TechDefcon.com

Connected World. Connected Experiences.

ENTERPRISE SECURITY & RISK MANAGEMENT (ESRM)

Securing the Enterprise

Organizations want to grow business rapidly through adopting new technologies.
Our job is to help CISOs enable that growth by managing risk accordingly and not hindering that business momentum.

Connect with us: ESRM@TechDefcon.com

click here for website

ESRM Capabilities Overview

Delivery Approach

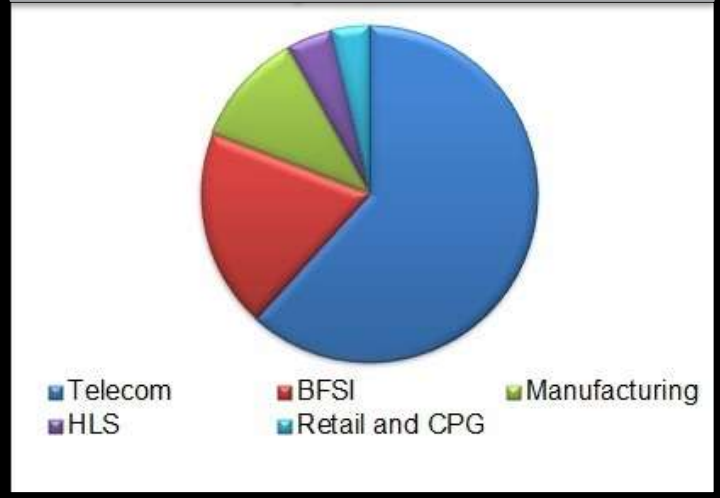
- End-to-end **Intelligent** Enterprise security services
- Guide clients through **digital transformation** while keeping them secure
- Deep **know-how** of security products

ESRM Capabilities

- **Our Partnerships Comprise of: -**
- **1 of Top 30** Security Consulting companies in Gartner's Market Guide, 2016
- **750+** dedicated security specialists
- **140+ large enterprise clients including 5 Fortune 20 clients**
- **15+** years practice of Cyber Security Services
- **Track record of successful delivery of 500+ large security outsourcing projects**
- **60+ Security OEMS and MSSP Partners**

Customer profile

By vertical



By geography

Securing Enterprises Across Verticals

- Telecommunication services
- Banking & Financial services
- Manufacturing
- Healthcare
- Energy & Utility
- Retail
- Media & Entertainment

Fortune Global 500 Clients

7 Telecommunications

5 Banking & Financial services

4 Manufacturing

3 Technology

TechDefcon.com Risk Management DNA

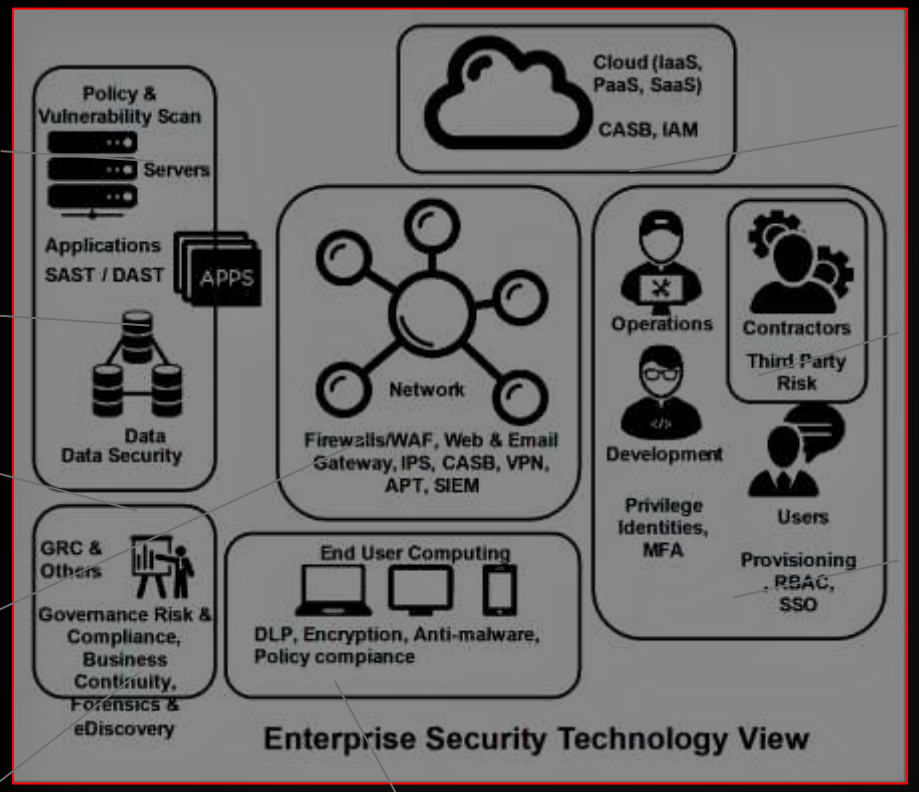
- Vulnerability management
- Penetration testing
- Policy compliance
- Antimalware, encryption, HSM

- Advanced persistent Threat mgmt.
- Vulnerability Engineering

- Data protection program, DLP, DAM, Encryption, tokenization,

- Designing defensive network
- Micro segmentation, NAC
- Public, private and hybrid cloud ready design

- RSA Archer automation or IT GRC, ERM, Audit and BCM
- eDiscovery and Forensics



- Security policy compliance
- Data classification, discovery and protection

- Cloud security strategy
- Cloud Security with zones, firewalls, IPS, CASB, federation, monitoring, forensics

- Vendor risk management program
- Risk bases assessment models

- IAM strategy & policy definition
- Identity governance & admin
- Role based access governance
- Internal and external SSO,
- Privilege identity management with multi-factor support
- Risk based authentication techniques i.e. biometric
- Password vaults and service accounts management

We offer Advisory, Protection , Monitoring & Remediation services in our risk based portfolio

AUTHENTICATION FOR SWIFT

The Problem

1. NO PROTECTION ON SWIFT LOGINS BEYOND USERNAME/PASSWORD

2. PRONE TO IDENITY TAKEOVERS

THE MANDATE

2017

Ref: https://www.swift.com/ordering-support/security-guidelines

1.2 2-step verification

2-step verification is a security measure that helps protect your account from unauthorised access if someone manages to obtain your password. An additional layer of security requires a verification code to be entered along with your username and password.

This code can be delivered to you by SMS, voice message, or e-mail. SMS and voice message are the preferred means of delivering the verification code. This is because your e-mail address is already linked to your swift.com account and an external means of providing the authentication code is favoured.

Note that the secure channel application on swift.com uses a one-time password to secure each transaction that involves sensitive data. Security officers accessing the application must use their personal secure code card to generate the required one-time passwords.

Case Study (2FA): SWIFT

Case Study

Problem

- Compliance with SWIFT Mandate
- Vulnerable to Global SWIFT hacks
- No inclination for Open Source Products like Google Authenticator

Top 5 largest Bank of India

Protecting 500 Users for SWIFT with Mobile Soft Token and Hardware Tokens

Added Benefits

- Integration-Ready plugin for SWIFT application
- Compliance Mandate achieved ahead of time

"The Solution has responded to global threat of SWIFT hacking by building a quick ready-to integrate plugin for SWIFT application. With bank hesitant to try anything open such as Google Authenticator for a critical financial application such as SWIFT, the solution provided a quick and fast manner to protect our SWIFT users and thereby, complying to SWIFT mandate quickly."

COMPREHENSIVE AUTHENTICATION SUITE FOR TEMENOS

COMPREHENSIVE AUTHENTICATION SUITE FOR TEMENOS

eKYC

Biometrics

Behavioral Authentication

Keyboard Dynamics
PIN
GAIT

TEMENOS
The Banking Software Company

T24
TCIB
TCMB

OUR AUTHENTICATION SOLUTION

Risk based
Adaptive Authentication

One Time
Password
(100% coverage)

Case Study (2FA): Bank in Cambodia – Temenos

Case Study

Problem

- Authentication for Temenos Product TCIB
- Internet Banking
- 13,000 users

Cambodia's First & Foremost Bank

1FA (Username/Password)

- 2FA Hardware Tokens
- 2FA Mobile Soft Tokens with PUSH OOB, protected with PIN and Biometric TouchID

Added Benefits

- Cost Effective
- Scalable
- Temenos Certified
- Future-Ready
- Risk- based Adaptive Authentication
- Behavioral Analytics
- Biometrics
- eKYC

Case Study: Bank in the UK – Protect PCI data

Case Study

Challenges

- Brand new bank selected FISERV to provide a hosted core banking system and card processing service.
- Bank subsequently found that FISERV do not provide any data security or PCI compliance with the hosted service.
- Bank did not want any of their IT estate to contain clear PANs in order to reduce their scope for PCI audit.

Requirements

- Protect all PCI data between the Digital Bank's estate and FISERV before it hits Bank's estate in the clear. Ensure clear data is sent back to FISERV for processing.
- Solution must be hosted in a PCI compliant environment and fully managed 24/7.
- Data must be format preserved and tokenised in order that all systems remain out of scope for PCI audit.
- Solution must be able to scale as the new bank grows in complexity.

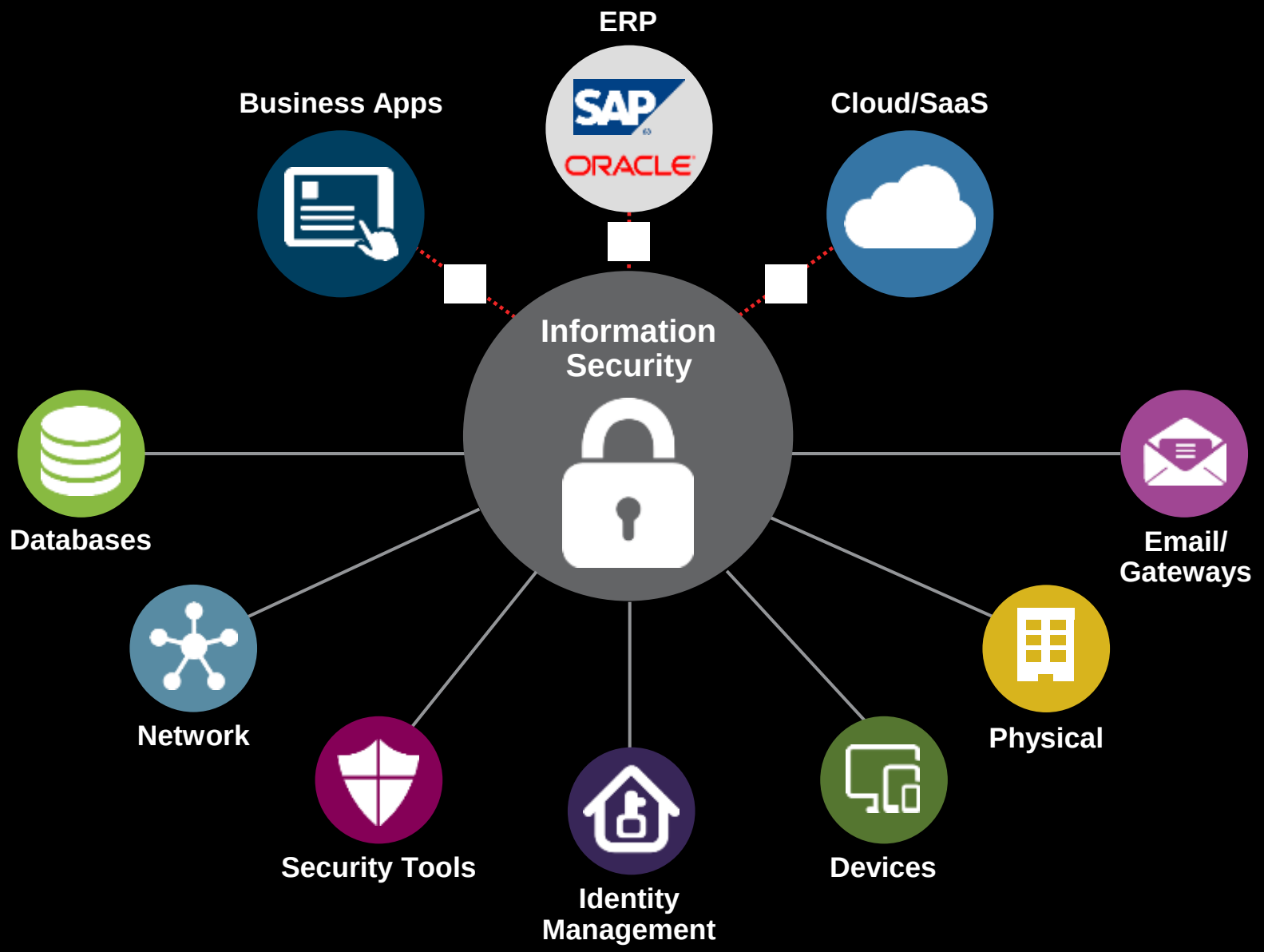
Solution

- Enterprise Security Administrator
- Data Security Gateway
- Tokenise and detokenise all PANs between Fiserv and the Bank

Business Apps Integration with Compliance Automation tool

Information Security's Blind Spot

Business Applications, Cloud & ERP



Why are Business Applications a Blind Spot for Security?

- [ ] **WHO?**
- [ ] **WHAT?**
- [ ] **WHEN?**
- [ ] **WHERE?**
- [ ] **HOW?**

Current tools focus on the potential **SECURITY ISSUE**	Infrastructure	Vulnerabilities	Intrusions
	Perimeter	Viruses	Identities
Security solutions should focus on the actual **BUSINESS IMPACT**	ERP	Cloud	Business Apps
	Financials	Critical Data	Master Data
	Access	Activity	Transactions
	Risk	Compliance	Exposure

A single pane of glass for Information Security

Business Context

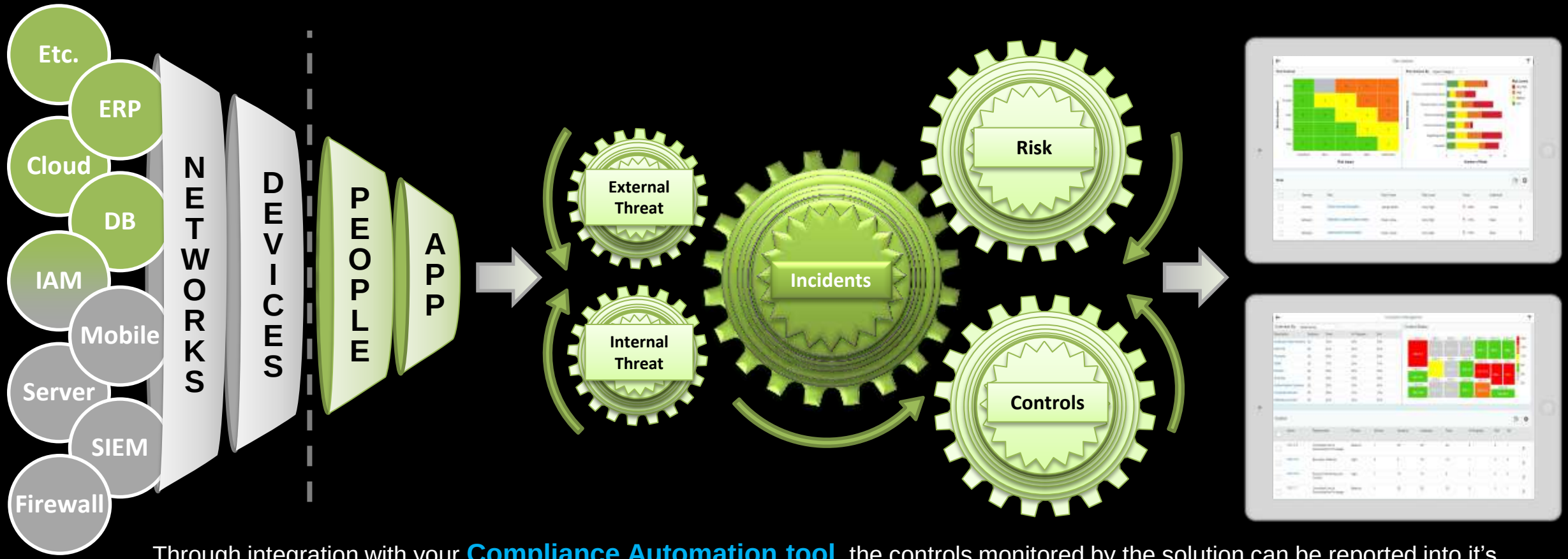
Governance across **networks**, **devices**, **applications** and **people**

Security Analytics

Advanced analytics linking **business** and **IT context**

Strategic Reporting

Actionable **security risk** for your **business**



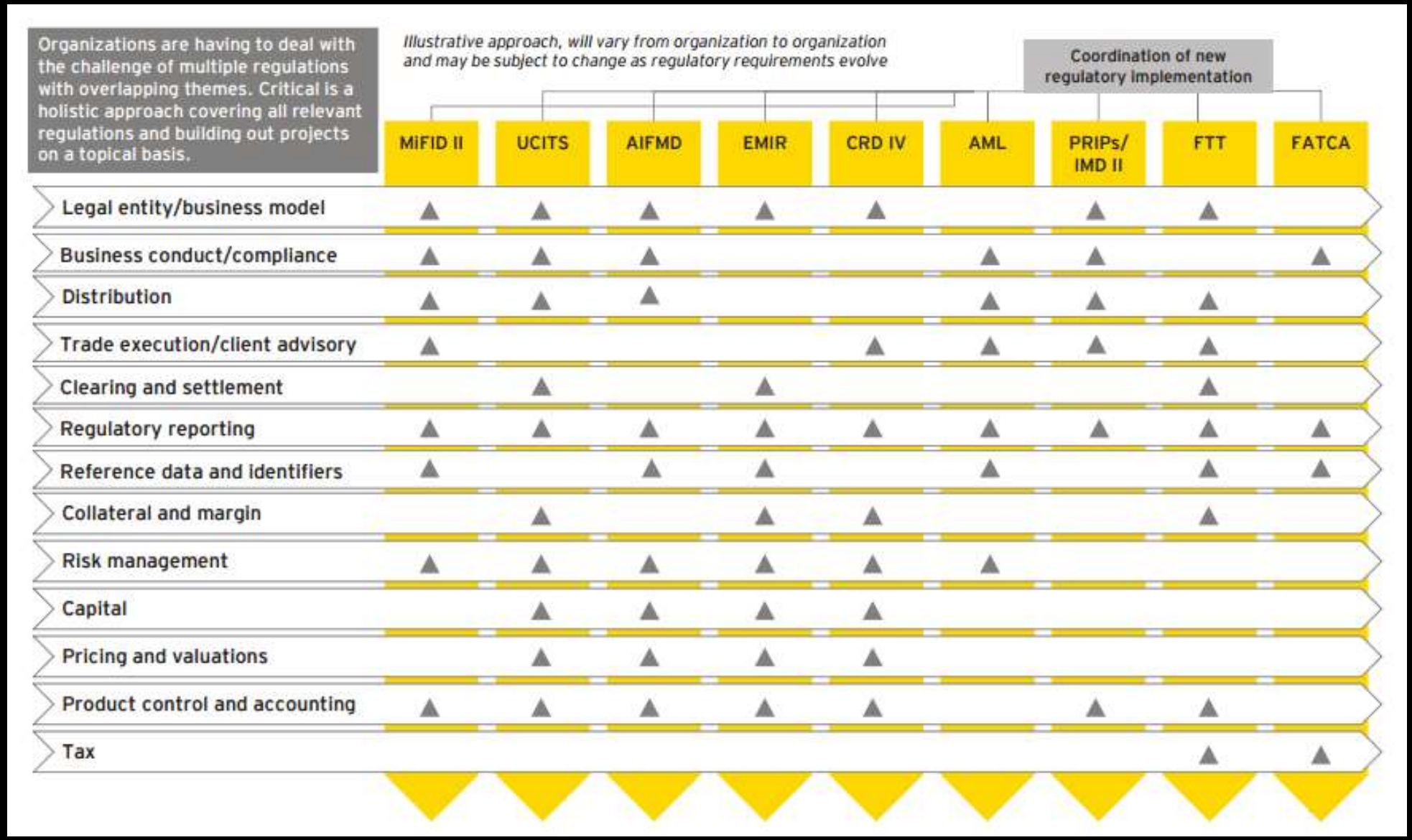
Through integration with your **Compliance Automation tool**, the controls monitored by the solution can be reported into it's control repository. In addition, the control exceptions detected through the correlation and contextualization of transaction and user data can be compiled and reported to it where it can be consolidated for compliance evidence.

MIFID II COMPLIANCE

MiFID II Regulation is based on 5 themes

Operating Conditions	The new rules require enhanced record keeping, detailed analysis of group-wide conflicts and amendments to the governance framework
Investor Protection	MiFID II aims to enhance the level of investor protection for all clients and counterparties. The new rules include detailed provisions covering financial promotions (i.e. marketing), client categorisation, best execution and disclosure
Transparency	The scope and volume of financial transactions to be reported under MiFID II (both publically and privately), has materially increased to cover all traded instruments
Electronic Trading	MiFID II places greater responsibility on regulated firms to demonstrate that electronic trading is conducted in a safe and controlled manner.
Market Structure	Revised market structure requirements to enhance the visibility of “dark pools”; i.e. trading conducted away from the public markets

Aligning MiFID II with other regulations



Source: EY MiFID II: Time to take action Wealth & Asset Management Report

Regulation Management Process

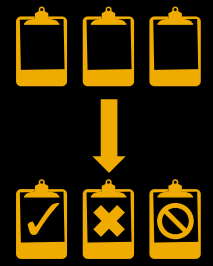
Regulatory Intake, Collaboration & Execution

1

Regulatory Citations

- Capture, intake and reporting of regulations
- Leverage publicly available content & subscriptions from UCF, LexisNexis, Thomson Reuters, etc.
- Regulatory alerts and monitoring

2

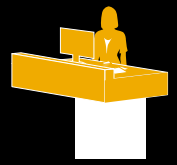


Requirements

- Version control and gap analysis
- Delta change management
- Pre-built reports and dashboards

3

Business



Compliance

Audit

Legal

Collaboration

- Central repository for regulatory content, requirement and reporting
- Comment and interact from start to finish
- Share and review best practices

Workflow

- Dynamic, multi-threaded workflow capabilities
- Review all or part of citations, requirements or controls at any time

Control Definition

- Best practice control mapping & content creation
- Unified control framework for all regulatory agencies
- Map controls back to citations

4

Control Management

- Manage, monitor and test controls*
- Automatically execute control tests against operational systems & business applications

5

Regulatory Reporting

- Capture, store and import report results
- Manage and maintain findings & evidence

Case Study: Large Spanish Bank, also in the UK

Case Study

Requirements

- Analyze regulatory changes
- Automate the RCM process. Using RegMan as a system of record to keep audit trail of all the activities done for regulatory change management and reporting to board and regulator
- Capture changes from ESMA and other feeds from the authorities, Thomson Reuters feeds, and process other unstructured content in pdf and other formats
- Assess regulatory obligations and reporting
- Report on degree of compliance through Compliance management (automated controls)

Value Driver	Detail	Improvement Estimate
Reduce Regulatory Planning Costs	• Reduce time spent by external legal councils on regulations	20-30%
	• Reduce time spent by internal legal teams on analysis of regulatory and legislative requirements	40-50%
Reduce Compliance Costs	• Reduce cost to implement controls	50-70%
	• Reduce cost of manual workflow approvals	40-80%
	• Reduce manual steps for compliance	40-80%
	• Reduce testing and monitoring costs	40-80%
	• Reduce internal audit costs	5-10%
	• Reduce fines and penalties	40-80%
	• Reduce cost of point solutions to support the regulatory response process	40-70%
	TOTAL	**$7.8-13.9 M**

PORTFOLIO OF SERVICES

Disruptive Advanced Security offerings

CLICK ANY BOX

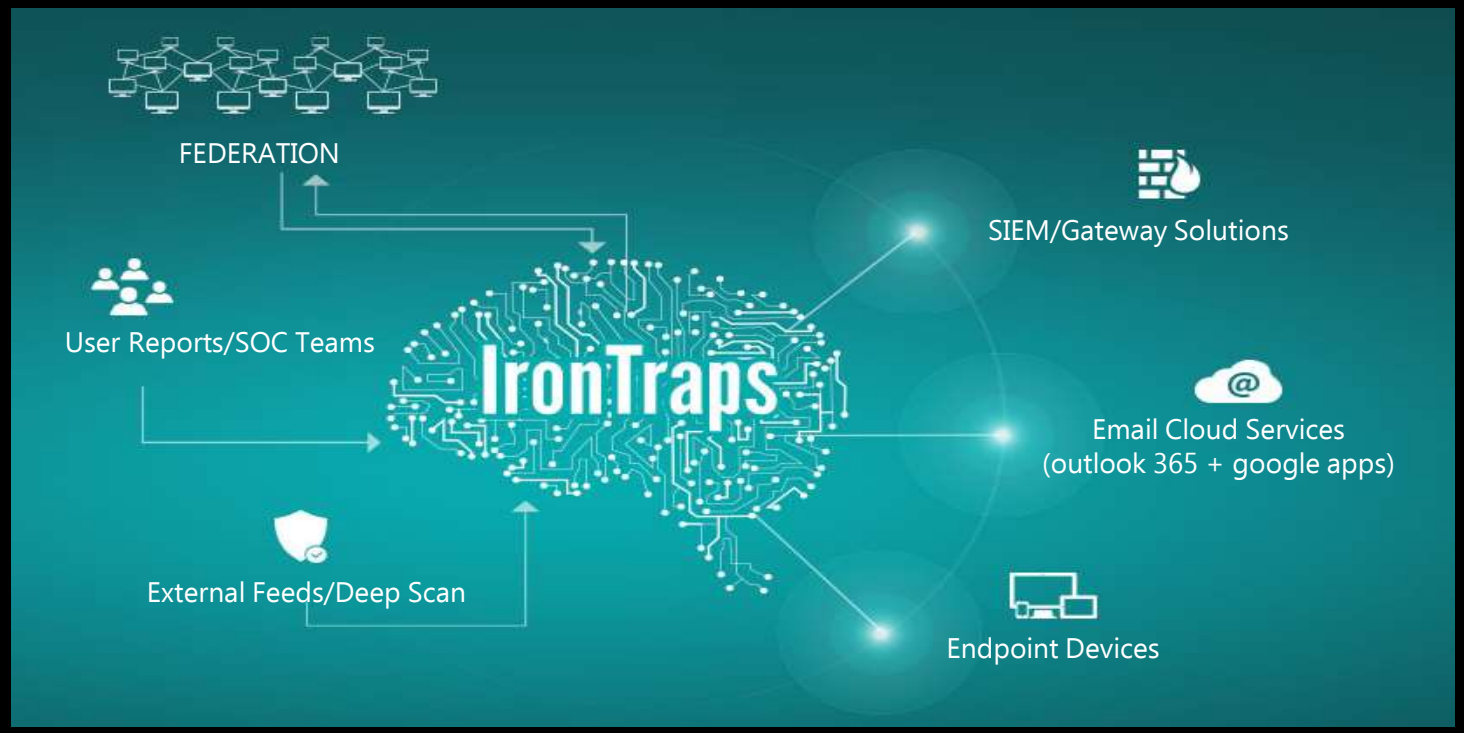
1 Brand & Executive Protection	2 Threat Scorecard Rating	3 Hacker Attack Simulation
4 De-identification of PHI/PII Data	5 Cloaking communication in critical assets	6 Protect against tampering & ransomware
7 Mobile-first Security	8 Instantaneous Endpoint visibility	9 Automated Phishing Response
10 Threat Hunting & Mitigation	11 Honey-potting (Deception)	12 Biometric Authentication
13 Cognitive Security Analytics	14 Unified GRC, DLP, SOC	15 Deception Disarmament & Reconstruction
16 Quantum Science based Security	17 OT Network Visibility	

1. **Proactive and preventative Brand & Executive Protection** offered through our Digital Risk Monitoring
2. **Threat Scorecard Rating**, an innovative dark-web rating service that provides a view of the company's confidential information uploaded on the internet & dark-web, and potential vulnerabilities unknown to the enterprise
3. **Simulate hacker attacks** keeping continuously executing breach methodologies to proactively find the holes in your environment
4. **De-identify PHI/PII data** permitting unhindered and secure predictive analytics on the data; secure entire big data lake while allowing tenants to see their own data
5. **Cloak communication between critical assets** to protect against Man-In-The-Middle (MITM) & DDoS
6. **Protect not only against theft but also tampering and ransomware in real-time** through comprehensive Data & Endpoint Protection Platform
7. **Secure smartphones, tablets, applications, mobile fleets, and more** through accurate detection of complex patterns using predictive cloud-based mobile security
8. **Instantaneously secure and manage millions of endpoints in seconds**; gain visibility and control to make better decisions
9. **Automatically detect and block email phishing attacks in real-time,** with or without human intervention, followed by an enterprise-wide remediation response
10. **Deploy unified threat protection** with the best threat intelligence, threat hunting & mitigating
11. **Detect, deflect, defeat cyber-attacks with algorithmically deployed unique deception traps,** to initiate the kill-chain and threat hunting process
12. **Biometric Authentication for real-time transaction security** combined with user behaviour authentication & risk-based authentication
13. **Cognitive security analytics** to replicate human intelligence at machine scale with Natural Language Processing (NLP), and automated research, prioritization and remediation capabilities
14. **Seamlessly address both malicious & inadvertent data/information exfiltration** with a real-time dashboard view of the entire Enterprise and/or Cloud including GRC enforcement, DLP & SOC
15. **Deception disarmament & reconstruction** to process all files, analyze the content, and rebuild duplicate files with clean and sanitized content
16. **Harness unique quantum science properties and cryptography** to ensure data confidentiality through encryption based on Random Number Generation
17. **OT Network visibility** for Industrial Control Networks in real-time

Threat Scorecard Rating: Assess your vulnerabilities in the Dark Web

An innovative service that provides a view of your **confidential information uploaded on the internet & dark-web**, and potential vulnerabilities unknown to the enterprise

Automated Phishing Detection & Response



Automatically detect and block email phishing attacks in real-time, with or without human intervention, followed by an enterprise-wide remediation response

Defined playbooks to cover anti phishing scenarios and user awareness/ education

Provisioned a separate mailbox/ queue to report the phishing mail related incidents and severity /impact tracking & remediation based on reported incidents

INCREASING DETECTION AND COLLABORATION
Making sure phishing attacks will be detected and stopped faster than ever

PREVENTION
Real-time mailbox protection against known/ongoing Phishing scams

AUTOMATED FORENSICS
Automatic AV & SandBox scanning, aggregating and clustering of user reports and other intelligence

AUTOMATING RESPONSE & REMEDIATION
Reducing the SOC workload burden by automatically detecting and removing malicious emails

ACTIONABLE COLLABORATION
Making sure attacks are shared instantly and automatically – proactively defending organizations

Advisory Services (Consulting & Compliance)

Consulting & Assessment Services

Strategic Consulting Services

- Digital Transformation Security Consulting
- IIoT SCADA Systems Consulting
- Offensive Simulation Consulting
- Hacking as a Service (HaaS)
- Brand / Executive Protection Consulting
- Enterprise Security & Information Protection Maturity Assessment (Security Assurance)
- Security Governance, Policies, Procedures
- ESRM awareness and change management
- Enterprise Security Architecture Review
- Data Classification/Protection/Privacy Governance/Leakage
- Advanced Data analytics SOC consulting
- Identity Governance & admin consulting
- Cryptography Consulting
- Perimeter Security (Network devices) consulting

Operational Consulting Services

- Information Security Officer
- Threat Scorecard Rating
- Security perimeter definition
- Inventory and classification of information assets
- Security risk assessment
- Business continuity and Disaster recovery

Audit & Assessment Services

- Cloud Compliance Assessment
- Mainframe Security Assessments
- System Penetration testing
- CLOUD-BASED Application security testing
- Data Discovery Assessment / Data Security Compliance consulting
- Forensics
- Security audits (org, configuration, architecture)
- Governance & Regulatory compliance
- Third Party Security Assessment

IBM LIFARS hp NYMITY TITUS varonis

Security-as-a-Service MSSP offerings

Advanced Threat Management

1. SIEM aaS
2. Threat intelligence aaS
3. Advanced Big Data Security Analytics aaS
4. Anti-phishing aaS
5. Vulnerability Management aaS
6. Security HQ portal
7. Deception aaS

Perimeter, Network & Endpoint Security

1. Intrusion Detection/ Prevention aaS
2. Anti-malware as a Service
3. DDoS Mitigation as a Service
4. Firewall Network Security as a Service
5. Web content & Gateway filtering as a Service
6. Endpoint Security as a Service

Data Security

1. Data Loss prevention (DLP) aaS
2. Database Encryption aaS
3. Database Activity Monitoring aaS

Identity & Access Management

1. Identity as a Service (IDaaS)
2. Authentication aaS
3. RISK based authentication
4. (Biometric) aaS
5. Privileged Identity & Access Management

Advanced Security Services

1. Cisco Network Segmentation aaS
2. Mobile Detection & Response aaS
3. Endpoint Threat Detection & Response aaS

Operational/ Compliance Consulting

1. GRC aaS
2. Financial transaction monitoring aaS
3. Data Discovery aaS

Application Security

1. Application Security aaS
2. Mobile Application Security aaS

Strategic Consulting

1. GDPR aaS
2. Hacking aaS
3. Brand / Executive Protection aaS
4. CISO aaS

Cloud Security

1. Cloud Access Security Brokers (CASB) aaS
2. O365 Security aaS
3. Secure Endpoint backup to cloud

Threat Management Services

Threat Detection & Mitigation

Threat Management Services

- SIEM as a service
- Cognitive Security Analytics
- Threat Hunting as a Service
- Malware analysis / Reverse engineering
- Threat Intelligence as a Service
- Advanced Data Analytics SOC (SOCaaS)
- Advanced OT/IoT Analytics SOC
- User-behavior Analytics (UEBA)
- Security Incident Response (SIRT)
- Financial Crime Analytics
- Fraud & Compliance
- Forensic Services
- Vulnerability Management as a service
- Threat Management as a service

BALABIT, NOZOMI, SCADAfence, BAE SYSTEMS, LOOKINGGLASS, sqrrl, LogRhythm, QUALYS, smokescreen, SECURONIX, exabeam, splunk>, Nessus, IBM resilient an IBM Company, RSA, logpoint, IAI, FORTSCALE, ArcSight, sparkcognition

360

ISO 27001

- ISO /IEC 27001:2013 certified

Protection Services I

Protection Services

Perimeter Security Services

- Reverse Proxy & Load Balancer
- OT Network Security
- Intrusion Detection/ Prevention (IDS/IPS) as a Service
- Network Access Security
- Anti-malware & Anti Spam (email) as a Service
- DDoS Mitigation as a Service
- Web content & Gateway filtering
- Firewall Network Security as a Service

Application Security Services

- Secure code review
- WAPT for Applications hosted on Cloud
- Secure DevOps
- IoT/Device Application Security
- IIoT Vulnerability Assessments
- Application Security as a Service
- DevOps Security
- Mobile Application Security as a Service

Data Security Services

- Database Activity Monitoring as a Service
- Data Loss prevention (DLP) as a Service
- Data Tokenization & Masking
- Digital / Information Rights Management
- Data Encryption Services (Disk Encryption)
- Database Encryption as a Service
- PKI & Digital Certificate / Key Management
- Cryptography
- Cloud Access Security Brokers (CASB)

Protection Services II

Protection Services

Identity and Access Management

- Enterprise ID Management
- Third Party access Management
- User & Privilege Access Management
- Identity Governance
- Multifactor & Risk-based authentication
- IAM Federation
- Behavioural Authentication
- Risk-based Adaptive Authentication
- Biometric Authentication
- Consumer Access Management
- Authentication as a Service (Multifactor & Risk based, Biometric, Behavioral as well as adaptive)
- Privileged account /Identity management (PIM/PAM)
- Identity as a Service (IDaaS)

Endpoint Security Services

- Endpoint Security as a Service
- Mobile Security - MDM security
- File Integrity Monitoring
- Endpoint Antivirus

Thank You

- Contact us: sales@techdefcon.com
- www.techdefcon.com