NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

18TH NEW YORK STATE
CYBER SECURITY CONFERENCE

Cyber Security's Weakest Link: YOU

June 2, 2015

RATIONAL Enterprise

Michael McCutcheon
Chief Solution Officer
MMcCutcheon@RationalEnterprise.com
NYC Office | +1 212.719.4444

genda

Baseline Cyber-Security Protections

Notable Security Failures

Data Breach Trends & Statistics

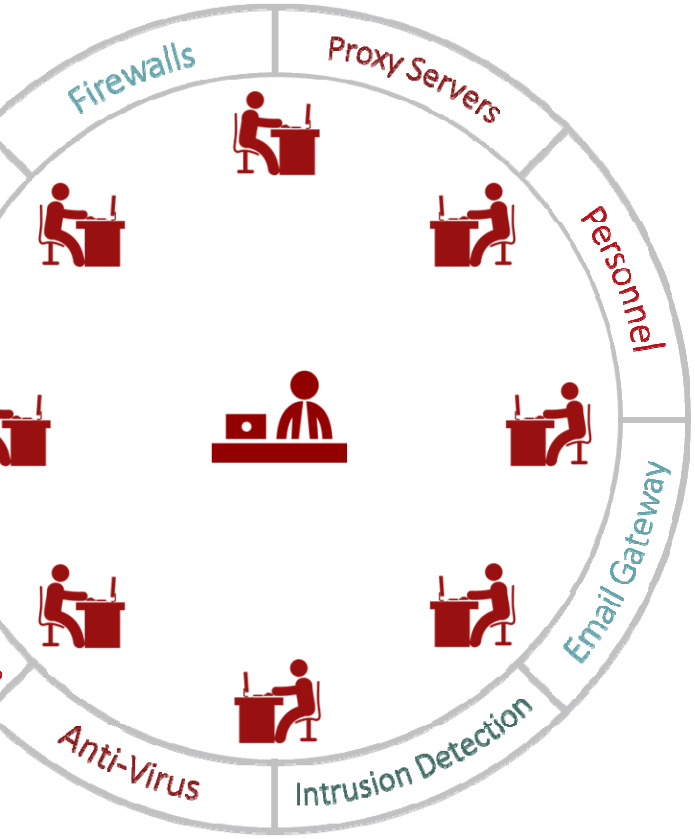
Example Data Security Shortcomings

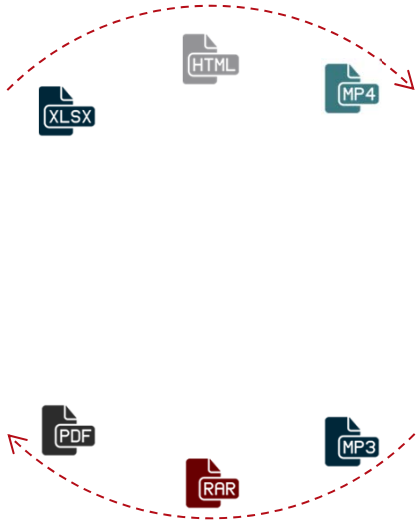
Enforce Information Governance to Improve Cyber & Data Security

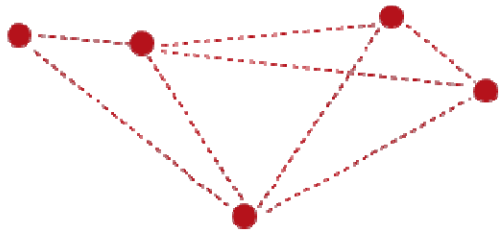
Solutions to Data Security Shortcomings

Q&A

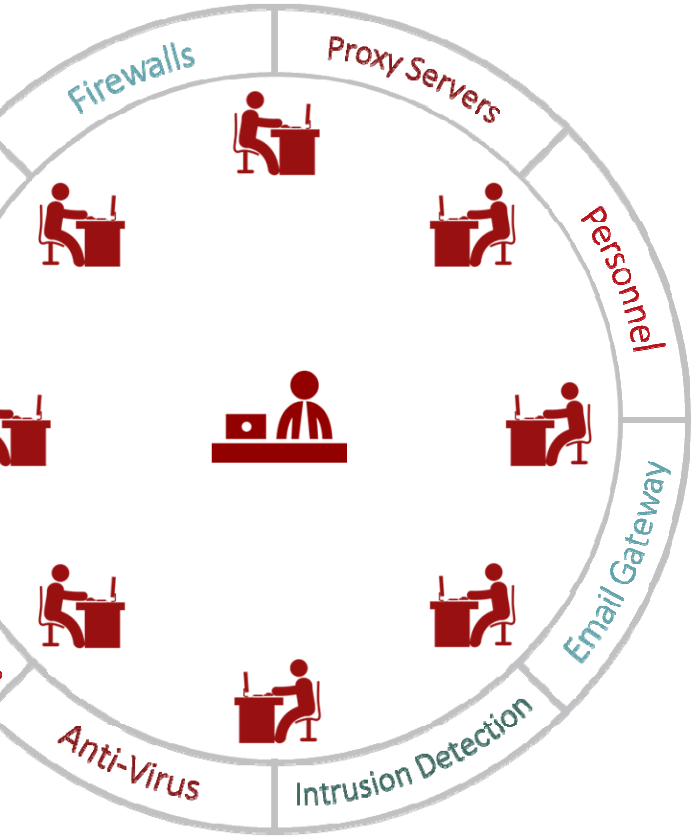
aseline Security Measures







aseline Security Measures



- ✓ Spam Filtering
- ✓ Anti-Virus Protection
- ✓ Firewalls
- ✓ Proxy Servers
- ✓ Data Loss Prevention
- ✓ Intrusion Detection
- ✓ Trained Personnel
- ✓ Email Gateways

otable Security Failures

Hacking/Malware

- Ebay (21/05/2014)
  - Records Breached: 145,000,000
- J.P. Morgan Chase (28/08/2014)
  - Records Breached: 76,000,000
- The Home Depot (02/09/2014)
  - Records Breached: 56,000,000

Insider

- The Variable Annuity Life Insurance Company (26/02/2014)
  - 6 years to uncover breach of unknown personal info.
  - Records Breached: 774,723
- The Home Depot (06/02/2014)
  - Employees stole personal info of other employees, using company email to transmit stolen files
  - Records Breached: 30,000

Physical Loss/Theft

- Cedars-Sinai Medical Center (22/08/2014)
  - Employee laptop stolen, compromising patient data, initially reported as only 500 records
  - Actual No. of Records Breached: 33,136
- Department of Health, Los Angeles County, Sutherland Healthcare Solutions (06/03/2014)
  - Desktop computers stolen, compromising patient data
  - Records breached: 68,000

- Unintended Disclosure
  - Riverside Community College (16/06/2014)
    - Employee emailed a file containing student information to a wrong email address
    - Records breached: 35,212

/www.huffingtonpost.com/kyle-mccarthy/32-data-breaches-larger-t_b_6427010.html

ata Breach Trends & Statistics

Y FINDINGS :: 2015 VERIZON DATA BREACH INVESTIGATIONS REPORT

> "…the common denominator … accounting for nearly 90% of all incidents – is people. Whether it's goofing up, getting infected, behaving badly, or losing stuff, …take your index finger, place it on your chest, and repeat 'I am the problem.'" (p. 32)

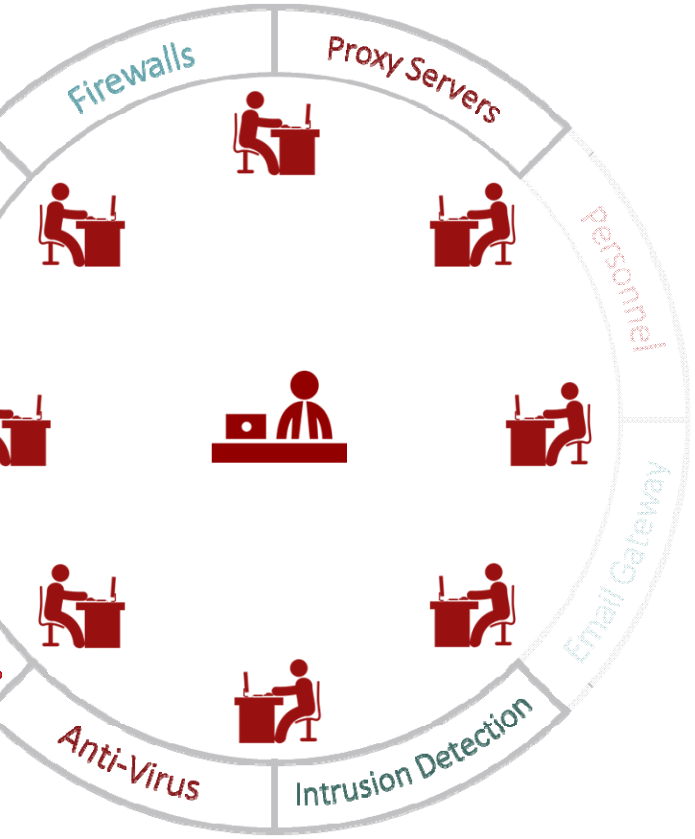
Vast majority of compromises beachhead with people (p. 31)

Time from compromise to data theft is trending downward (p. 6)

50k out of 80k incidents are in public entities (p. 3)

No silver bullet

o Err is Human

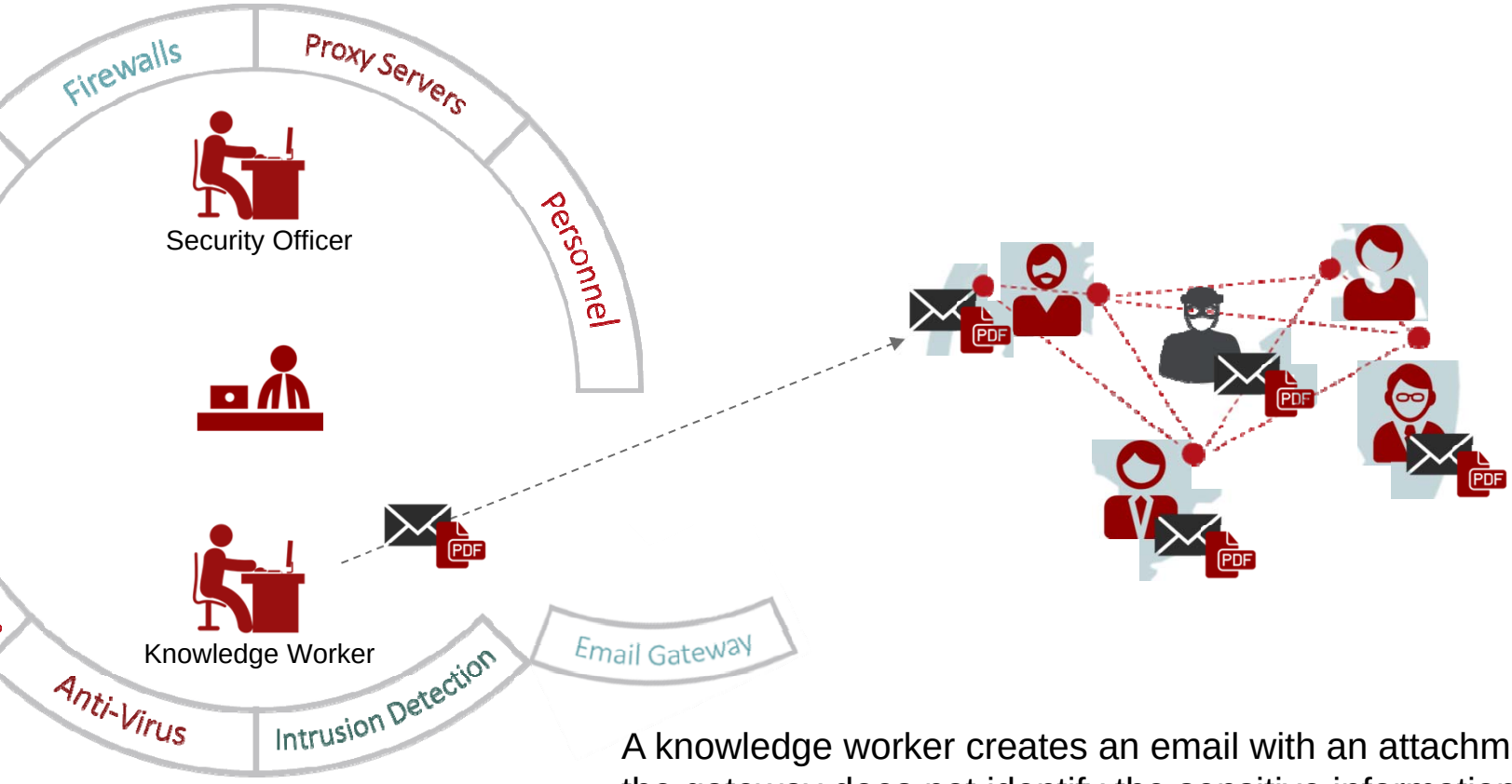


No matter how large your security budget, gaps will still exist.

No matter how well trained your staff is, they will still:

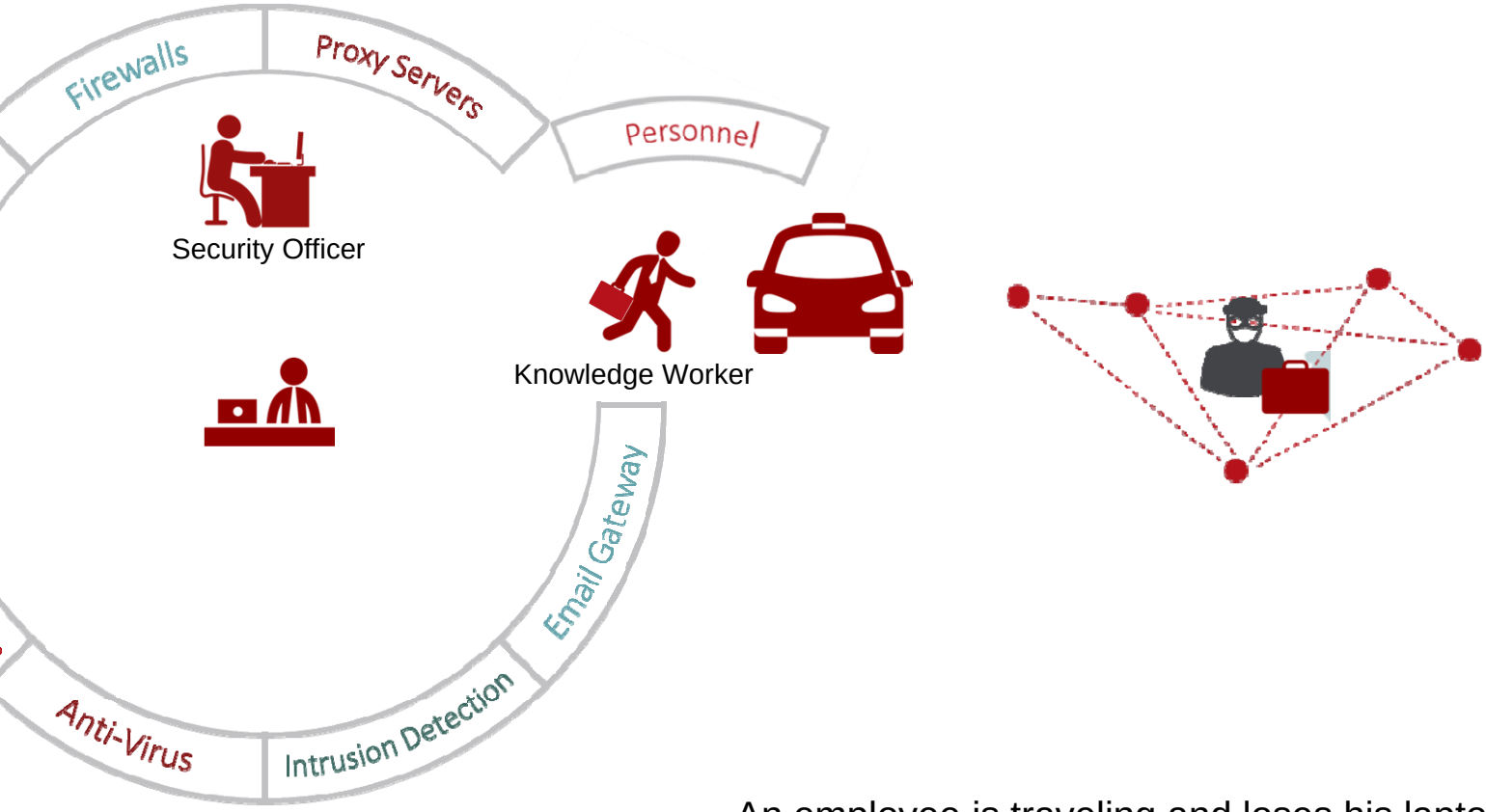
- Keep sensitive material on unsecured devices
  - Laptops
  - Desktops
  - Email servers
- Misplace company property
  - Laptops
  - Mobile devices
  - USB drives
- Send emails with sensitive information attached

xample 1 :: Email with Risky Attachment



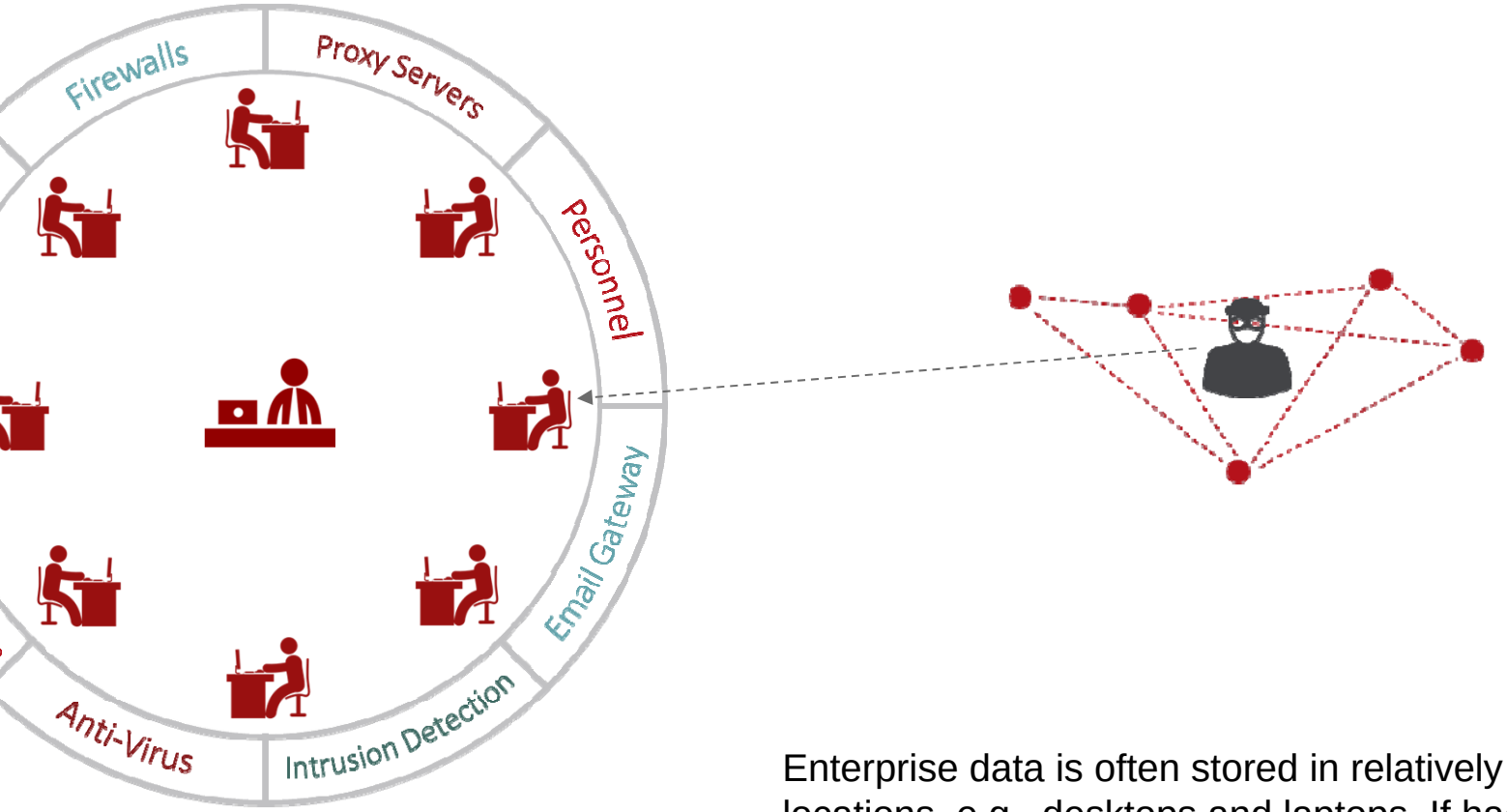
A knowledge worker creates an email with an attachment; the gateway does not identify the sensitive information contained in the attachment, so it is allowed to be sent.

xample 2 :: Lost Work Device



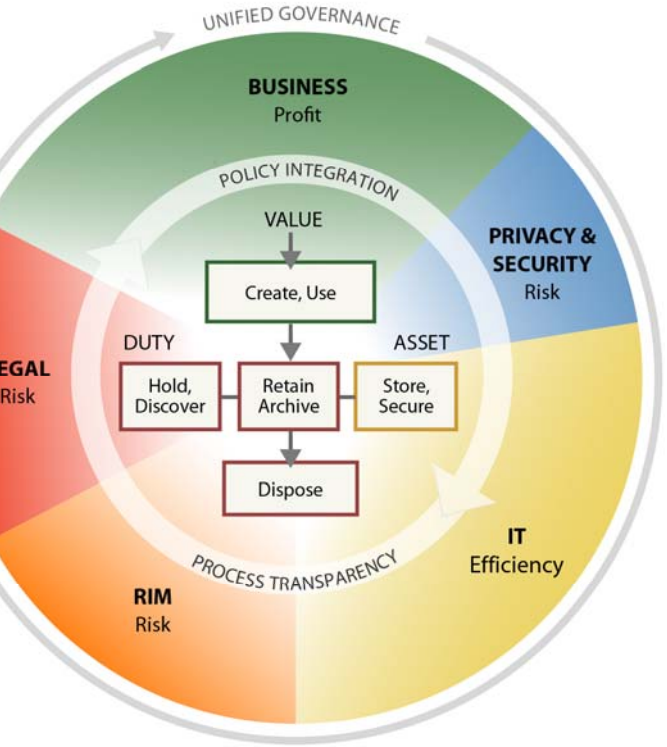
An employee is traveling and loses his laptop. Did the machine have any sensitive information on it?

xample 3 :: Sensitive Data in Risky orage



Enterprise data is often stored in relatively risky locations, e.g., desktops and laptops. If hacked, even within the enterprise network, these systems are much more vulnerable than a DMS.

nforce Information Governance



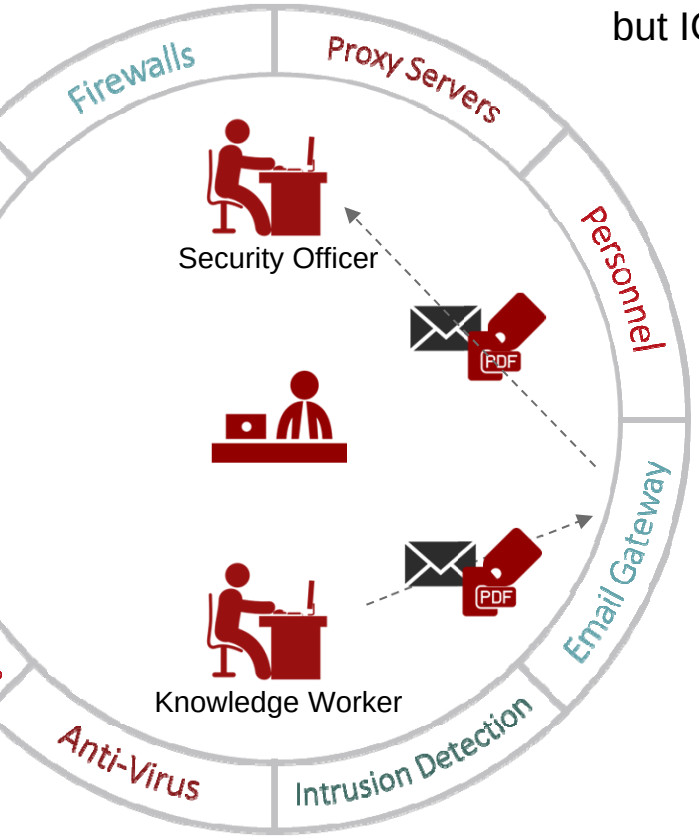
BECOME CONTENT-AWARE

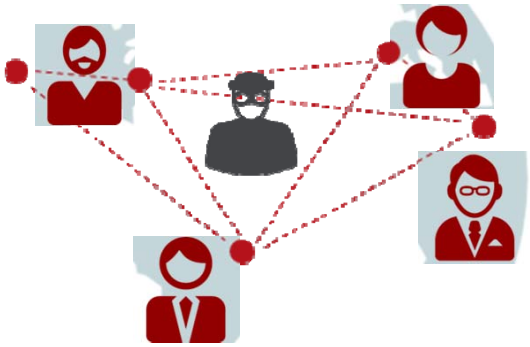
IG software can provide content-centric data visibility and classification, which significantly improve your organization's baseline security protections.

- Track and control data at its source and in real time, helping to mitigate the inevitable human error.
- Use document classification to inform existing security systems to enforce smarter rules
- Scan and index content on business devices so that the organization can quickly assess risk if a device is lost or stolen
- Proactively remove the most sensitive information from devices that are not properly secure to house it

xample 1 :: Email with Risky Attachment

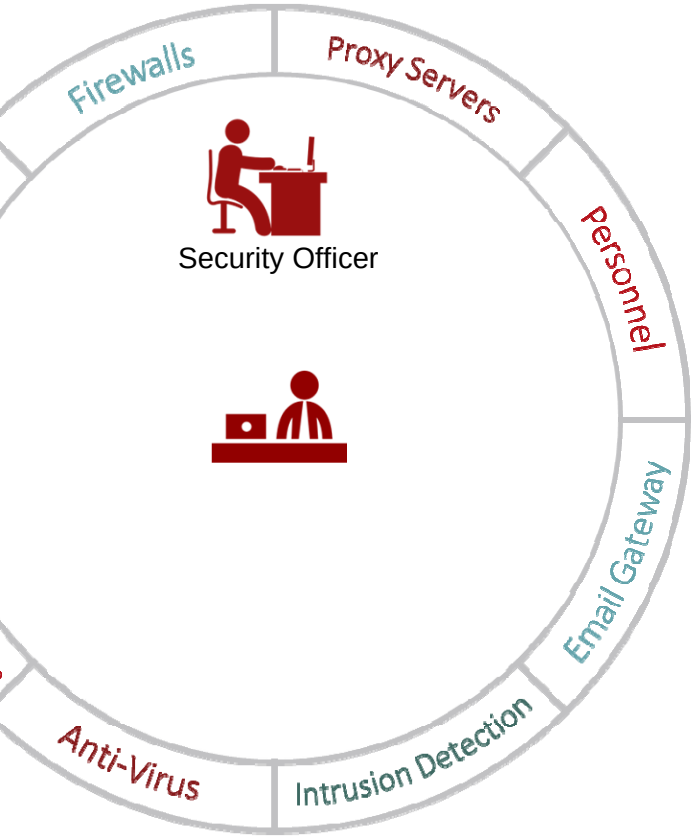
A knowledge worker prepares an email with attachment, but IG software tags the content as sensitive.





The gateway recognizes the tag, the security officer is notified of the threat, and the attachment can be revised to protect sensitive content.

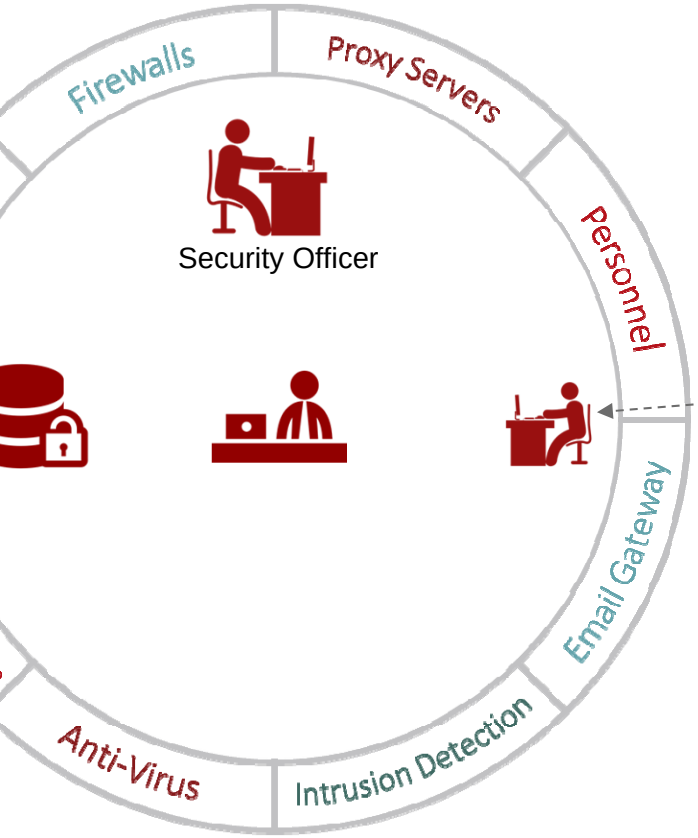
xample 2 :: Lost Work Device

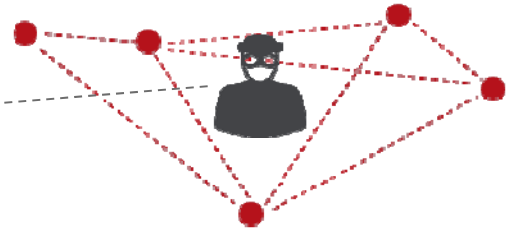


0110100100101
0010010110010
1001011010010
0101010011101
0100101001101
0100101001001
0010010010010
0010010010100
10010101

IG software scans all company devices, meaning that organizations know exactly what information poses a risk if a device goes missing.

xample 3 :: Sensitive Data in Risky orage





IG policies and enforcement technology ensure that sensitive content is regularly moved to secure locations, keeping it out of reach from hackers.

&A

?

he End.

ank you!

Michael McCutcheon
Chief Solution Officer
MMcCutcheon@RationalEnterprise.com
NYC Office | +1 212.719.4444