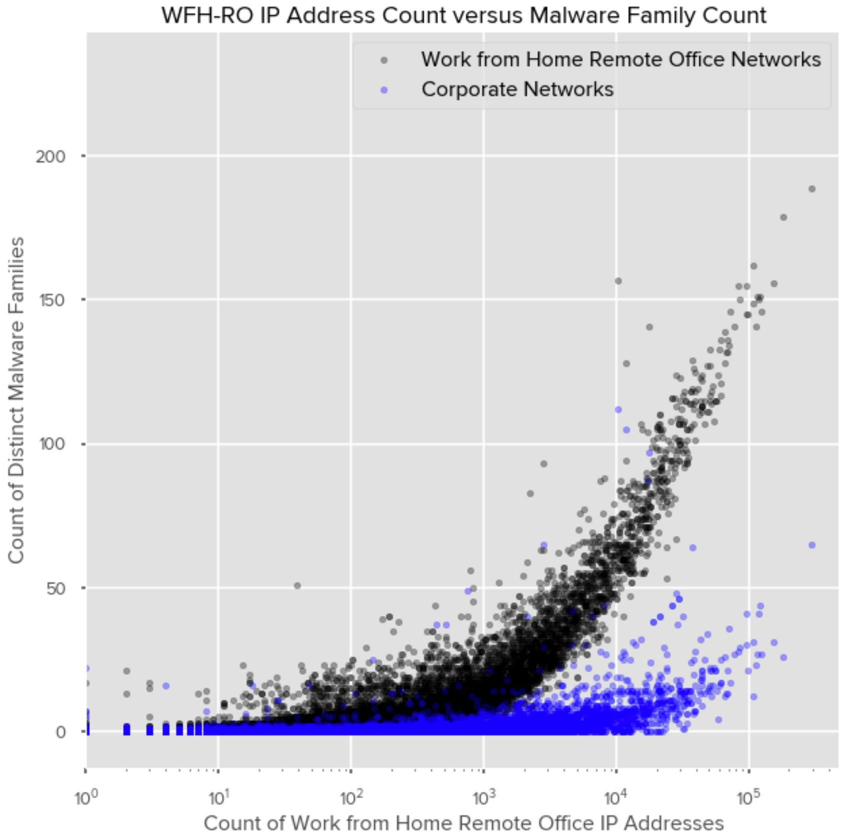
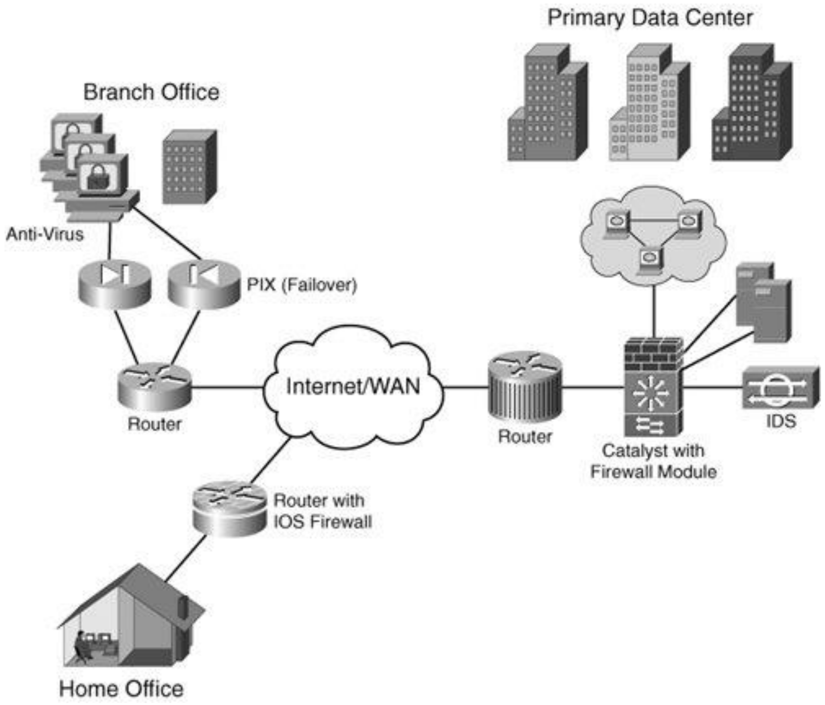
Alec Karry – Sr. Risk Advisor, Optiv Security

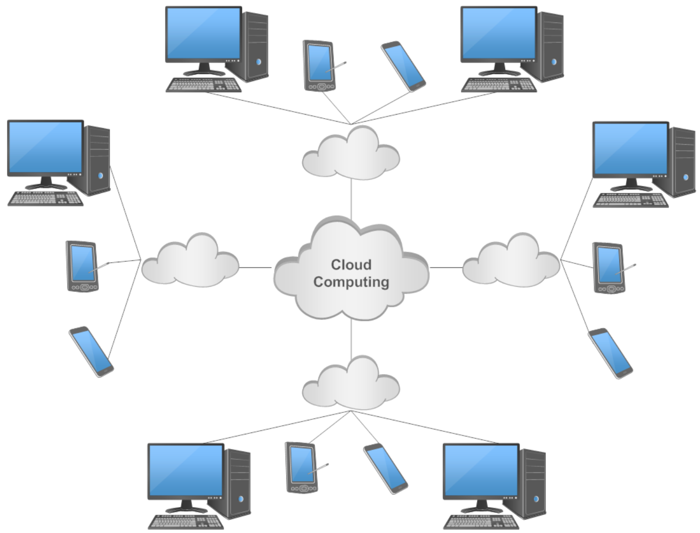
Risk Management Focus: Risks Outside the Fence Line in the Age of Digital Transformation



Changes in the Corporate Network Model



Traditional Network Model



Cloud Network Model

RISKS OUTSIDE THE FENCE LINE

Working from Home

Evolving Threat Landscape

IoT and Cloud Applications

Privacy

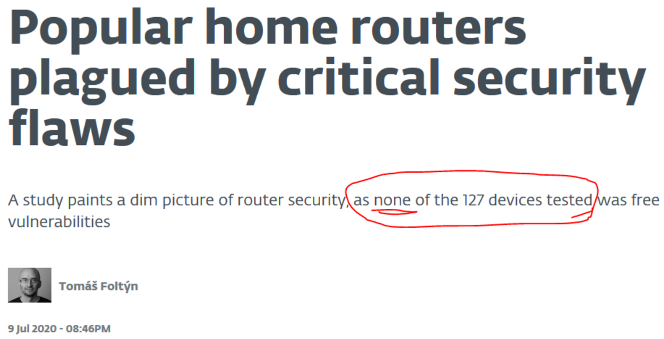
RISKS OUTSIDE THE FENCE LINE: WORKING FROM HOME

Pre-Pandemic Model

- Only select groups have remote access
- Limited access and functionality (email, select portals)
- Manageable home-worker deployment model

100% Remote Worker Model

- Everyone is working remotely
- Do VPN users have access to all things?
- What does your remote network security profile look like?
- Has security been relaxed to accommodate remote users?
- Do you have the technical and support resources to handle the load?



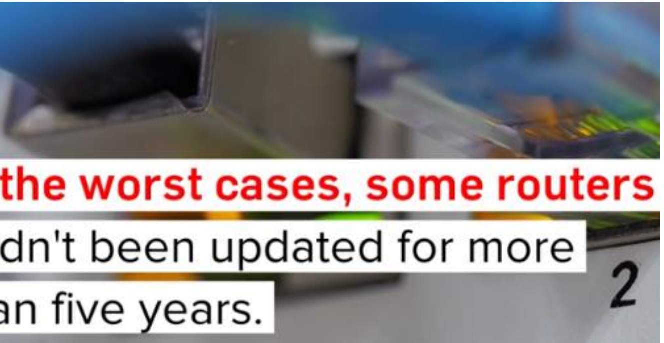
Popular home routers plagued by critical security flaws

A study paints a dim picture of router security, as none of the 127 devices tested was free vulnerabilities

Tomáš Foltýn

9 Jul 2020 - 08:46PM

other finding was that most of th
uters are affected by hundreds
known vulnerabilities.



the worst cases, some routers
dn't been updated for more
an five years.

RISKS OUTSIDE THE FENCE LINE: THE RISKS OF WORKING FROM HOME

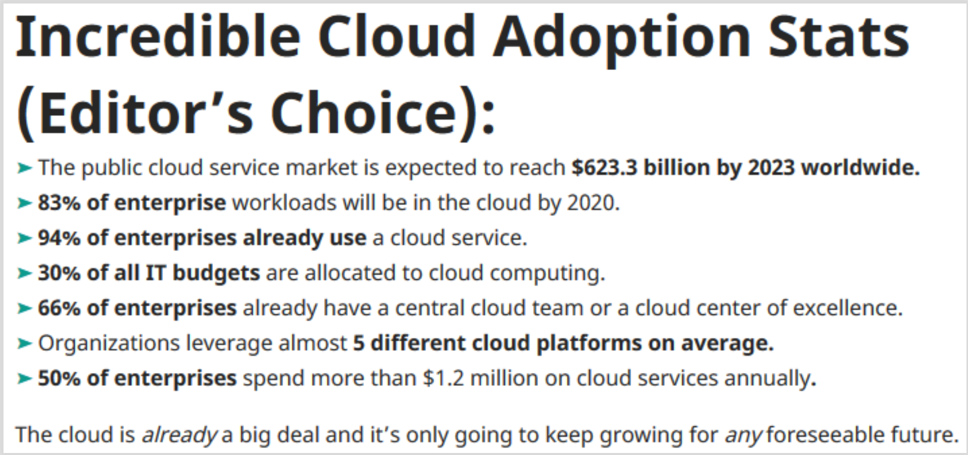
Scenario: Risks from IoT & Home Network Config

- Threat actor conducts proximity attacks from smart devices
- Home routers have insecure configurations, default passwords, outdated firmware, known exploitable software vulnerabilities, remote administration accessible from the Internet

Once compromised

- DNS server addresses often changed (DNS Hijacking)
- Inside home traffic intercepted in general
- Router infected with malware to be used as part of a botnet

RISKS OUTSIDE THE FENCE LINE



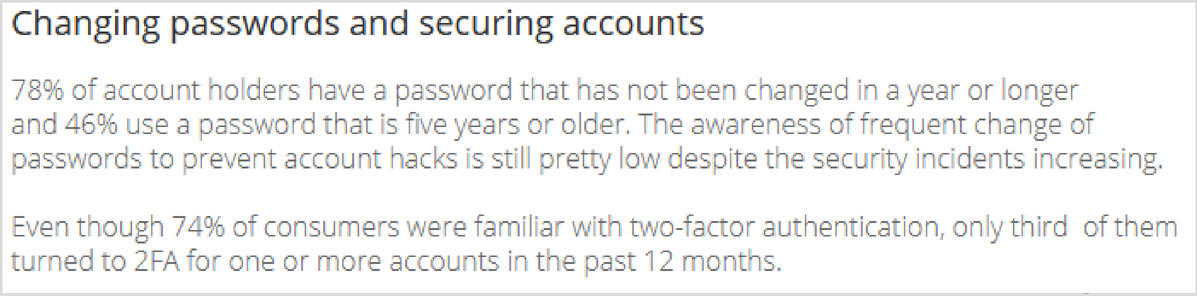
Incredible Cloud Adoption Stats (Editor's Choice):

- The public cloud service market is expected to reach **$623.3 billion by 2023 worldwide.**
- **83% of enterprise** workloads will be in the cloud by 2020.
- **94% of enterprises already use** a cloud service.
- **30% of all IT budgets** are allocated to cloud computing.
- **66% of enterprises** already have a central cloud team or a cloud center of excellence.
- Organizations leverage almost **5 different cloud platforms on average.**
- **50% of enterprises** spend more than $1.2 million on cloud services annually.

The cloud is *already* a big deal and it's only going to keep growing for *any* foreseeable future.

IoT, Cloud
Applications, & Data

Privacy



Changing passwords and securing accounts

78% of account holders have a password that has not been changed in a year or longer and 46% use a password that is five years or older. The awareness of frequent change of passwords to prevent account hacks is still pretty low despite the security incidents increasing.

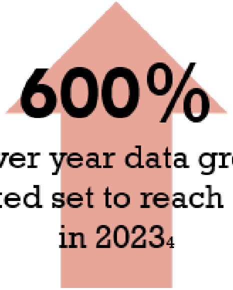
Even though 74% of consumers were familiar with two-factor authentication, only third of them turned to 2FA for one or more accounts in the past 12 months.

WHAT’S GOING ON WITH THE DATA?

DATA

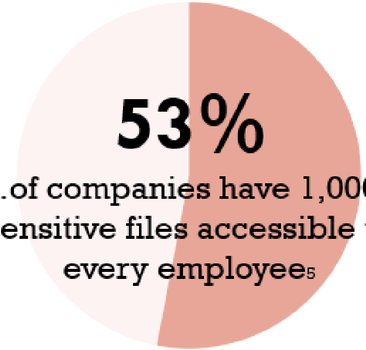
80%

of all data
is unstructured



600%

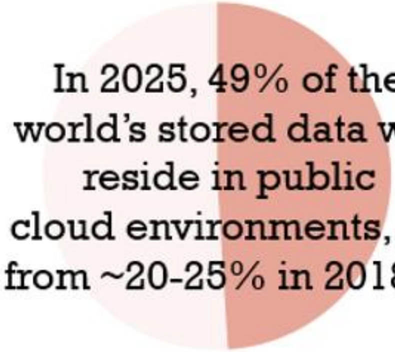
Year over year data growth is expected set to reach 11.7ZB in 2023[4]



53%

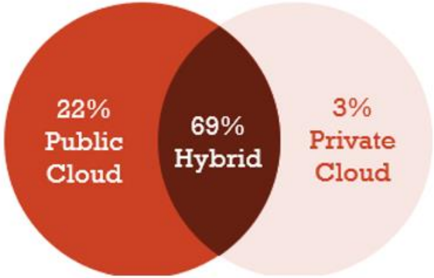
…of companies have 1,000+ sensitive files accessible to every employee[5]

Sources in slide notes

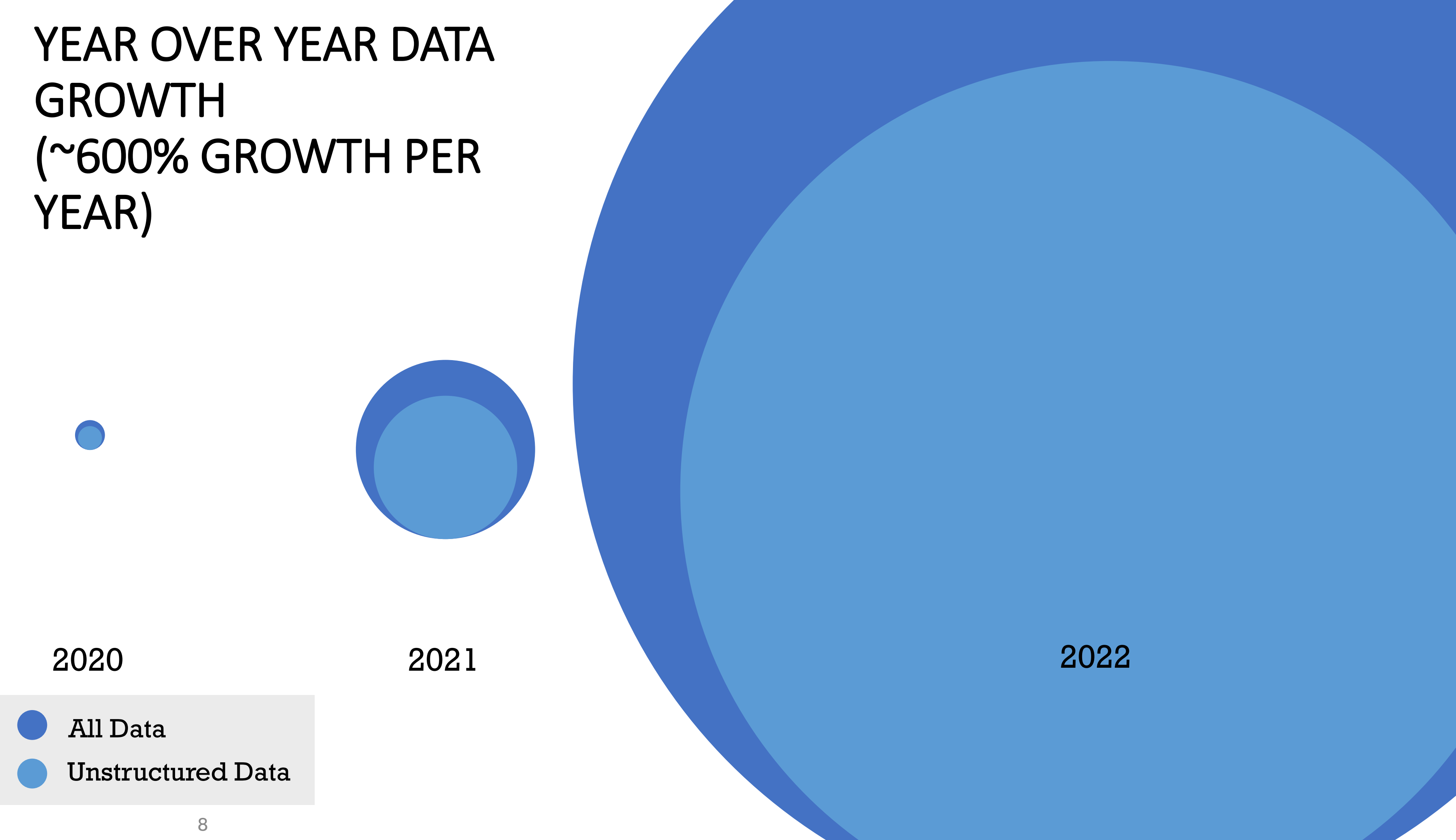


In 2025, 49% of the world’s stored data will reside in public cloud environments, up from ~20-25% in 2018**

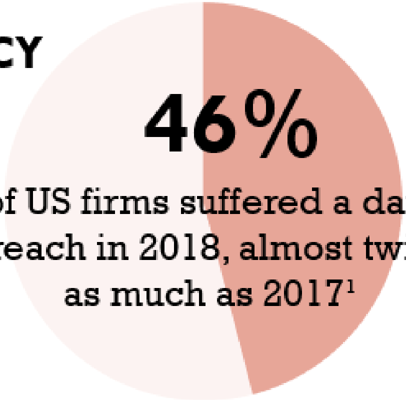
94% of Respondents Using Cloud*



YEAR OVER YEAR DATA GROWTH (~600% GROWTH PER YEAR)

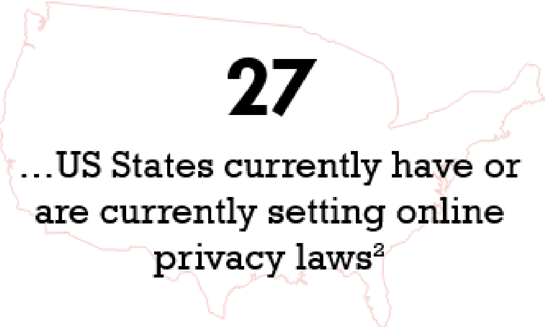


PRIVACY



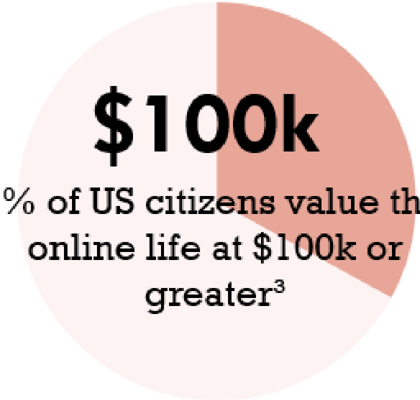
46%

of US firms suffered a data breach in 2018, almost twice as much as 2017[1]



27

…US States currently have or are currently setting online privacy laws[2]



$100k

33% of US citizens value their online life at $100k or greater[3]

WHY PRIVACY AND DATA ARE CRITICAL

- 95% are concerned about businesses collecting and selling personal information without permission

- 55% of consumers say companies should have primary responsibility for the security of their online and mobile accounts

PRIVACY RIGHTS

New and continuously updated privacy regulations

- International, Federal and State
- SOX, HIPAA, FINRA, GDPR, Sarbanes-Oxley, NYDFS, CCPA

Consistently changing audit and regulatory issues

- Heavy fines for non-compliance
- Inability to quickly meet audit requests and requirements
- Lack of data lineage to allow for completing DSARs

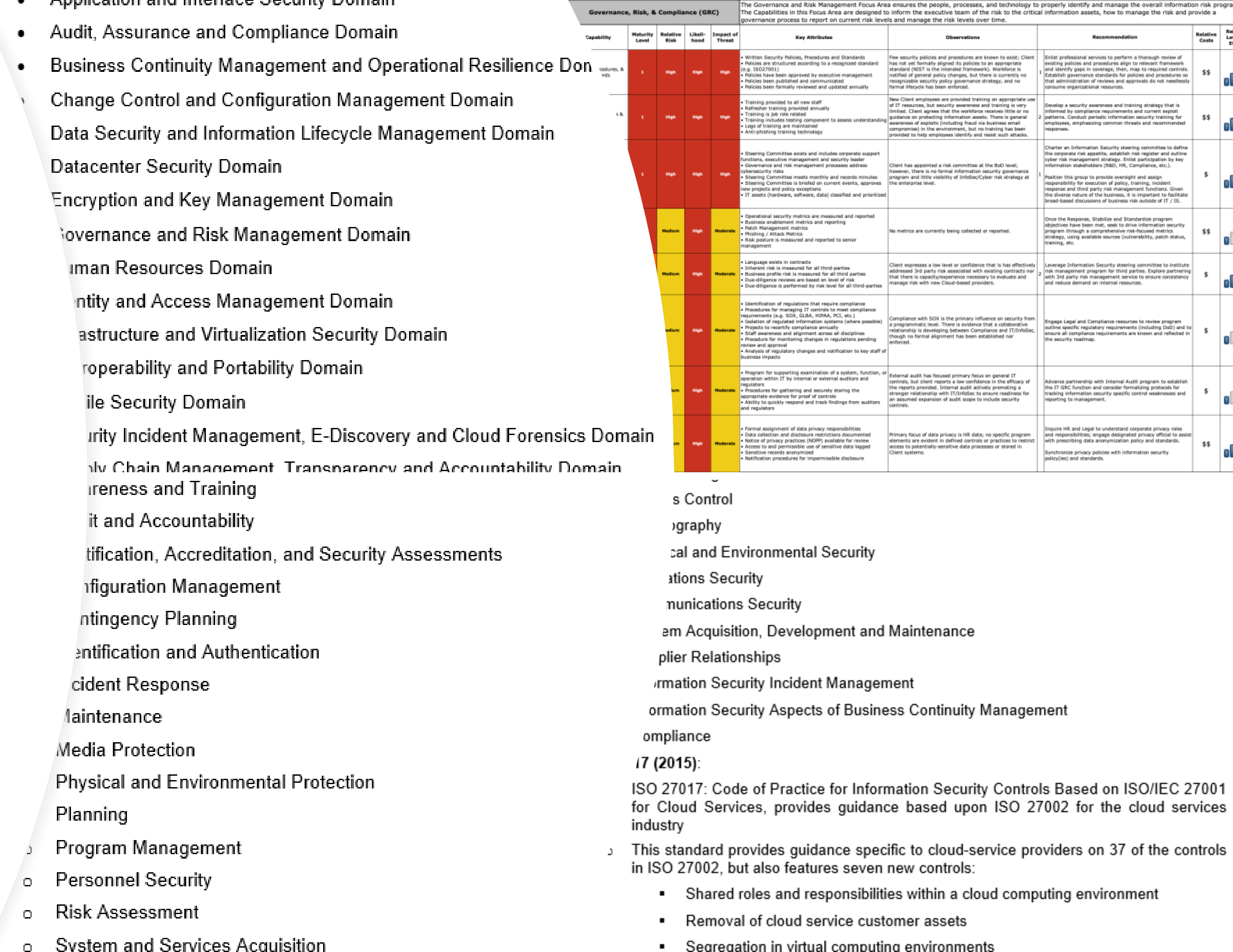
Lack of security controls leads to over-exposed sensitive data

- What data is to be regulated, where it is and who has access?

Frameworks & Reference Architectures

Frameworks & Standards

- ISO (27001, 27002, 27017)
- NIST (RMF, 800-53, CSF)
- CSA Cloud Controls Matrix
- CIS Top 20



- Application and Interface Security Domain
- Audit, Assurance and Compliance Domain
- Business Continuity Management and Operational Resilience Don
- Change Control and Configuration Management Domain
- Data Security and Information Lifecycle Management Domain
- Datacenter Security Domain
- Encryption and Key Management Domain
- overnance and Risk Management Domain
- uman Resources Domain
- ntity and Access Management Domain
- astructure and Virtualization Security Domain
- roperability and Portability Domain
- ile Security Domain
- urity Incident Management, E-Discovery and Cloud Forensics Domain
- ply Chain Management, Transparency and Accountability Domain

Governance, Risk, & Compliance (GRC)					The Governance and Risk Management Focus Area ensures the people, processes, and technology to properly identify and manage the overall information risk progra The Capabilities in this Focus Area are designed to inform the executive team of the risk to the critical information assets, how to manage the risk and provide a governance process to report on current risk levels and manage the risk levels over time.				
Capability	Maturity Level	Relative Risk	Likeli-hood	Impact of Threat	Key Attributes	Observations		Recommendation	Relative Costs
cedures, & vds	1	High	High	High	• Written Security Policies, Procedures and Standards • Policies are structured according to a recognized standard (e.g. ISO27001) • Policies have been approved by executive management • Policies been published and communicated • Policies been formally reviewed and updated annually	Few security policies and procedures are known to exist; Client has not yet formally aligned its policies to an appropriate standard (NIST is the intended framework). Workforce is notified of general policy changes, but there is currently no recognizable security policy governance strategy, and no formal lifecycle has been enforced.	1	Enlist professional services to perform a thorough review of existing policies and procedures align to relevant framework and identify gaps in coverage, then, map to required controls. Establish governance standards for policies and procedures so that administration of reviews and approvals do not needlessly consume organizational resources.	$$
s &	1	High	High	High	• Training provided to all new staff • Refresher training provided annually • Training is job role related • Training includes testing component to assess understanding • Logs of training are maintained • Anti-phishing training technology	New Client employees are provided training on appropriate use of IT resources, but security awareness and training is very limited. Client agrees that the workforce receives little or no guidance on protecting information assets. There is general awareness of exploits (including fraud via business email compromise) in the environment, but no training has been provided to help employees identify and resist such attacks.	2	Develop a security awareness and training strategy that is informed by compliance requirements and current exploit patterns. Conduct periodic information security training for employees, emphasizing common threats and recommended responses.	$$
	1	High	High	High	• Steering Committee exists and includes corporate support functions, executive management and security leader • Governance and risk management processes address cybersecurity risks • Steering Committee meets monthly and records minutes • Steering Committee is briefed on current events, approves new projects and policy exceptions • IT assets (hardware, software, data) classified and prioritized	Client has appointed a risk committee at the BoD level; however, there is no formal information security governance program and little visibility of InfoSec/Cyber risk strategy at the enterprise level.	1	Charter an Information Security steering committee to define the corporate risk appetite, establish risk register and outline cyber risk management strategy. Enlist participation by key information stakeholders (R&D, HR, Compliance, etc.). Position this group to provide oversight and assign responsibility for execution of policy, training, incident response and third party risk management functions. Given the diverse nature of the business, it is important to facilitate broad-based discussions of business risk outside of IT / IS.	$
		Medium	High	Moderate	• Operational security metrics are measured and reported • Business enablement metrics and reporting • Patch Management metrics • Phishing / Attack Metrics • Risk posture is measured and reported to senior management	No metrics are currently being collected or reported.		Once the Response, Stabilize and Standardize program objectives have been met, seek to drive information security program through a comprehensive risk-focused metrics strategy, using available sources (vulnerability, patch status, training, etc.	$$
		Medium	High	Moderate	• Language exists in contracts • Inherent risk is measured for all third-parties • Business profile risk is measured for all third parties • Due-diligence reviews are based on level of risk • Due-diligence is performed by risk level for all third-parties	Client expresses a low level or confidence that is has effectively addressed 3rd party risk associated with existing contracts nor that there is capacity/experience necessary to evaluate and manage risk with new Cloud-based providers.	2	Leverage Information Security steering committee to institute risk management program for third parties. Explore partnering with 3rd party risk management service to ensure consistency and reduce demand on internal resources.	$
		edium	High	Moderate	• Identification of regulations that require compliance • Procedures for managing IT controls to meet compliance requirements (e.g. SOX, GLBA, HIPAA, PCI, etc.) • Isolation of regulated information systems (where possible) • Projects to recertify compliance annually • Staff awareness and alignment across all disciplines • Procedure for monitoring changes in regulations pending review and approval • Analysis of regulatory changes and notification to key staff of business impacts	Compliance with SOX is the primary influence on security from a programmatic level. There is evidence that a collaborative relationship is developing between Compliance and IT/InfoSec, though no formal alignment has been established nor enforced.		Engage Legal and Compliance resources to review program outline specific regulatory requirements (including DoD) and to ensure all compliance requirements are known and reflected in the security roadmap.	$
		ium	High	Moderate	• Program for supporting examination of a system, function, or operation within IT by internal or external auditors and regulators • Procedures for gathering and securely storing the appropriate evidence for proof of controls • Ability to quickly respond and track findings from auditors and regulators	External audit has focused primary focus on general IT controls, but client reports a low confidence in the efficacy of the reports provided. Internal audit actively promoting a stronger relationship with IT/InfoSec to ensure readiness for an assumed expansion of audit scope to include security controls.		Advance partnership with Internal Audit program to establish the IT GRC function and consider formalizing protocols for tracking information security specific control weaknesses and reporting to management.	$
		um	High	Moderate	• Formal assignment of data privacy responsibilities • Data collection and disclosure restrictions documented • Notice of privacy practices (NOPP) available for review • Access to and permissible use of sensitive data logged • Sensitive records anonymized • Notification procedures for impermissible disclosure	Primary focus of data privacy is HR data; no specific program elements are evident in defined controls or practices to restrict access to potentially-sensitive data processes or stored in Client systems.		Inquire HR and Legal to understand corporate privacy roles and responsibilities; engage designated privacy official to assist with prescribing data anonymization policy and standards. Synchronize privacy policies with information security policy(ies) and standards.	$$

- ireness and Training
- it and Accountability
- tification, Accreditation, and Security Assessments
- nfiguration Management
- ntingency Planning
- entification and Authentication
- cident Response
- laintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Personnel Security
- Risk Assessment
- System and Services Acquisition

s Control

graphy

cal and Environmental Security

ations Security

nunications Security

em Acquisition, Development and Maintenance

plier Relationships

rmation Security Incident Management

ormation Security Aspects of Business Continuity Management

ompliance

I7 (2015):

ISO 27017: Code of Practice for Information Security Controls Based on ISO/IEC 27001 for Cloud Services, provides guidance based upon ISO 27002 for the cloud services industry

This standard provides guidance specific to cloud-service providers on 37 of the controls in ISO 27002, but also features seven new controls:

- Shared roles and responsibilities within a cloud computing environment
- Removal of cloud service customer assets
- Segregation in virtual computing environments

RISK FRAMEWORK ASSISTANCE
(WORK FROM HOME)

NIST 800-46 & CIS Top 20

POLICY TRAINING & AWARENESS

- Policy and Procedures
- Remote Training
- Remote Incident Response
- Remote Policy Acceptance

SECURITY ARECHITECTURE

- System Hardening
- Threat Modeling
- Risk Assessment
- Compensating Controls
- Threat Protections
- Network Segmentation
- Sensitive Data Access Rights
- Remote Access Server Security

REMOTE ACCESS SECURITY

- Remote Access Server Patch Mgmt.
- Remote Access Server Security
- Remote Access System Threat Modeling
- Remote Access Server
- Network Architecture
- Remote Access Policy
- Authentication Processes
- Multi-Factor Authentication
- Mobile Device Remote Access
- Compliance Validation
- High Security Connections
- Administrative Remote Access
- Encrypted Transmission

DEVICE SECURITY

- Security Control Compliance
- VDI/VMI Support
- Remote Endpoint Patching
- Remote Endpoint Vulnerability Scanning
- Endpoint Firewalls
- Mobile Device Remote Access Controls
- Data Encryption
- Session Management
- BYOD Management

SYSTEMS LIFECYCLE

- Risk Based Decision Process
- Periodic Program Review
- Network Solution Security
- Access Solution Design Process
- Operational Management
- Asset Disposal

ACCOUNT MONITORING AND CONTROL

- Multi-Factor Account Management
- Re-Authentication Policy and Standards
- BYOD Account Restrictions
- Data Flow Mapping and Compliance

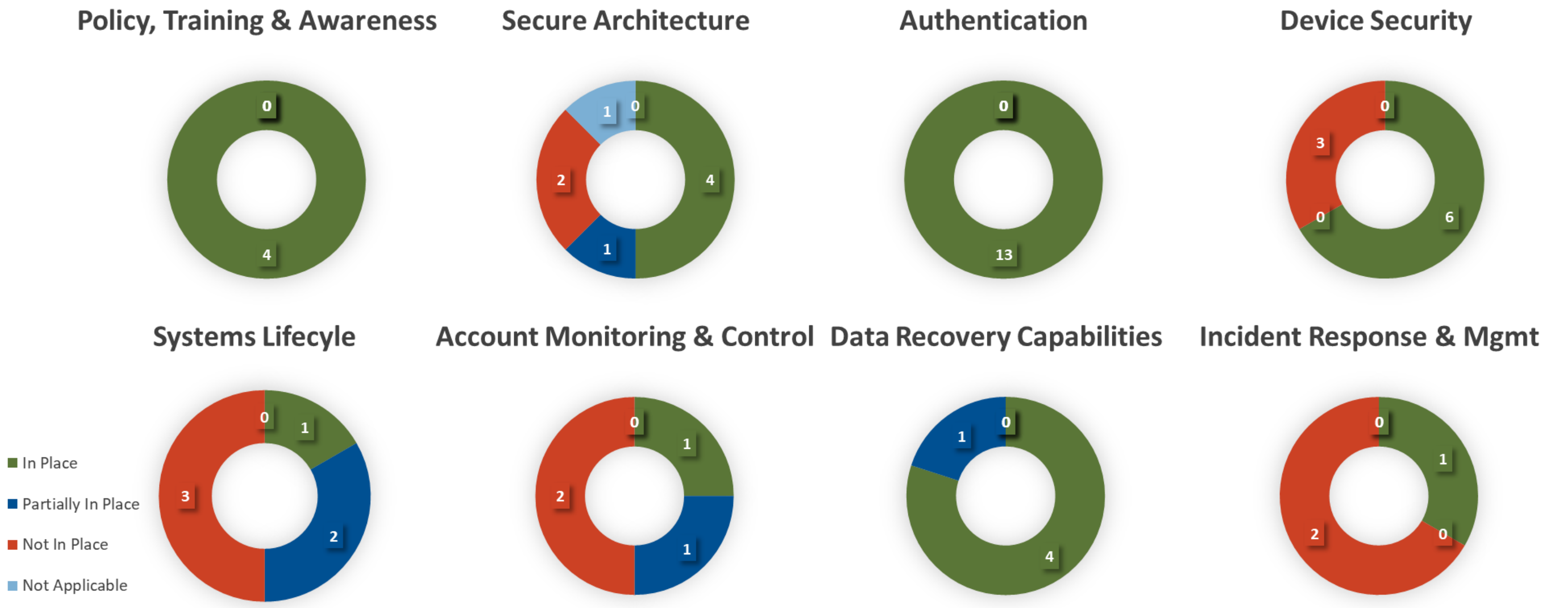
DATA RECOVERY

- Business Continuity
- Backup/Recovery system
- Disaster Recovery
- Sensitive Information Backup/Recovery
- Backup Data Protection

INCIDENT RESPONSE & MGMT

- Incident Management Program
- Incident Management Roles and Responsibilities
- Incident Response Communication Plan

RISK FRAMEWORK ASSISTANCE
(WORK FROM HOME)


Policy, Training & Awareness

Secure Architecture

Authentication

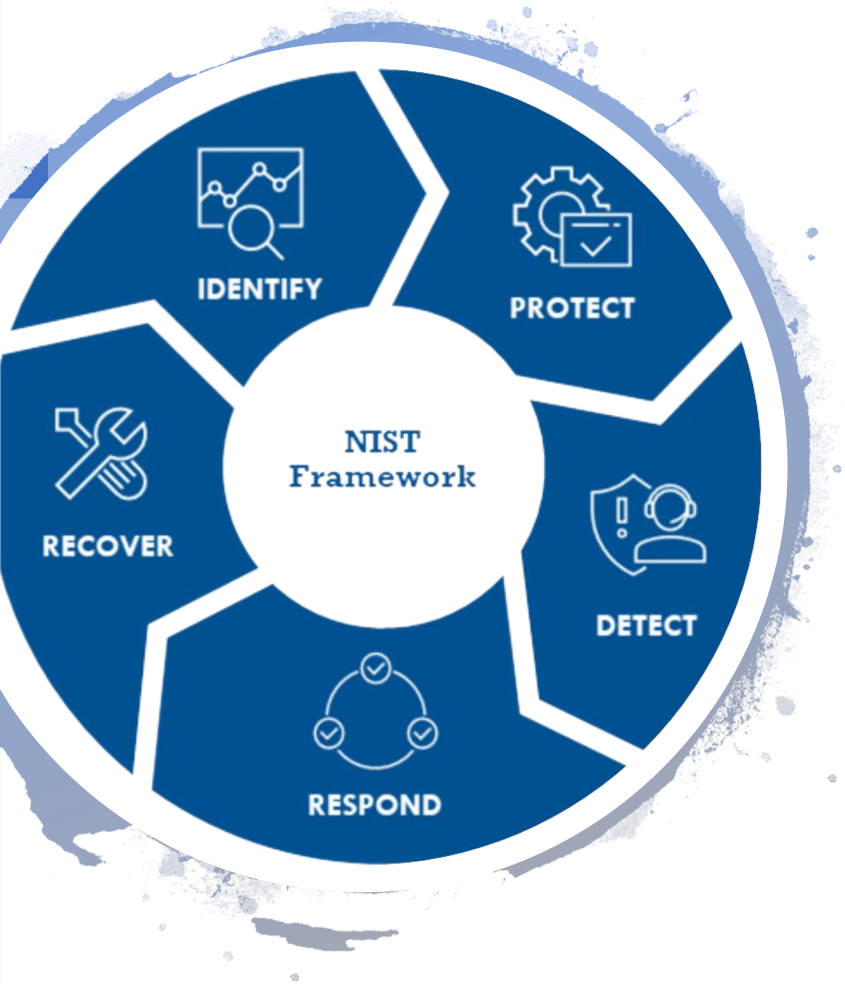
Device Security

Systems Lifecycle

Account Monitoring & Control

Data Recovery Capabilities

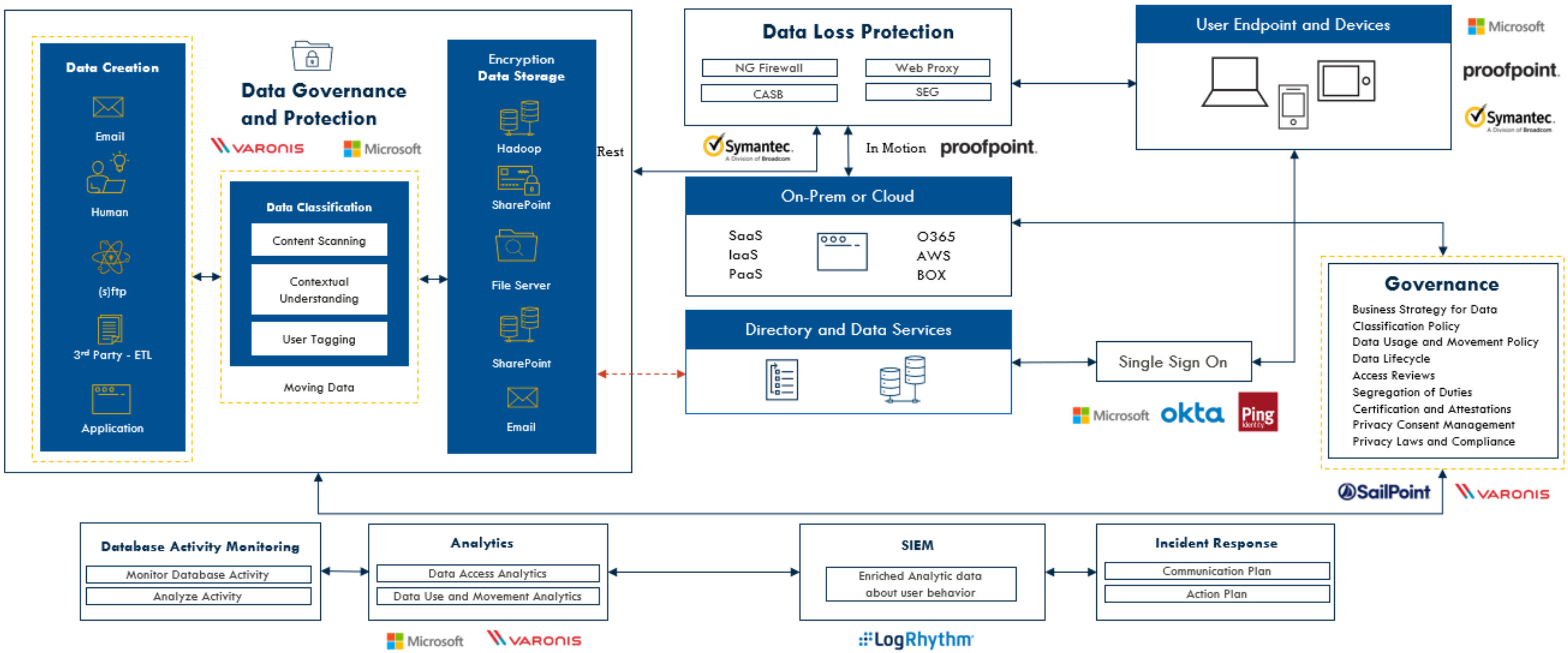
Incident Response & Mgmt



NIST PRIVACY FRAMEWORK

- **Released version 1.0 on January 16**
- **Defines Personal Data**
  - Includes information about specific individuals, such as their addresses or Social Security numbers, that a company might gather and use in the normal course of business
- **A voluntary tool that can help organizations manage privacy risk arising from their products and services, as well as demonstrate compliance with laws that may affect them;**
  - CCPA or GDPR compliance
- **Aligns with NIST CSF Security Framework**

DIGITAL DATA REFERENCE ARCHITECTURE



Data Creation

Email

Human

(s)ftp

3rd Party - ETL

Application

Data Governance and Protection

VARONIS

Microsoft

Data Classification

Content Scanning

Contextual Understanding

User Tagging

Moving Data

Encryption
Data Storage

Hadoop

SharePoint

File Server

SharePoint

Email

Rest

Data Loss Protection

NG Firewall

Web Proxy

CASB

SEG

Symantec. A Division of Broadcom

In Motion

proofpoint.

User Endpoint and Devices

Microsoft

proofpoint.

Symantec. A Division of Broadcom

On-Prem or Cloud

SaaS
IaaS
PaaS

O365
AWS
BOX

Directory and Data Services

Single Sign On

Microsoft

okta

Ping Identity

Governance

Business Strategy for Data

Classification Policy

Data Usage and Movement Policy

Data Lifecycle

Access Reviews

Segregation of Duties

Certification and Attestations

Privacy Consent Management

Privacy Laws and Compliance

SailPoint

VARONIS

Database Activity Monitoring

Monitor Database Activity

Analyze Activity

Analytics

Data Access Analytics

Data Use and Movement Analytics

Microsoft

VARONIS

SIEM

Enriched Analytic data about user behavior

LogRhythm

Incident Response

Communication Plan

Action Plan

Questions?