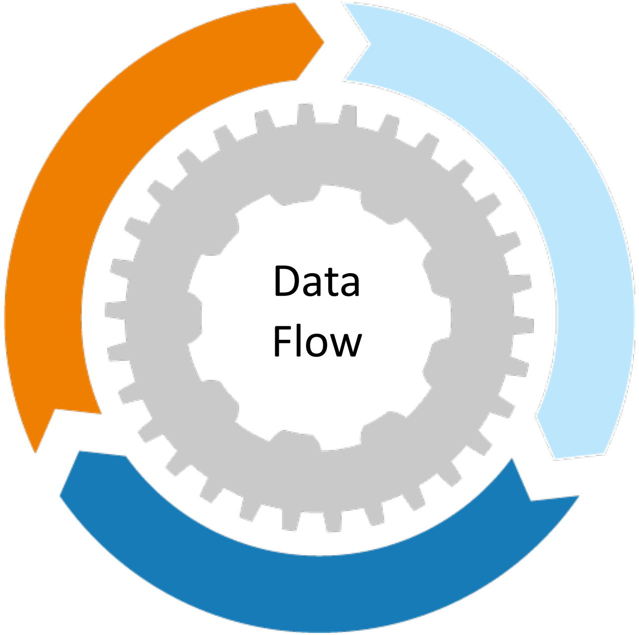
1 Securely transfers attachments between employees or trading partners.

2 The ICAP Gateway only intercepts content when threat protection and requirements exist.

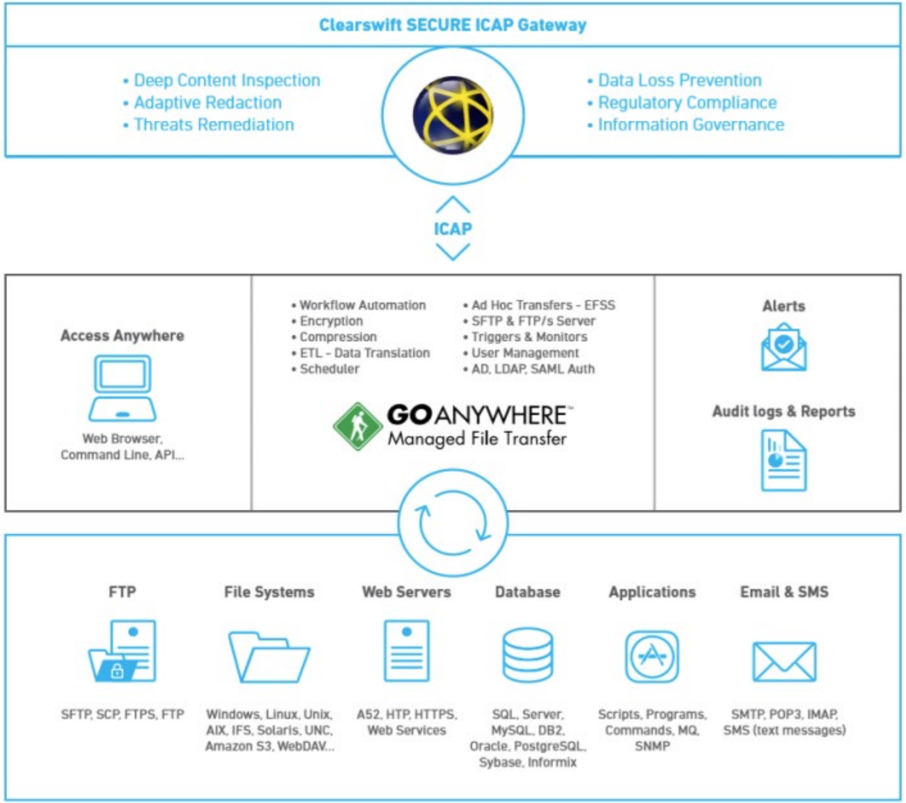
3 ICAP runs rule set (keyword search, executable renaming, script removal,etc.).

4 If the content *can* be sanitized, the transmission is allowed and continues.

5 If the content *cannot* be sanitized, the transmission is blocked.



Demo



Clearswift SECURE ICAP Gateway

- Deep Content Inspection
- Adaptive Redaction
- Threats Remediation

- Data Loss Prevention
- Regulatory Compliance
- Information Governance

ICAP

Access Anywhere

Web Browser, Command Line, API...

- Workflow Automation
- Encryption
- Compression
- ETL - Data Translation
- Scheduler

- Ad Hoc Transfers - EFSS
- SFTP & FTP/s Server
- Triggers & Monitors
- User Management
- AD, LDAP, SAML Auth

GOANYWHERE™ Managed File Transfer

Alerts

Audit logs & Reports

FTP

SFTP, SCP, FTPS, FTP

File Systems

Windows, Linux, Unix, AIX, IFS, Solaris, UNC, Amazon S3, WebDAV...

Web Servers

A52, HTP, HTTPS, Web Services

Database

SQL, Server, MySQL, DB2, Oracle, PostgreSQL, Sybase, Informix

Applications

Scripts, Programs, Commands, MQ, SNMP

Email & SMS

SMTP, POP3, IMAP, SMS (text messages)

Helpsystems Clearswift ICAP Use cases

1. **Orders received via emailed Excel, active content not allowed**
2. External user upload a file into Secure Folders, virus found
3. Sending Bank Statements to a trading partner, redact credit cards
4. Accounts Payable Invoice PDFs received via email, active content not allowed

Helpsystems Clearswift ICAP Use cases

1. Orders received via emailed Excel, active content not allowed
2. **External user upload a file into Secure Folders, virus found**
3. Sending Bank Statements to a trading partner, redact credit cards
4. Accounts Payable Invoice PDFs received via email, active content not allowed

Helpsystems Clearswift ICAP Use cases

1. Orders received via emailed Excel, active content not allowed
2. External user upload a file into Secure Folders, virus found
3. **Sending Bank Statements to a trading partner, redact credit cards**
4. Accounts Payable Invoice PDFs received via email, active content not allowed

Helpsystems Clearswift ICAP Use cases

1. Orders received via emailed Excel, active content not allowed
2. External user upload a file into Secure Folders, virus found
3. Sending Bank Statements to a trading partner, redact credit cards
4. **Accounts Payable Invoice PDFs received via email, active content not allowed**

Thank you for joining us!

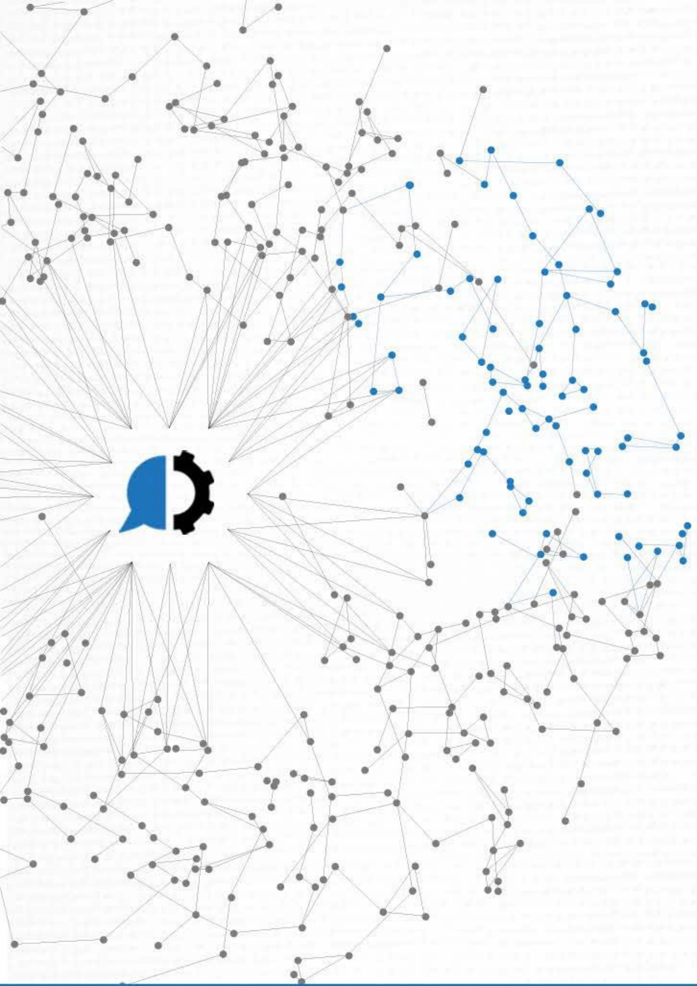
- Questions? We’re happy to help.
  - info@helpsystems.com
  - www.goanywhere.com
-
- Let us know in the post-webinar survey if you’re interested in a custom demo.

Learn more on our websites:

- www.goanywhere.com

www.clearswift.com

A survey will display after the webinar ends.
Please let us know how we did. Thanks for your feedback!



Any Questions

www.clearswift.com
www.goanywhere.com