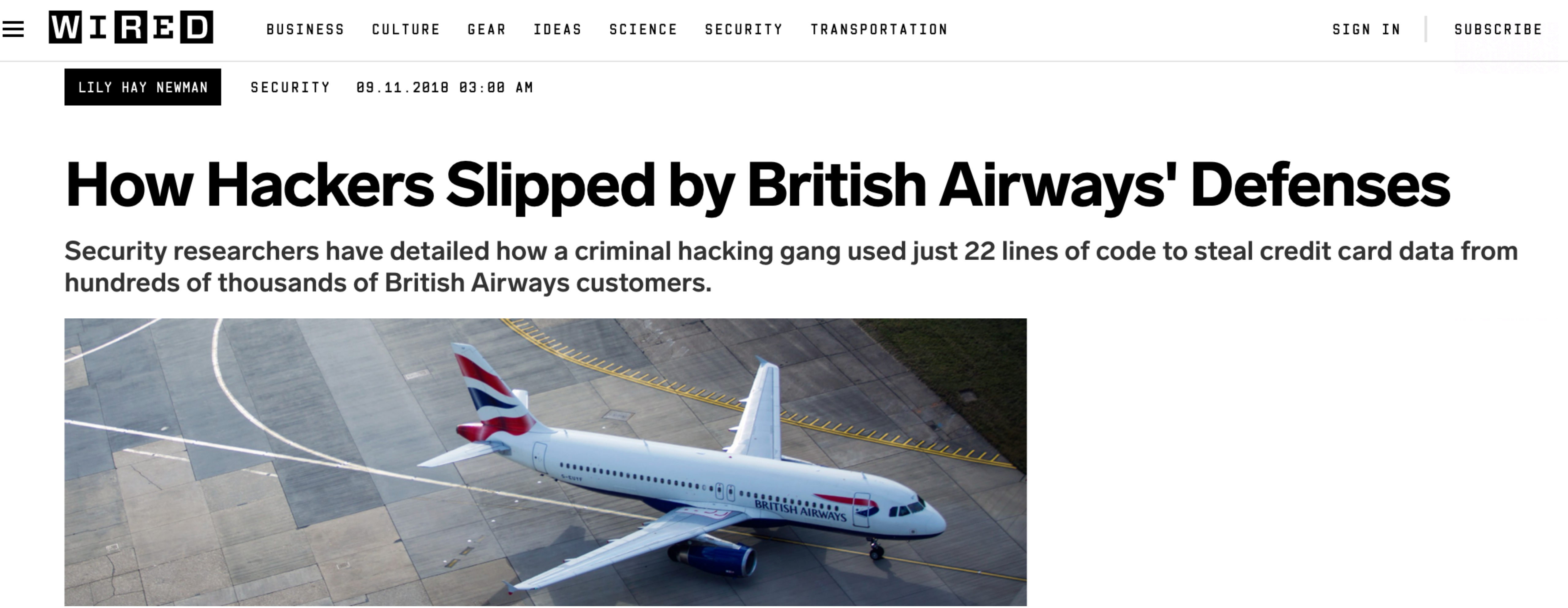
Security Assurance in an Agile world

30th October – ISACA SecureIT Conference 2019

Application based hacks are still a problem

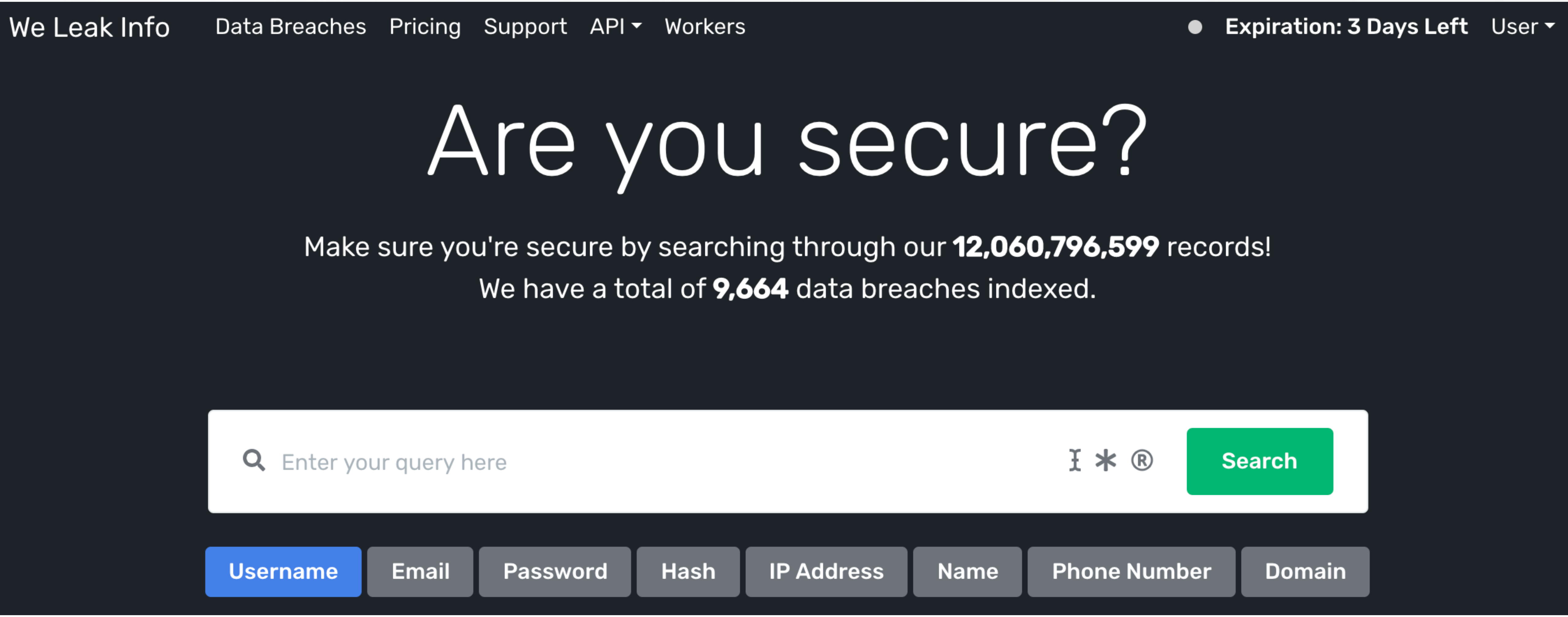


LILY HAY NEWMAN SECURITY 09.11.2018 03:00 AM

How Hackers Slipped by British Airways' Defenses

Security researchers have detailed how a criminal hacking gang used just 22 lines of code to steal credit card data from hundreds of thousands of British Airways customers.

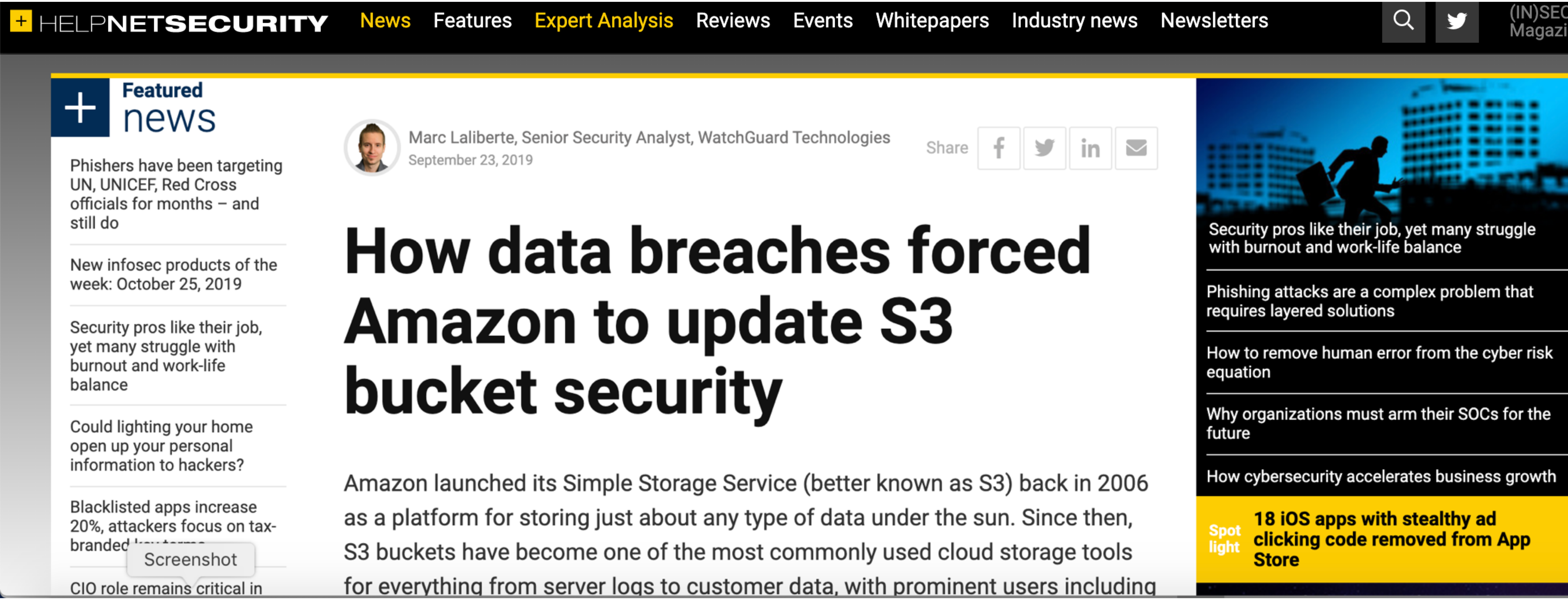
Breached credentials are being mined and weaponized



Are you secure?

Make sure you're secure by searching through our **12,060,796,599** records!
We have a total of **9,664** data breaches indexed.

New vectors of attack – Data Warehouses



Featured news

Phishers have been targeting UN, UNICEF, Red Cross officials for months – and still do

New infosec products of the week: October 25, 2019

Security pros like their job, yet many struggle with burnout and work-life balance

Could lighting your home open up your personal information to hackers?

Blacklisted apps increase 20%, attackers focus on tax-branded

CIO role remains critical in

Marc Laliberte, Senior Security Analyst, WatchGuard Technologies
September 23, 2019

How data breaches forced Amazon to update S3 bucket security

Amazon launched its Simple Storage Service (better known as S3) back in 2006 as a platform for storing just about any type of data under the sun. Since then, S3 buckets have become one of the most commonly used cloud storage tools for everything from server logs to customer data, with prominent users including

Security pros like their job, yet many struggle with burnout and work-life balance

Phishing attacks are a complex problem that requires layered solutions

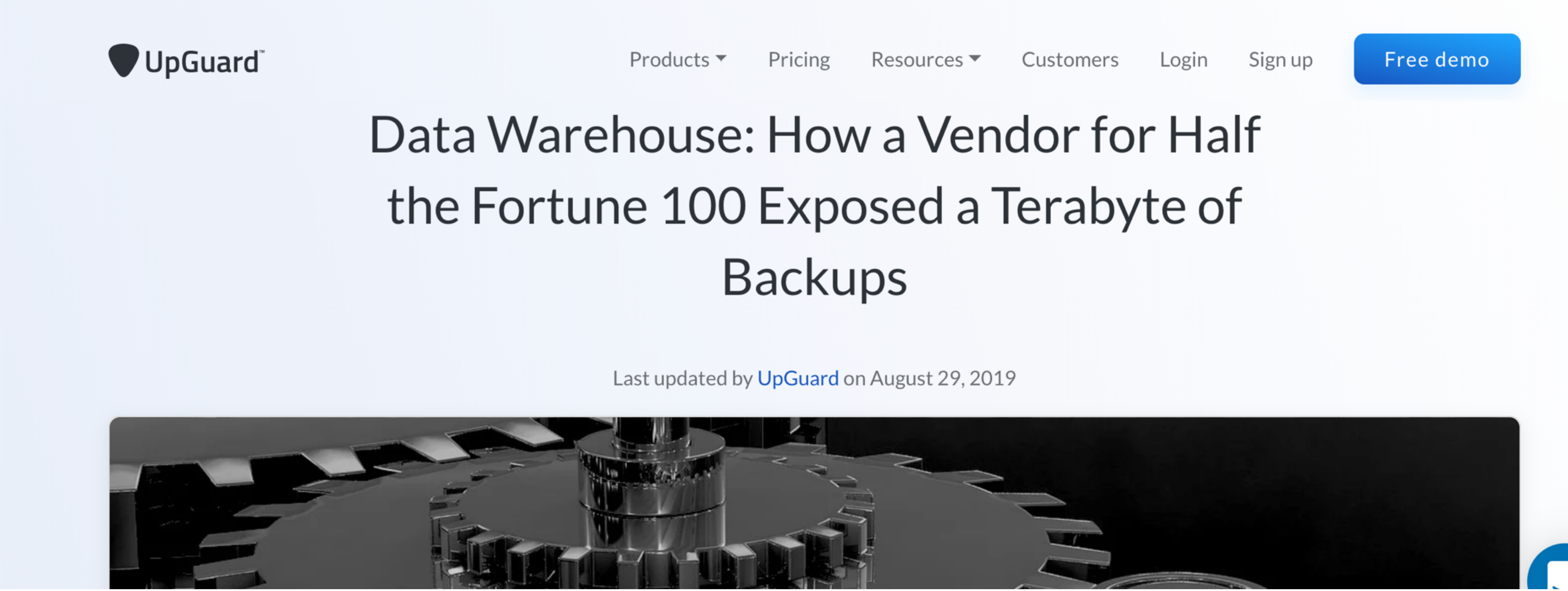
How to remove human error from the cyber risk equation

Why organizations must arm their SOCs for the future

How cybersecurity accelerates business growth

Spot light 18 iOS apps with stealthy ad clicking code removed from App Store

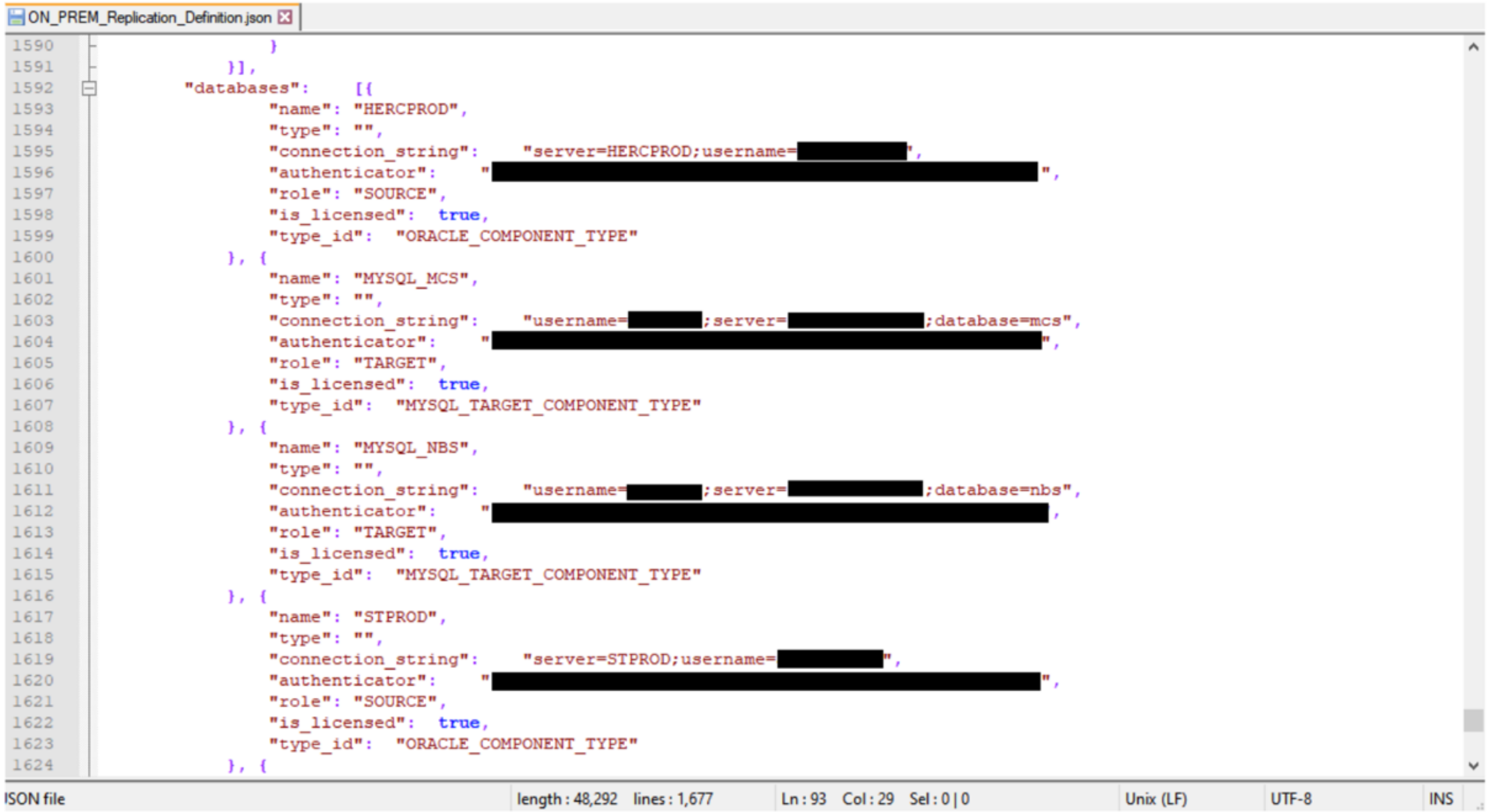
New vectors of attack – Supply Chain



Data Warehouse: How a Vendor for Half the Fortune 100 Exposed a Terabyte of Backups

Last updated by UpGuard on August 29, 2019

New vectors of attack – Code and Keys

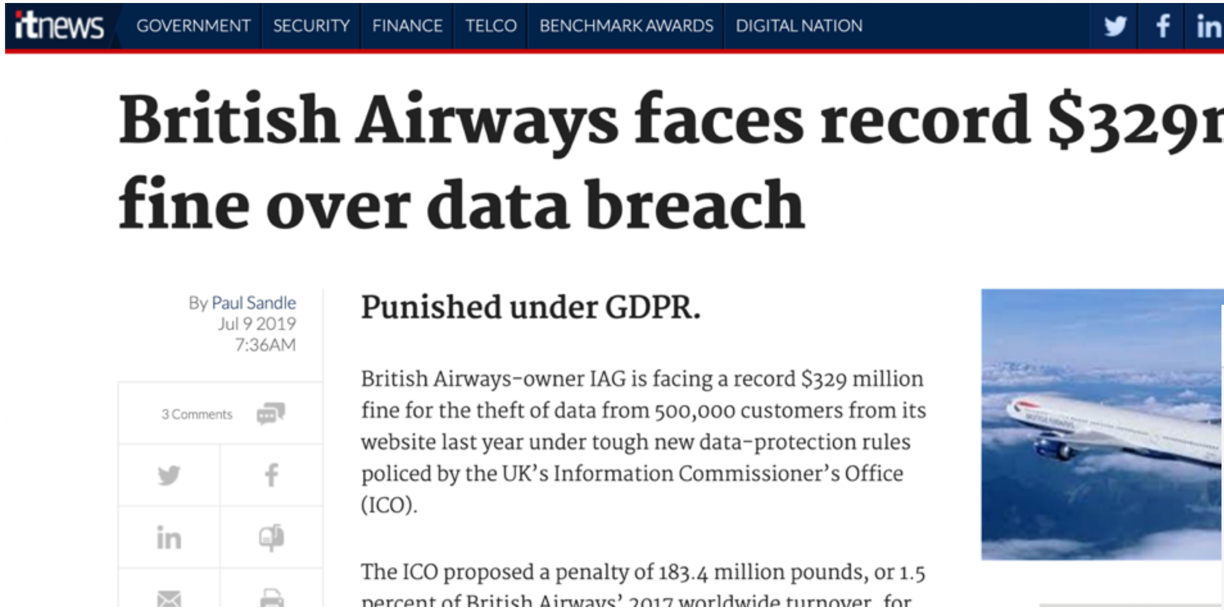


```
            }
        }],
    "databases":    [{
            "name": "HERCPROD",
            "type": "",
            "connection_string":    "server=HERCPROD;username=[redacted]",
            "authenticator":    "[redacted]",
            "role": "SOURCE",
            "is_licensed":  true,
            "type_id":  "ORACLE_COMPONENT_TYPE"
        }, {
            "name": "MYSQL_MCS",
            "type": "",
            "connection_string":    "username=[redacted];server=[redacted];database=mcs",
            "authenticator":    "[redacted]",
            "role": "TARGET",
            "is_licensed":  true,
            "type_id":  "MYSQL_TARGET_COMPONENT_TYPE"
        }, {
            "name": "MYSQL_NBS",
            "type": "",
            "connection_string":    "username=[redacted];server=[redacted];database=nbs",
            "authenticator":    "[redacted],
            "role": "TARGET",
            "is_licensed":  true,
            "type_id":  "MYSQL_TARGET_COMPONENT_TYPE"
        }, {
            "name": "STPROD",
            "type": "",
            "connection_string":    "server=STPROD;username=[redacted]",
            "authenticator":    "[redacted]",
            "role": "SOURCE",
            "is_licensed":  true,
            "type_id":  "ORACLE_COMPONENT_TYPE"
        }, {
```

Netflix database authentication strings.

ES2 ES2 PEOPLE ES2 KIDS ES2 INCIDENT RESPONSE

Regulatory Compliance is driving security objectives



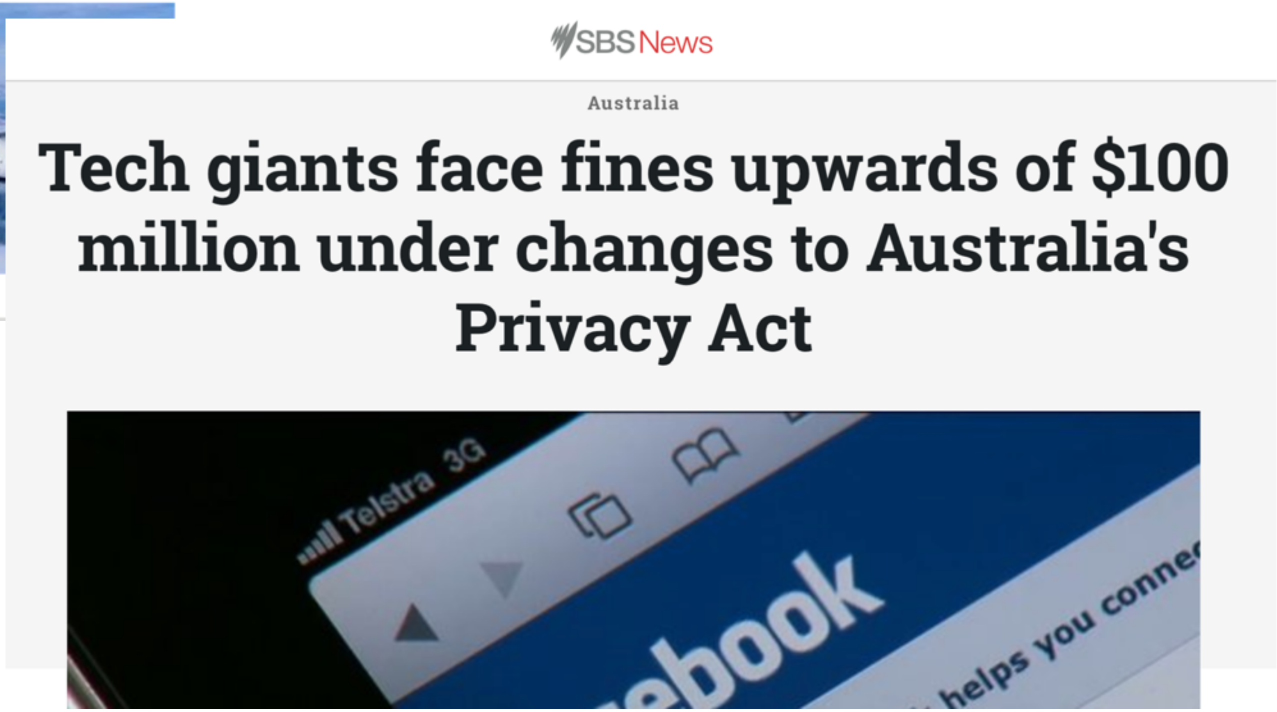
British Airways faces record $329m fine over data breach

By Paul Sandle
Jul 9 2019
7:36AM

Punished under GDPR.

British Airways-owner IAG is facing a record $329 million fine for the theft of data from 500,000 customers from its website last year under tough new data-protection rules policed by the UK's Information Commissioner's Office (ICO).

The ICO proposed a penalty of 183.4 million pounds, or 1.5 percent of British Airways' 2017 worldwide turnover, for



Australia

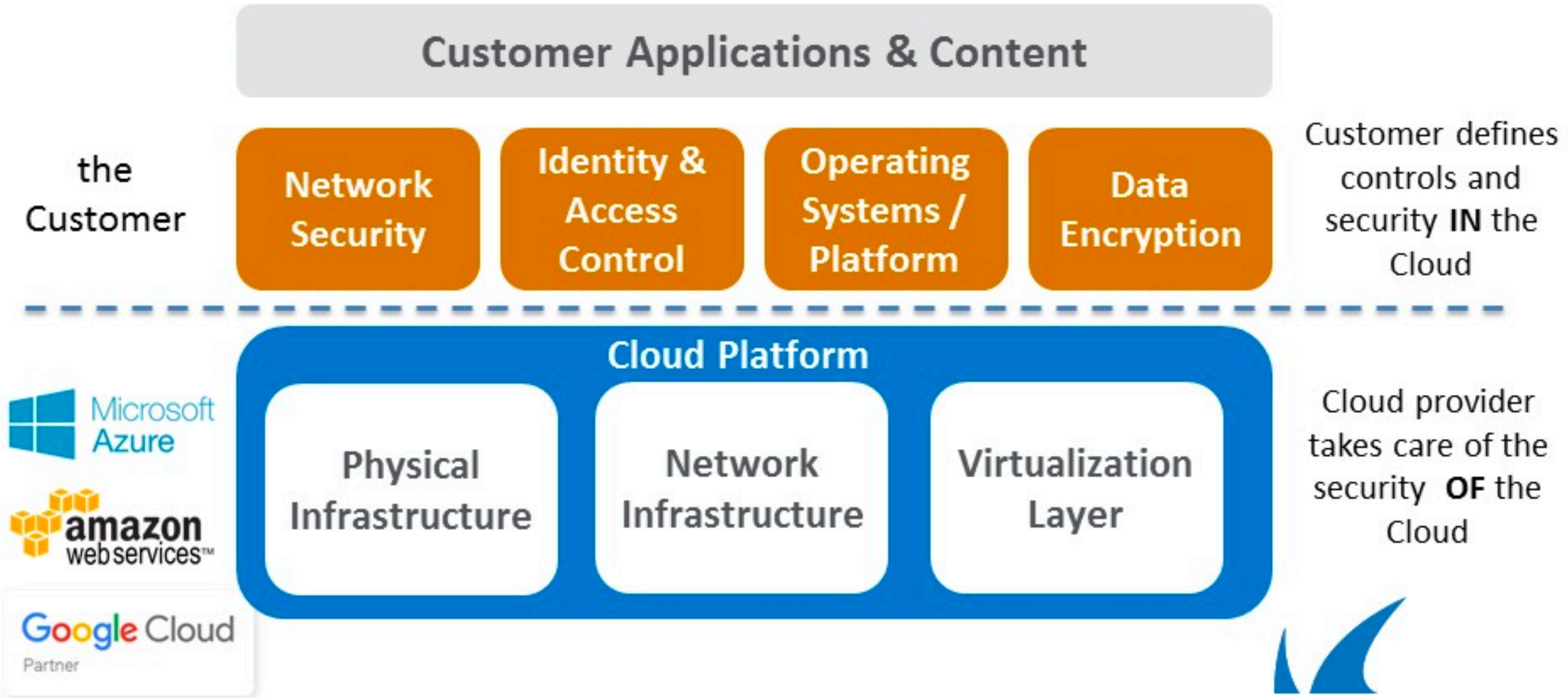
Tech giants face fines upwards of $100 million under changes to Australia's Privacy Act

ES2 ES2 PEOPLE ES2 KIDS ES2 IR INCIDENT RESPONSE

Businesses are moving to the Cloud

- Dashboards
- Data Management
- Data Retention
- Data Analytics
- Data Loss
- Serverless Workloads
- Cloud Native Applications

Shared Responsibility Model



Customer Applications & Content

the Customer

Network Security

Identity & Access Control

Operating Systems / Platform

Data Encryption

Customer defines controls and security **IN** the Cloud

Cloud Platform

Physical Infrastructure

Network Infrastructure

Virtualization Layer

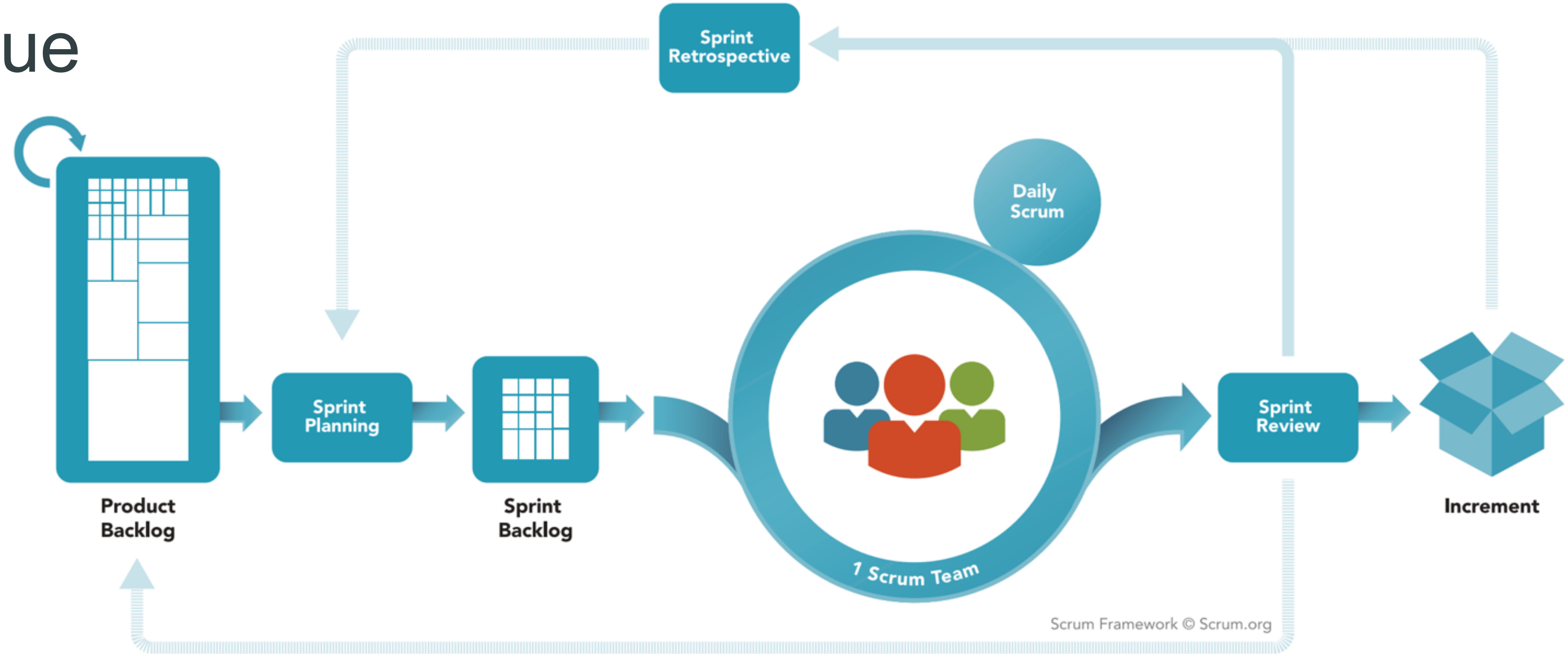
Cloud provider takes care of the security **OF** the Cloud

Source: https://smartermsp.com/ask-msp-expert-important-secure-public-cloud/

Maintaining Security in an Agile Environment

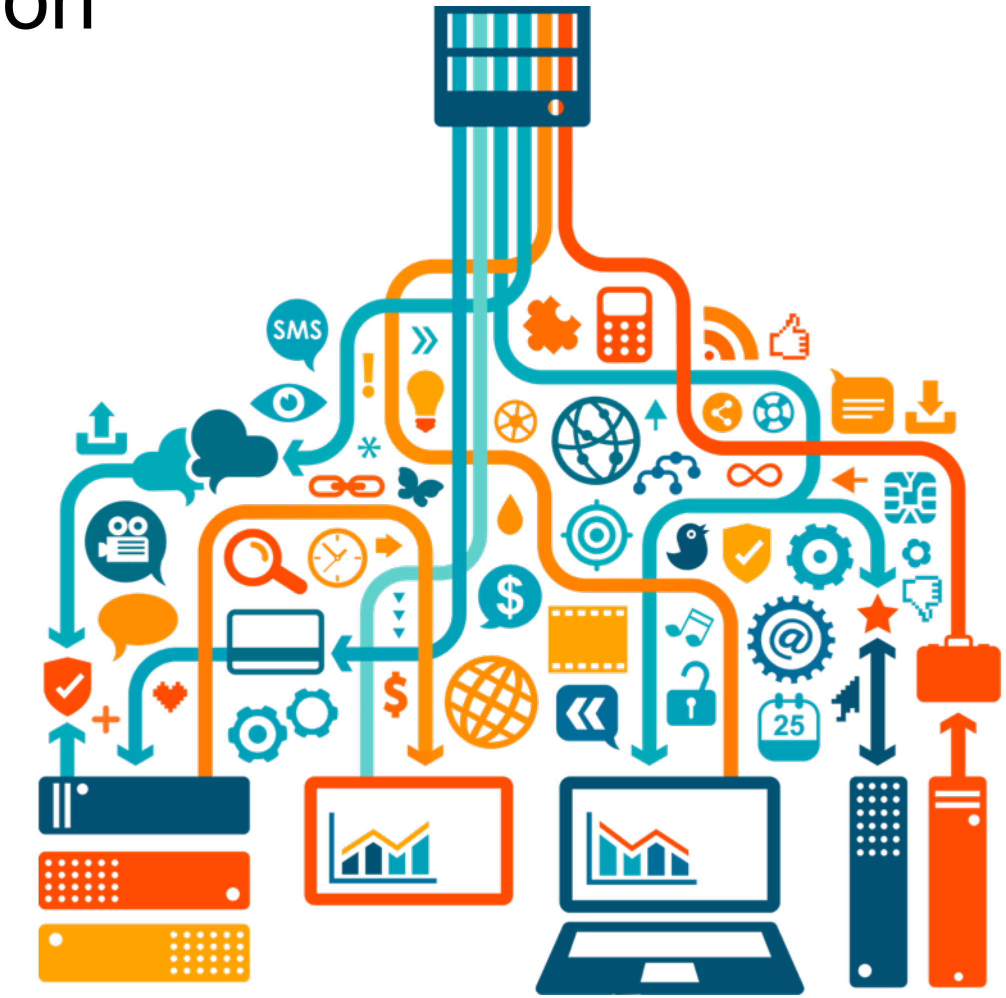
Why Agile?

- Anticipate Change
- Stay flexible
- Focus on Value



When is a good time to discuss Security

- When building, **significantly modifying**, or implementing a system or application



When should Security teams get involved

- Implementing a new system or application (On-Premise, IaaS, PaaS, SaaS)
- Significantly modifying an existing system or application (API, Authentication, Databases)
- Like-for-like migrations to new platform (Cloud)
- ~~Like-for-like migration within existing platforms~~
- ~~Minor software release or upgrade~~
- Major software release or upgrade
- ~~Minor code changes (feature / form / function)~~
- Major code changes (feature / form / function)
- Increase in System Criticality or Sensitivity level

Why Security Assurance

- Re-enforce Company Policies & Standards
- Discuss Privacy and Security Requirements & Risks
- Provide Clear Guidance
- Recommend Controls
- Validate Controls
- Test Controls

Agile poses new security challenges

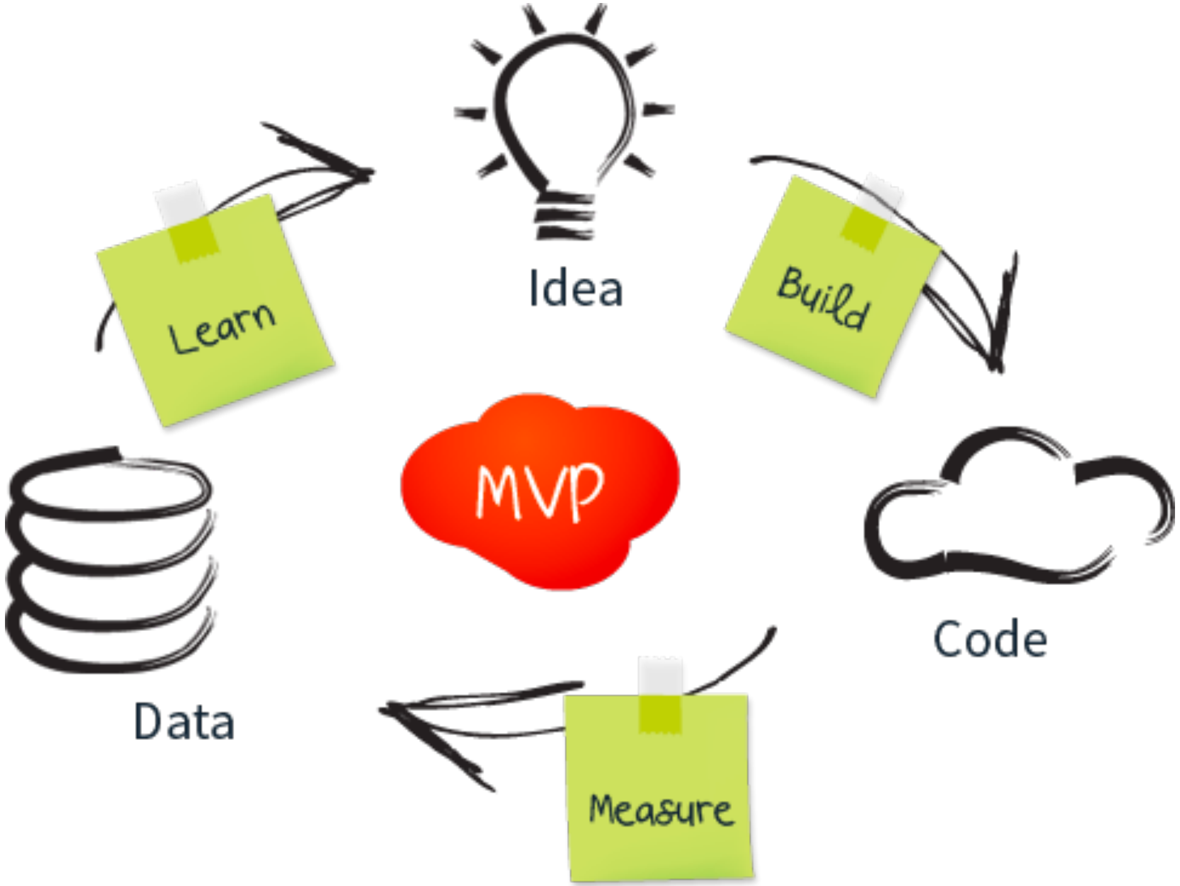
- Minimal Security Knowledge
- Reduced documentation
- No Security Architecture
- No Threat Modelling
- Limited Risk assessments
- Late Security Testing adds delays and reduces agility

MVPs are designed to accelerate time to deliver

Minimal **V**iable **P**roduct

- 1 – 2 sprints
- Clear Requirements

CORE FUNCTIONS
FOCUS ON VALUE
EARLY ADOPTION
FEATURE BASED



ES² ES² PEOPLE ES² KIDS ES² IR INCIDENT RESPONSE

Understanding where the magic happens

- Inception planning
- Sprints
- Walls
- Daily Stand ups
- Showcases / Demos
- Retrospectives

Even IT Operations teams are becoming more agile

- DevOps
- Full Stack
- Infrastructure as code
- Continuous Integration (CI)
- Continuous Delivery (CD)

Successfully building Security into Agile

- Embed the security team within the squads / ceremonies
- Implement Security Controls as code
- Test Security Controls in Code
- Increase Code Quality / Security
- Audit Common Security Controls automatically (CIS/ASD/NIST)

The key focus areas

- Secure Development Lifecycle (SDLC)
- Testable Standards
- Secure Code reviews as part of pipeline
- Uplift Non-production environments
- Check Open Source / Dependencies
- Learn development platforms and tools

So when is the right time to assess Security

- Not at the end
- Ideal within key sprints
- Educate & Empower Development teams
- Embed Security as a Peer review process

New challenges require new tools

IAST – Interactive Application Security Testing
VMS - Vulnerability Management Systems
CM – Configuration Management

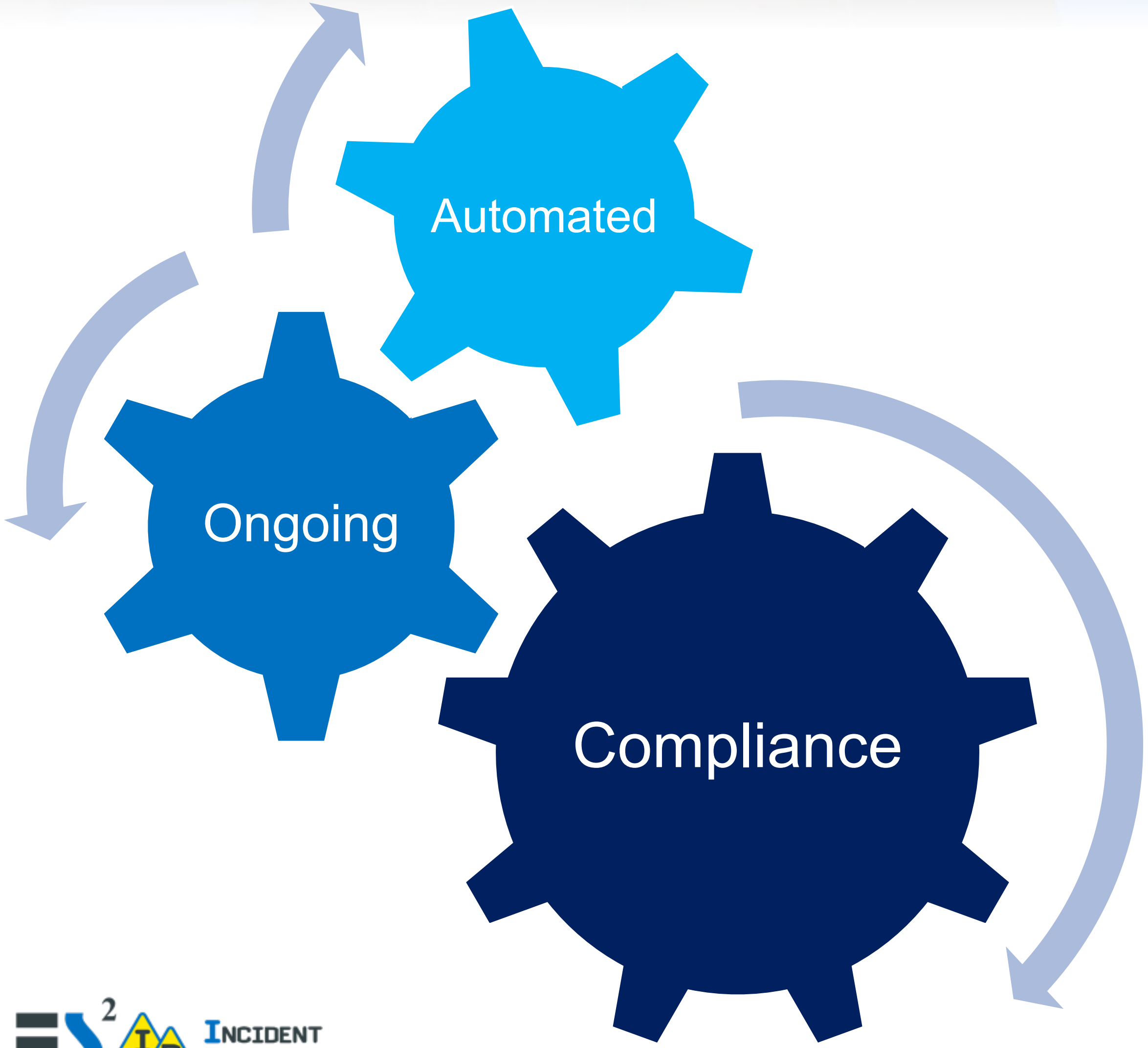
DAST – Dynamic Application Security testing
-
SAST – Static Application Security testing

Amazon GuardDuty, AWS Security Hub, Amazon Inspector
-
Azure Policy, Secure Score, Secure DevOps Kit
-
CIS Assessment Tool

Amazon Macie
-
Azure Information Protection Scanner
-
Enterprise Recon
-
S3 Scanner

SIEM – Security Incident & Event Monitoring
-
EDR – Endpoint Detection & Response
-
SOAR – Security Orchestration, Automation & Response

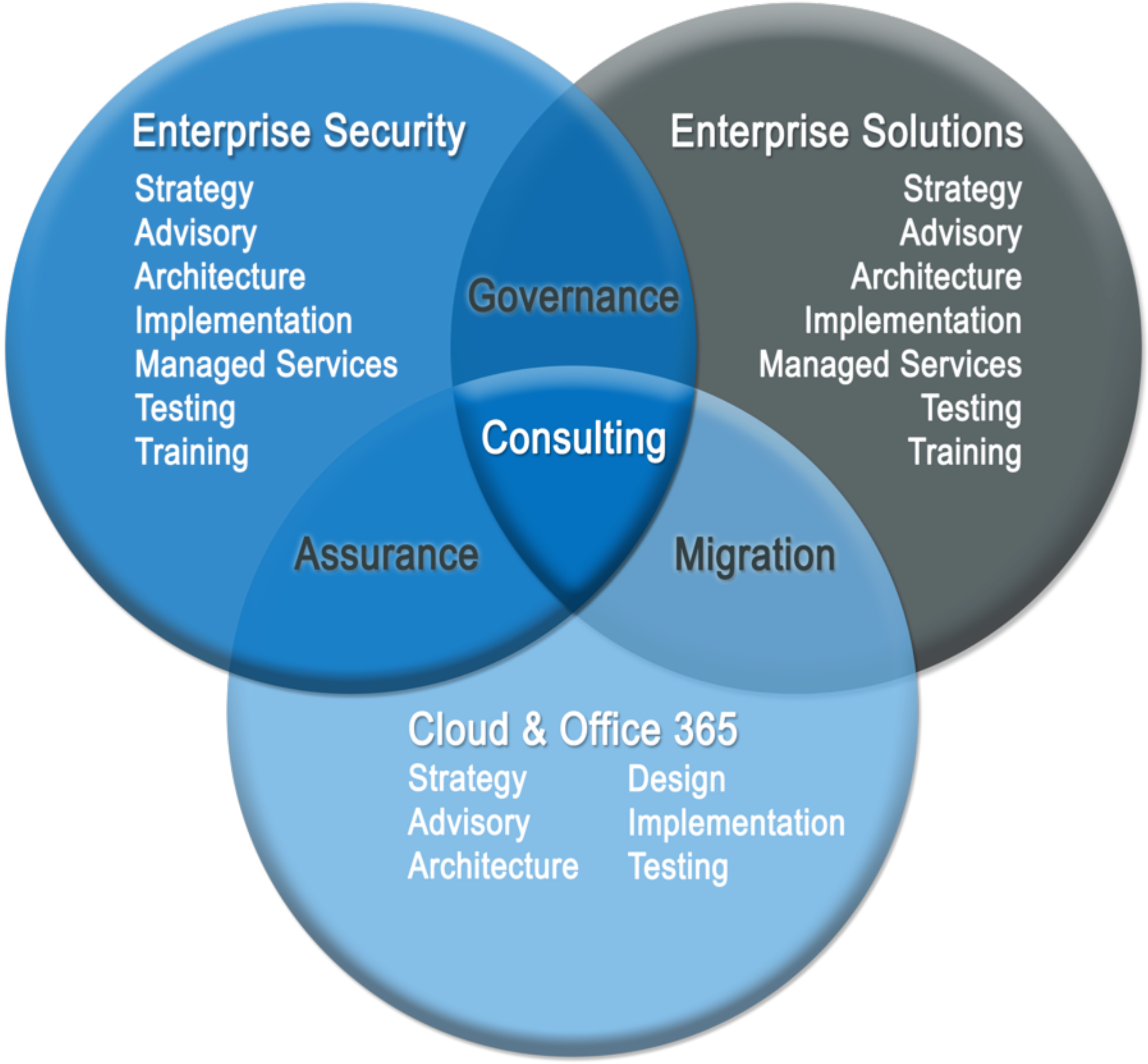
The Holy Grail



Questions?

Andy Battle
Chief Technology Officer
0449 985169

https://www.linkedin.com/in/andybattle/



Enterprise Security
Strategy
Advisory
Architecture
Implementation
Managed Services
Testing
Training

Enterprise Solutions
Strategy
Advisory
Architecture
Implementation
Managed Services
Testing
Training

Governance

Consulting

Assurance

Migration

Cloud & Office 365
Strategy
Advisory
Architecture
Design
Implementation
Testing