VIRGINIA IT AGENCY

ISOAG MEETING

SEPT. 1, 2021

VIRGINIA IT AGENCY

AGENDA

- BARRY DAVIS, DSS
- CHRISTINA SINCLAIR, MATTHEW NEAL, F5
- ERIC HILL, STEVE COLLE & LEE MCMILLIAN, NTT DATA
- AARON MATHES, CGI
- ALOK OJHA, & LORI LAGUARDIA, BOX
- UPCOMING EVENTS
- ADJOURN

ECOS and the Agency Risk Management Program

a VDSS Experience

Presentation Objective:
Create a shared awareness of how ECOS fits into the Agency Risk Management/SEC501 program…

Barry Davis, CISSP
VDSS Information Security Officer

ISOAG 9/1/2021

VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

ISRM

Agenda

- MythPerceptions around ECOS and RMF
- We've only just begun….
- Using ECOS products for Application Risk Management
- Key Takeaways
- Q&A

ECOS MythPerceptions

- This application is ECOS’d, my agency has no other security obligations other than the required exceptions;
- If it is ECOS approved, there are no security concerns;
- We can use the ECOS Assessment as the Application Risk Assessment;

We’ve only just begun….

- Data Classification;
- Threat Assessment, Controls Assessment, Risk Assessment,
- System Security Plan,
- Authority to Operate
- Third Party Monitoring….
  - Who is reviewing SOC-2?
  - Who is reviewing monthly reports?
  - Is procurement involved?

Using ECOS as inputs to RMF…

- ECOS only provides assurance the third-party is providing the same level of assurance as you would find with a VITA hosted service
- ECOS Assessment = Agency controls inherited from VITA
- Typical controls met with ECOS..
  - CM, IA, MA, MP, PE, PS*, SC, SI
- Controls/Activities remaining for Agency System Owner, Data Owner, ISO..
  - AC, AT, AU, CA, CP, IR, RA, SA, PM….

Key Takeaways

- ECOS approval is not the final act of agency acquisition of third- party services

- ECOS 525 Assessment does not replace the SEC 501 agency Risk Assessment requirements.

- Agency system and data owners still responsible for assessing “organization” controls in SEC 501

- Agency must still “onboard” the application for IT Ops support…

Questions & Answers

Thank You!

F5 Silverline – Managed Security Services

PRESENTED BY:

Christina Sinclair – Silverline Specialist

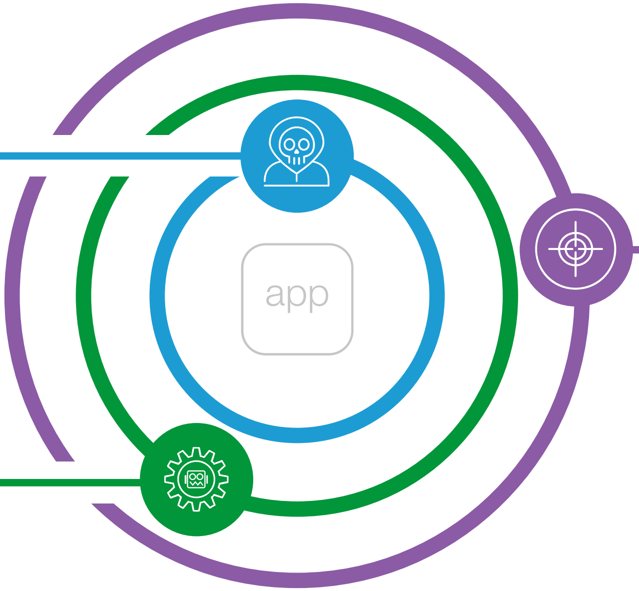
Matthew Neal – Silverline Solutions Engineer

WE MAKE APPS GO FASTER. SMARTER. SAFER.

F5 Silverline
WebApplication Firewall (WAF)

Application Layer Threat Types:

SAMPLE SET OF APPLICATION LEVEL ATTACK VECTORS



SOFTWARE VULNERABILITIES

- Known vulnerabilities (CVEs)
- OWASP Top 10 & well-known attack vectors
- Zero-day attacks

BOTS AND UNWANTED AUTOMATION

- Denial of Service (L7 and volumetric)
- Denial of Inventory
- Business logic attacks (fraud, intellectual property theft, abuse of service, abuse of brand)
- AND exploitation of software vulnerabilities and common attack vectors

TARGETED ATTACKS AND ADVANCED THREAT ACTORS

- Application reconnaissance and profiling
- Site specific vulnerabilities
- Bypass of security services
- AND development of exploits and methods used by bots and unwanted automation
- AND exploitation of software vulnerabilities and common attack vectors

F5 Silverline: WAF Policy Management Benefits

AUGMENT IN-HOUSE TEAMS WITH F5 SECURITY EXPERTS ON HAND TO DELIVER REQUIRED SECURITY INTENT

DECLARE INTENT

Define how your apps should be protected

Allow the SOC to handle the administrative effort

BENEFITS

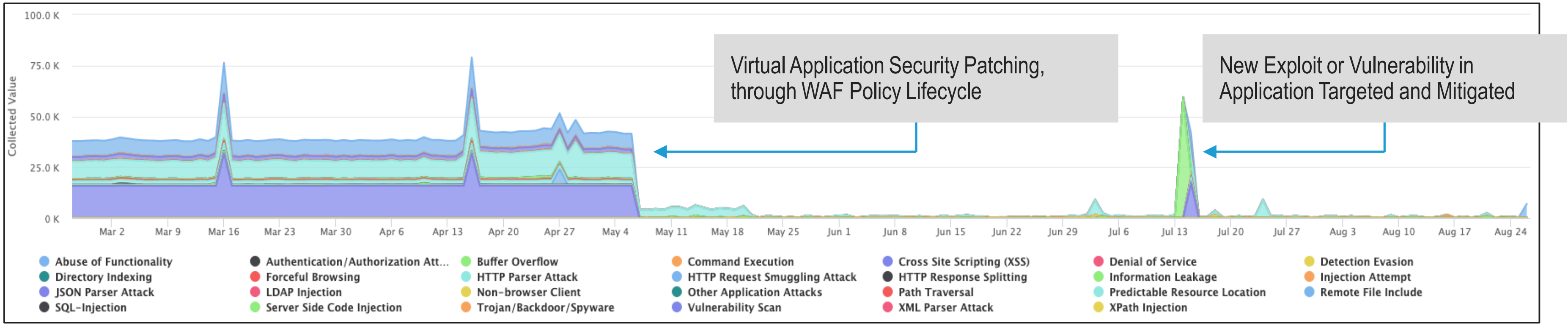
- Minimizes need for in-house F5 expertise
- Speeds deployment time
- Requires minimal effort
- Minimizes deployment errors
- Eases provisioning of application security
- Abstracts policy configuration complexity
- Repeatable and enforces policy compliance

Leverage the Silverline SOC as the **system** to deliver your declared intent

F5 Silverline WAF: Long Term Efficacy

SOLVE THE BLOCKING CYCLE OF OWASP APPLICATION THREATS

Attack Type Count



Virtual Application Security Patching, through WAF Policy Lifecycle

New Exploit or Vulnerability in Application Targeted and Mitigated

Malicious actors continually vary tactics and attack vectors
by retooling to take advantage of exploits or vulnerabilities in web applications

F5 Silverline Managed Services Offerings

:

Silverline DDoS Protection

- Network and application DDoS
- BGP/network and Proxy DDoS options
- Full provisioning and configuration
- Monitors and prevents attacks
- Integrated with on-premises F5 DDoS service

Silverline Web Application Firewall

- Complete infrastructure and software management
- Managed provisioning and service enablement
- Guided transition from learning to protected mode
- Expert created WAF policies and iRules

Silverline Shape Defense

- Protection against Bots and other automated attacks
- Blocks sophisticated credential stuffing and account take over attacks, carding, and the rest of the OWASP Automated Threats to Web Applications list
- Patented telemetry and signal collection along with advanced AI/ML
- Mitigates fraudulent and unwanted traffic in real-time

Silverline Threat Intelligence

- Restrict access to customer's networks and infrastructure for known bad actors (botnets, scanners, spammers, anonymous proxies, etc.)
- Enable granular threat reporting and automated blocking
- Flexible deployment options with expert provided guidance

F5 Silverline: The Difference

WHAT MAKES SILVERLINE UNIQUE

PEOPLE

SOC experts have an unrivalled breadth and depth of industry experience

F5 cyber security experts on-hand 24x7

Agile DevOps methodologies across product development teams

PLATFORM

Built on industry leading proven security technology

Flexible multi-layered application security stack

Cloud-based platform built with the highest levels of regulatory compliance & continuity in mind

PORTAL

Globally available and easy to use portal with integrated online chat services

Instant visibility & situational awareness for all application traffic

Rich contextual dashboards for analysis before, during and after attack mitigation

Enhance Security Efficacy

- **Purpose built - Dedicated Security Platform**
  - ➢ *Fastest to Identify – Fastest to Resolve*
- **Proven Proprietary Technology (F5 ASM/AWAF Closed-Sourced Security Module)**
  - ➢ *Reduced threat of reverse engineering Open-Sourced code exposure.*
- **Application Centric WAF Policies Built and Maintained by F5 Security Experts.**
  - ➢ *Proactive WAF Defense Policies: Minimize False/Positives and reduce Zero Day threats.*
- **Broaden Security Resources (Knowledge Base, Awareness, and Support).**
  - ➢ *Augment IT Security staff with F5 Cyber Security Experts on-hand 24x7x365.*

Optimize Operations

- **Rapidly Deploy and Scale**
  - *Security-as-a-Service further enables agile development and streamlining of End-to-End Defenses.*
  - *Managed Service backed by 150+ security experts, activated and directed by you, that become an extension of your team. Providing near real-time responses and execution with continuous oversight.*

- **Lower Total Costs of Ownership**
  - *Reduce time, Gain resources, and Eliminate the costs of managing Compliance, Continuity, and Hardware.*

- **Simplified Management**
  - Intuitive Portal, provides granular visibility and reporting. Parent/Child Account and TAG (RBAC) functionality within provides a seamless fit into any Operational Management Structure.

- **Maintain Visibility and Enhance Forensics**
  - *Integrate event log data into current SIEM, capture full payload data (PCAPS) on request, and unlimited 'Violation Assessments' by F5 Silverline SOC for additional forensic analysis.*

Protection and Performance Everywhere

- **Vendor Agnostic (In-Front of or Behind Silverline)**
  - ➢ *Protect web services, endpoints, or applications no matter where they reside.*

- **Future Proof**
  - ➢ *Future proof your security framework to or from any environment; pull policies from Silverline (Cloud) to F5 ASM (On-Prem) or vice versa.*

- **Interoperability**
  - ➢ *Leverage existing BIG-IP modules within your environment to pull threat detection data (Bandwidth, Bad Actors, Behavioral Violations)*

- **Improve End User Experience**
  - ➢ *Dedicated security platform provides 'Global Distribution with Local Resolution' and advance F5 Load-balancing functionality to your backend destination to optimize end-user resolution, performance, and costs.*

F5 Silverline Shape Defense: Use Cases

BOT MITIGATION & AUTOMATED ATTACK PREVENTION

Stop Account Takeover

Stops fraudsters from rapidly testing stolen credentials on your login applications which means they can’t take over accounts in the first place

Defend Against Web Scraping

Control how scrapers harvest data from your website so you can protect your most valuable and sensitive data

Mitigated Carding Fraud

Prevent criminals from using your checkout pages to validate stolen credit cards

Protect Loyalty Programs

Ensure gift card value, loyalty points and other stored values remain with your customers

Prevent Inventory Hoarding

Ensure your campaigns and most in demand items are sold directly to your customers, not to scalpers

Correct Skewed Analytics Data & Reduce Marketing Fraud

Ensure your business analytics and marketing spend are based on bot free data

F5 Silverline: The Outcome

INDUSTRY LEADING PROTECTION FOR MULTI-CLOUD HOSTED APPLICATIONS AND SERVICES

Applications Stay Available

- ✓ Delivers continuity for business-critical applications and online digital assets
- ✓ Apps stay available and secure to improve the end customer experience

Reduce Operating Costs

- ✓ Reduce traffic and bandwidth consumption costs
- ✓ Reduces time to achieve and the cost of managing application security
- ✓ Leverage F5 Silverline direct cloud peering

Insight & Visibility of Application Attacks

- ✓ Complete situational awareness of application security inline with intent based outcomes
- ✓ Drive efficiencies with comprehensive application security

Experts on-hand 24x7

- ✓ Augment IT security staff, with F5 cyber security experts on-hand 24x7
- ✓ Zero impact deployments with minimal cost and administrative overhead

Appendix

F5 Silverline DDoS Protection

MANAGED DDoS PROTECTION FOR YOUR MULTI-CLOUD INFRASTRUCTURE

ALWAYS ON:

Primary protection as the first line of defense

- Lowest "Time to Mitigate"
- Maximum visibility for attack trends and detected threats
- Consistent, reliable service delivery metrics and awareness
- Zero activation tasks
- Ideal for complex, dispersed customer application infrastructure

ALWAYS AVAILABLE:

Primary protection available on-demand

- On-Demand Service Activation by BGP or DNS Redirection
- No limit to the number of mitigation events or service activations
- Can be combined with Router Monitoring to provide detection and notification of DDoS events
- On-premises signaling functionality to accelerate attack detection and notification

Use Cases:

Protect Brand Reputation

Ensure your digital presence stays online during an attack, with real-time DDoS attack detection and mitigation in the Cloud

Defend your DNS

DNS is a key foundation to your digital presence. Defend it from DNS Flood, reflection and amplification attacks.

Defend against Volumetric Attacks

Globally available architecture, with multi-terabit capacity across high performant Tier 1 carriers, with direct public cloud peering

L7 DDoS Protection

Stop bad actors consuming resources and impacting application performance. Mitigations that adapt to user interactions

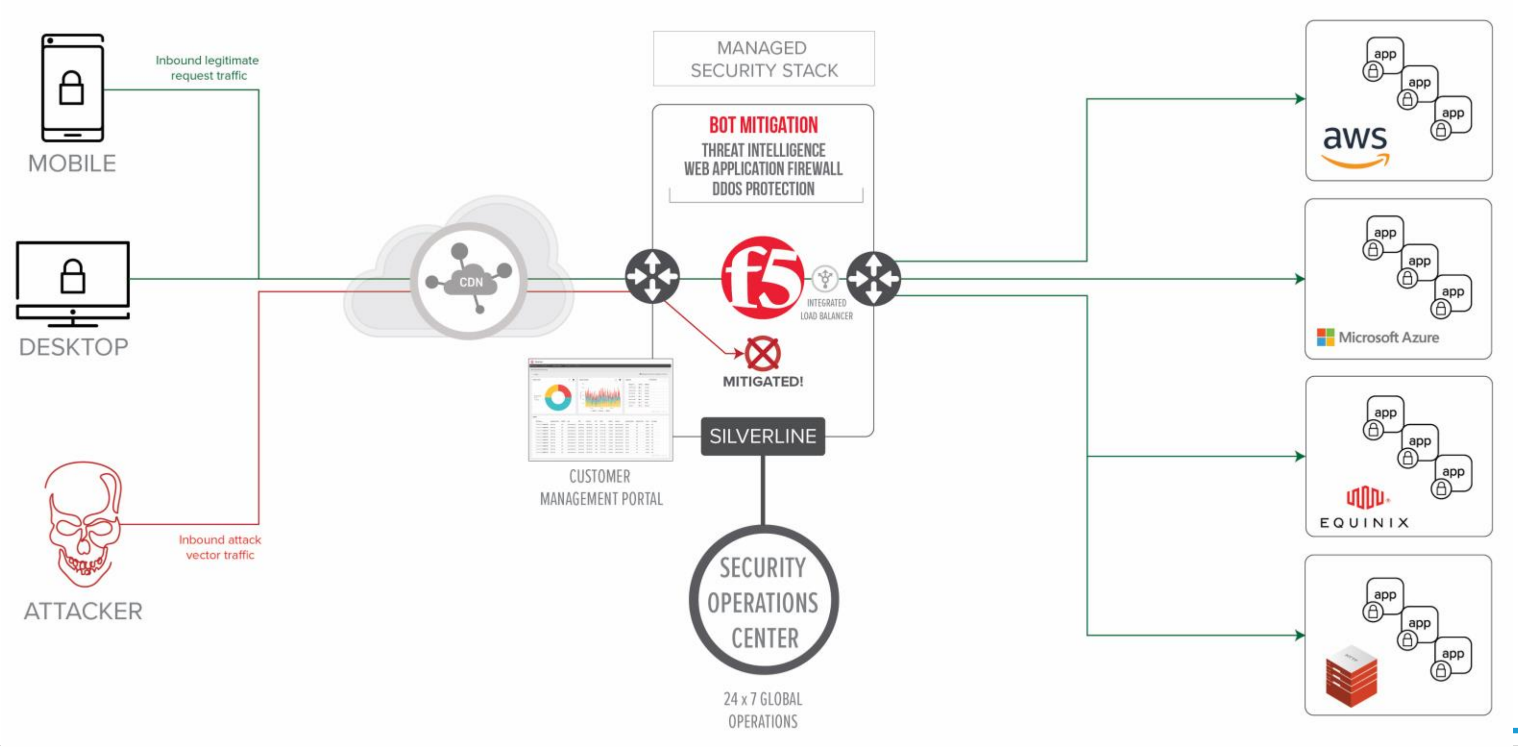
Attack Mitigation Insights

Transparent attack mitigation visibility from before, during and after attack. With complete awareness of mitigation implemented

Industry Unique Hybrid Deployments

Integrate on-prem F5 BIG-IP with Silverline Cloud based DDoS Mitigation, through threshold based automated signaling

Silverline Managed Layered Defense



F5 Silverline Managed Services

Global SOC 24x7x365

Continuous Monitoring and Incident Response

- Seattle, WA, United States
- Warsaw, Poland
- Guadalajara, Mexico

Global Deployment Model

Fully Redundant and Globally Distributed Data Centers

- San Jose, CA, US
- Ashburn, VA, US
- Columbus, OH, US
- Frankfurt, Germany
- London, UK
- Singapore, SG
- Sydney, AU
- Hong Kong, HK
- Mumbai, IN
- Montreal, CA
- São Paulo, BR
- Manama, BH
- Tokyo, JP

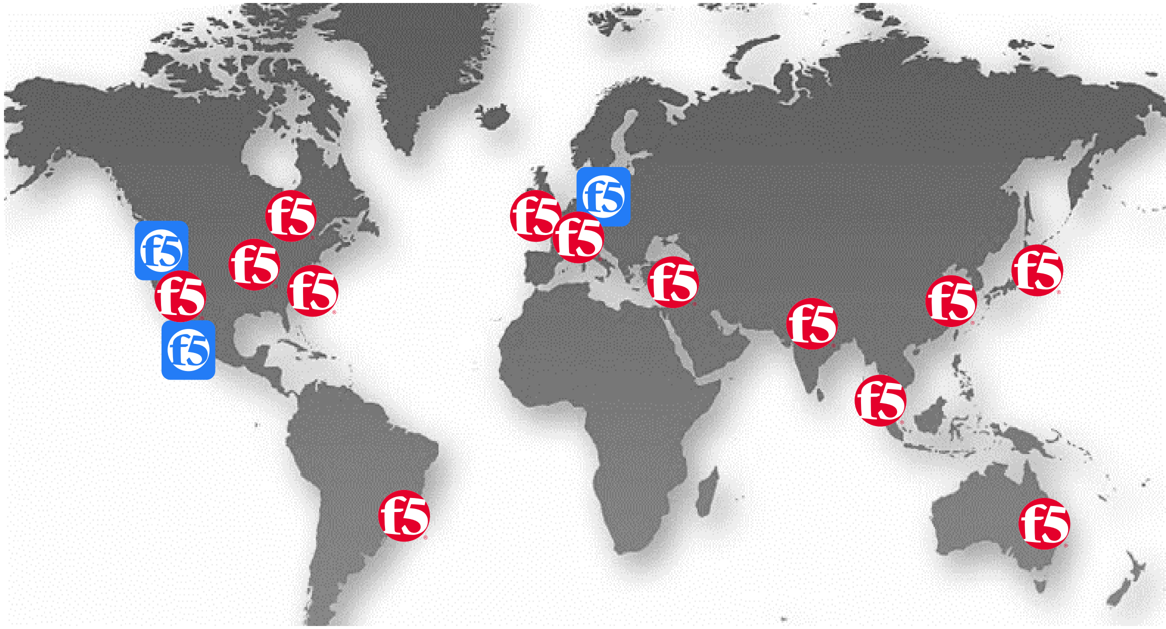
Performance Scalability Redundancy

- IP Anycast
- Dedicated L3/L4 and L7 scrubbing infrastructure
- Guaranteed bandwidth with Tier 1 carriers

HIPAA Compliant

PCI DSS COMPLIANT

EQUINIX



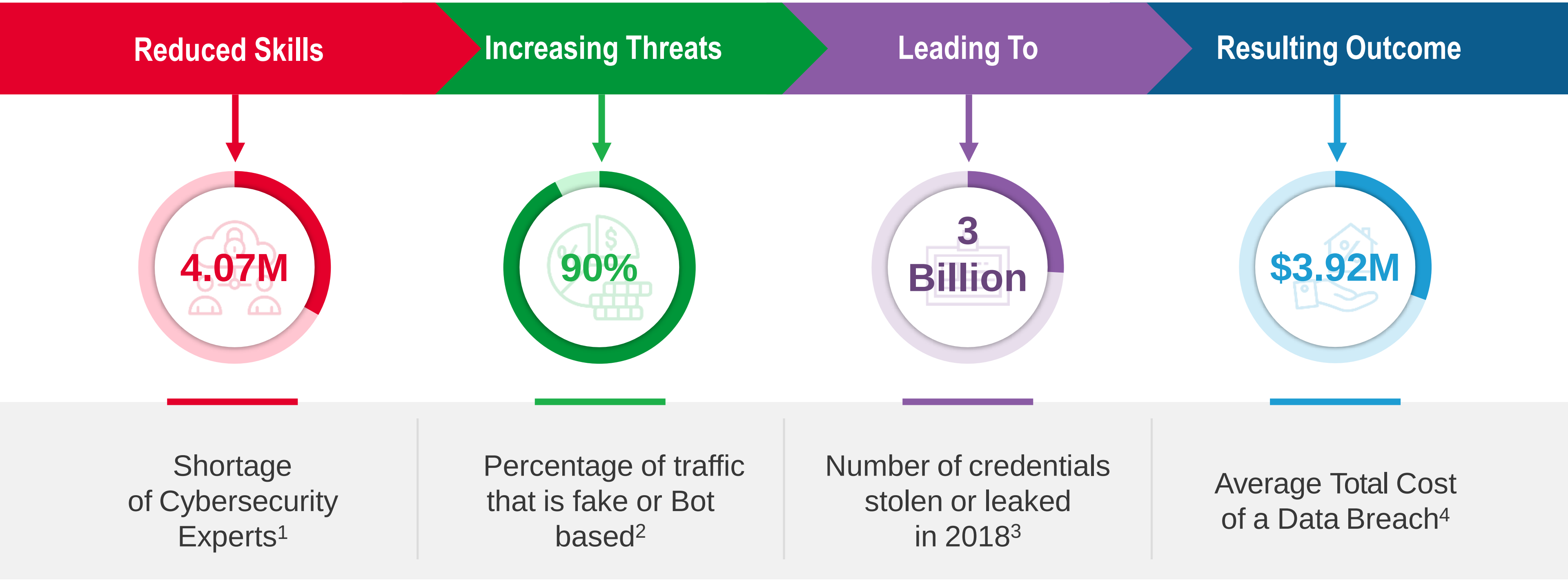
SOC Locations

Active Operations Centers

Future Operations Centers

Increasing Challenges of Digital Transformation

CAUSE AND EFFECT



Reduced Skills

4.07M

Shortage of Cybersecurity Experts[1]

Increasing Threats

90%

Percentage of traffic that is fake or Bot based[2]

Leading To

3 Billion

Number of credentials stolen or leaked in 2018[3]

Resulting Outcome

$3.92M

Average Total Cost of a Data Breach[4]

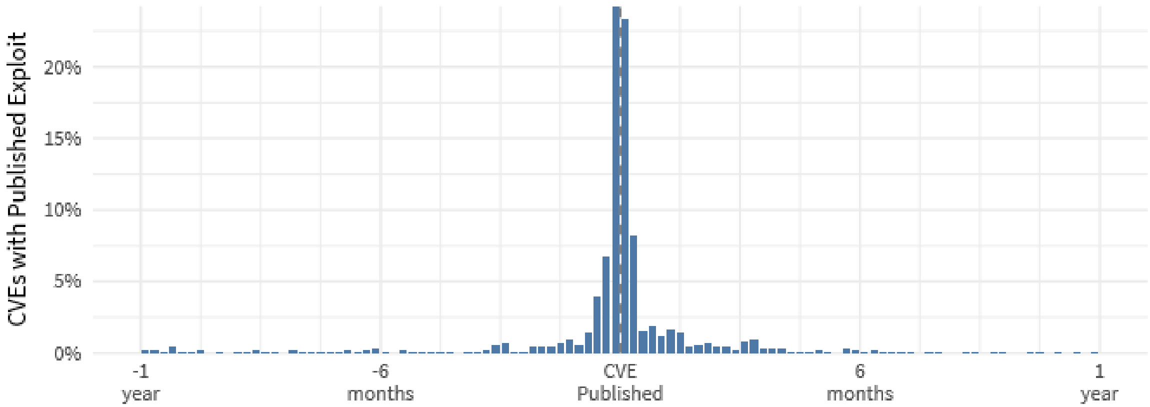
Data sources: 1. 2019 (ISC)^2 Cybersecurity Workforce Study; 2. Shape Security; 3. F5 Labs; 4. IBM/Poneman - 2019 Cost of a Data Breach Report.

22%

of vulnerabilities can be weaponized with public exploit code

Over half of all exploits are published with 2 weeks of the CVE publish date.

Exploit publication date relative to CVE publication date



Source: Kenna / Cyentia

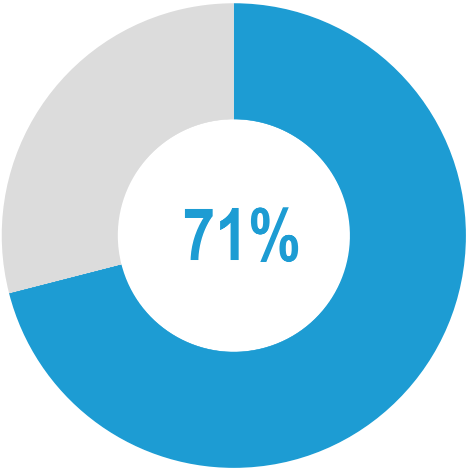
70% of all exploits are published within 1 month of CVE publish date.

Security skills are a challenge

OVER HALF OF ORGANIZATIONS REPORT APPLICATION SECURITY SKILLS DEFICIT

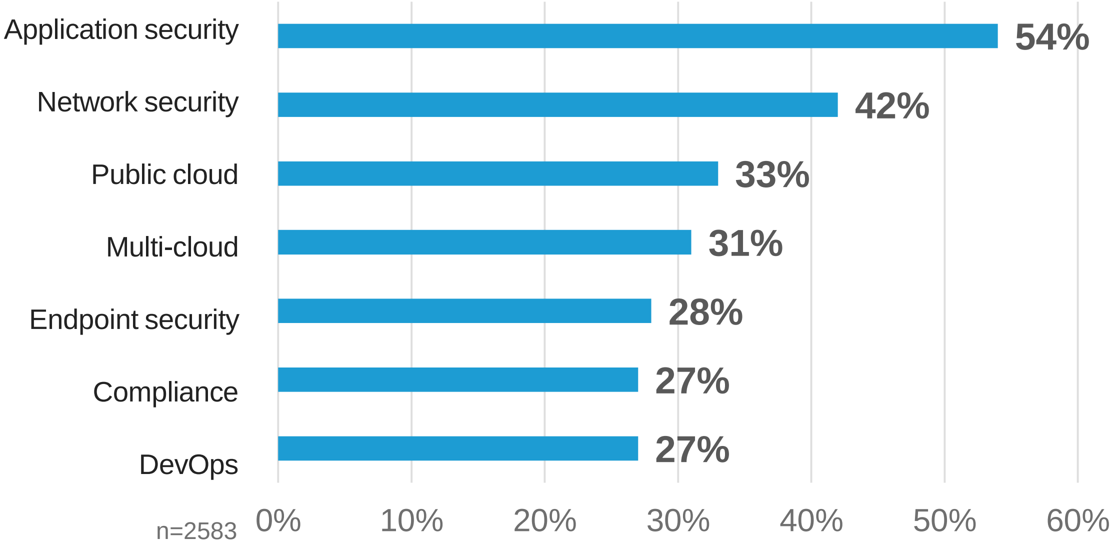
Q. Do you have a security gap/deficit in skills in your organization?

SECURITY SKILLS DEFICIT



Q. Which areas do you have a security gap/deficit in skills in your organization?

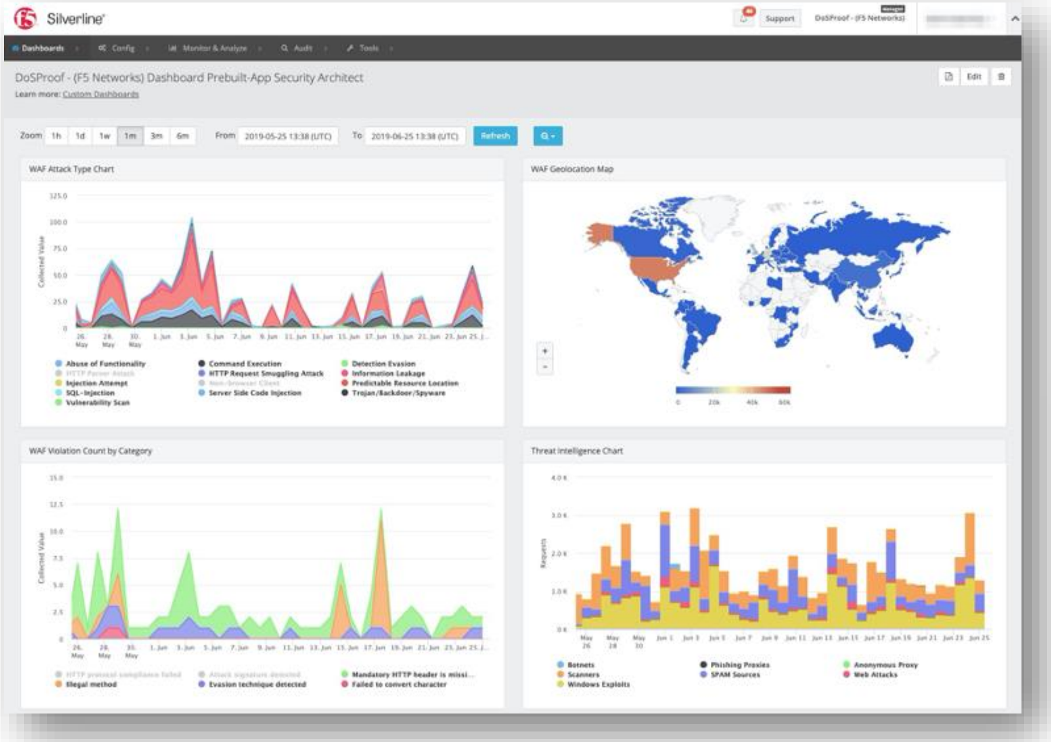
CATEGORY OF SKILLS DEFICIT



n=2583

Gain Insight and Visibility

REAL-TIME ANALYTICS BEFORE, DURING AND AFTER AN ATTACK



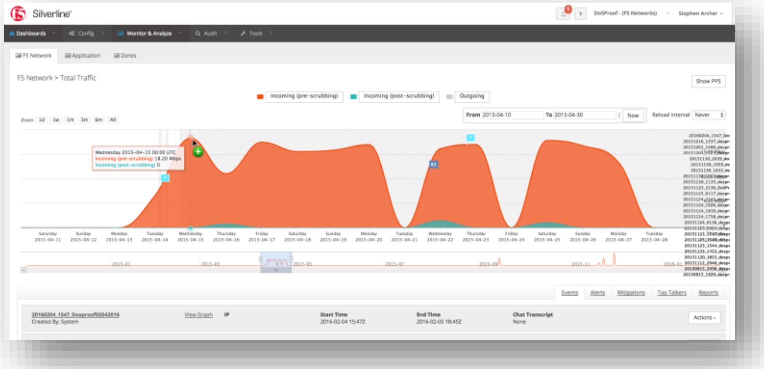
DoSProof - (F5 Networks) Dashboard Prebuilt-App Security Architect

Learn more: Custom Dashboards

From 2019-05-25 13:38 (UTC) To 2019-06-25 13:38 (UTC)

WAF Dashboards:

- ✓ Rich contextual insight into attacks
- ✓ Traffic timeline analysis
- ✓ Violations by count and/or category



F5 Network > Total Traffic

From 2015-04-10 To 2015-04-30

Reload Interval Never

Wednesday 2015-04-15 00:00 UTC
Incoming (pre-scrubbing) 18.20 Mbps
Incoming (post-scrubbing) 0

20160204_1547_Dosproof02042016
Created By: System

View Graph

IP

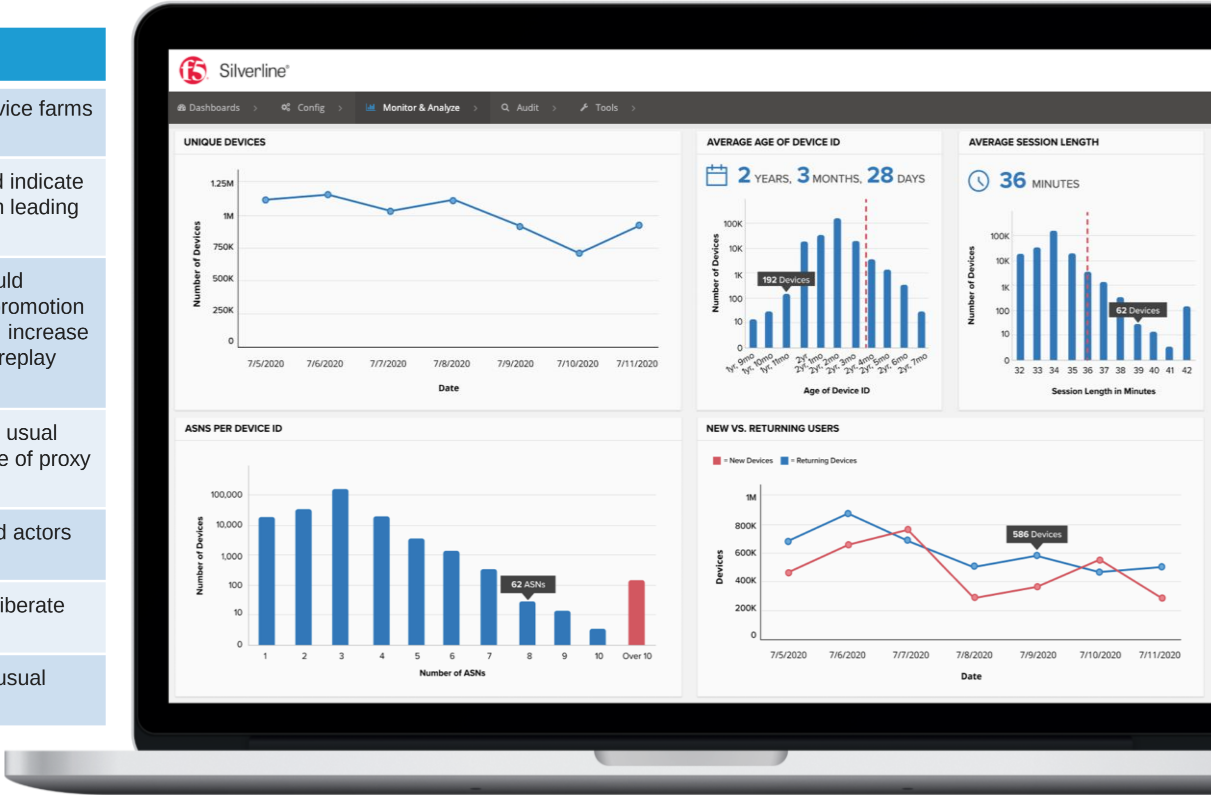
Start Time 2016-02-04 15:47Z

End Time 2016-02-05 18:45Z

Chat Transcript None

Device ID+ Dashboard Visibility

METRIC	PURPOSE
Number of devices per day	Sudden fluctuations could indicate device farms being used.
New vs Old Devices	Sudden increase in new devices could indicate malicious users or an active promotion leading to influx of new users.
Device age distribution	Sudden increase in young devices could indicate malicious users or an active promotion leading to influx of new users. Sudden increase in old devices could indicate a cookie replay attack.
Devices per country	New countries showing up outside the usual business geography could indicate use of proxy or malicious traffic
UA per device	Sudden fluctuations could indicate bad actors spoofing their environment
ASN per device	Sudden fluctuations could indicate deliberate use of proxy networks in an attack
Session length distribution	Sudden fluctuations could indicate unusual activity happening post login



FIRST MEETING — Customer / Security Operations Center

Customer introduction to onboarding process
WAF Questionnaire from Customer to SOC
Project Timelines and Team coordination
Customer Q&A with SOC team

PORTAL SETUP — Security Operations Center

Configure contract provisioning parameters
Create user accounts
Deploy base policy from questionnaire data

SSL UPLOAD — Customer

Upload SSL Certificate and Private Key
Confirm successful upload (SOC or Custom-

PROXY SETUP — Customer AND/OR Security Operations Center

Build and apply Front/Back End SSL profiles
Build and apply baseline Threat Intel profile
Build and apply baseline L7 DDoS profile
Build and apply baseline WAF policy
Configure back-end monitors (Default TCP)
Enable X-Forwarded-For
Place WAF policy in Transparent Mode
Set TCP Optimization Profile

PROXY TESTING — Customer

Test proxy http/s flow using local HOSTS file
Diff analysis on proxy page elements
Performance analysis (performed by customer)
Vulnerability Scan (performed by customer)
Resolve issues prior to production change

DNS CHANGE — Customer / Security Operations Center-OPT

Change DNS records to direct traffic to proxy
Identify and resolve any issues after change

PROXY TESTING — Customer

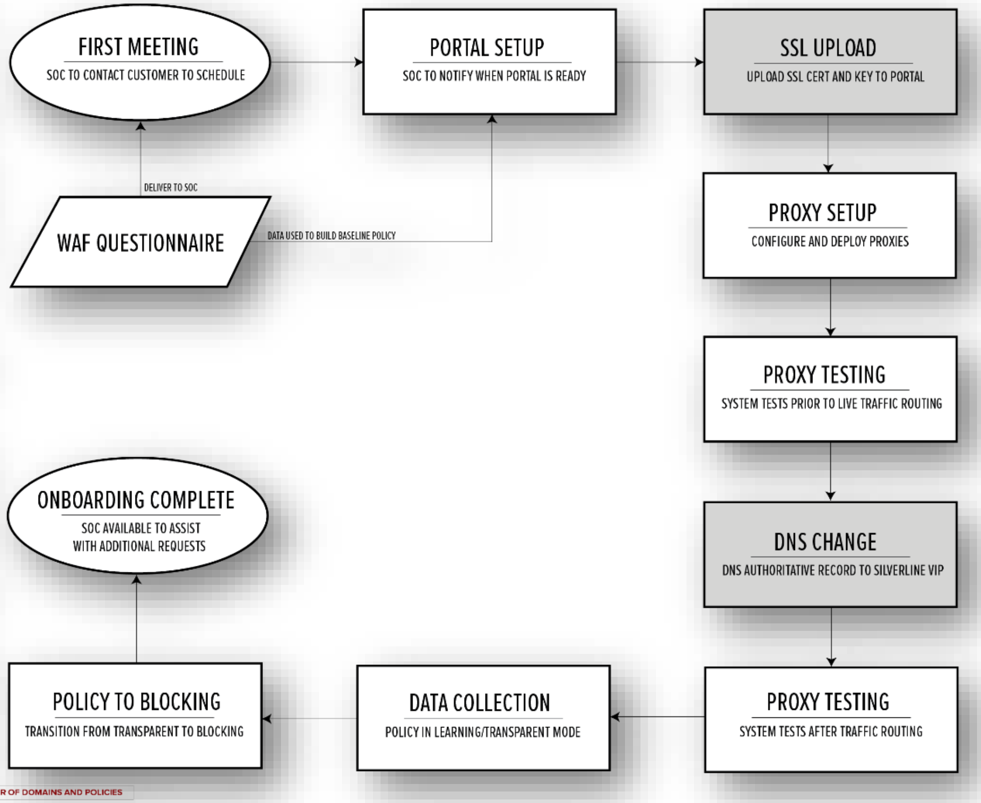
Diff analysis on proxy page elements
Performance analysis (performed by customer)
Vulnerability Scan (performed by customer)

DATA COLLECTION — Customer

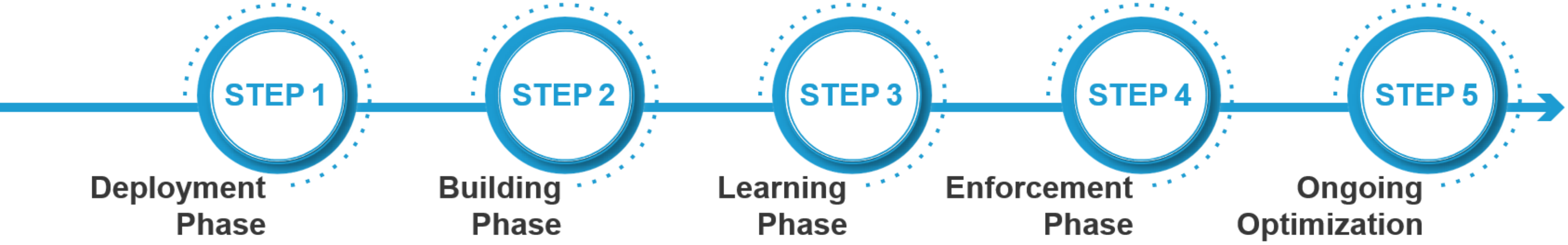
WAF Policy in ***Transparent*** *Mode only*
Define Data Collection period for baseline
Review WAF violation results during period
Initiate policy tuning based on collected data

BLOCKING — Customer / Security Operations Center

Request policy change to blocking phase one
Identify false postives and legitimate traffic
Remediate issues and tune policy as required
Geolocation Enforcement
Web Scraping
Parameter/URL length or format violations
Web Services violations


FIRST MEETING
SOC TO CONTACT CUSTOMER TO SCHEDULE
PORTAL SETUP
SOC TO NOTIFY WHEN PORTAL IS READY
SSL UPLOAD
UPLOAD SSL CERT AND KEY TO PORTAL
DELIVER TO SOC
WAF QUESTIONNAIRE
DATA USED TO BUILD BASELINE POLICY
PROXY SETUP
CONFIGURE AND DEPLOY PROXIES
PROXY TESTING
SYSTEM TESTS PRIOR TO LIVE TRAFFIC ROUTING
DNS CHANGE
DNS AUTHORITATIVE RECORD TO SILVERLINE VIP
ONBOARDING COMPLETE
SOC AVAILABLE TO ASSIST
WITH ADDITIONAL REQUESTS
POLICY TO BLOCKING
TRANSITION FROM TRANSPARENT TO BLOCKING
DATA COLLECTION
POLICY IN LEARNING/TRANSPARENT MODE
PROXY TESTING
SYSTEM TESTS AFTER TRAFFIC ROUTING

TIME TO EXECUTE ONBOARDING WILL VARY BASED ON NUMBER OF DOMAINS AND POLICIES



STEP 1
Deployment Phase

STEP 2
Building Phase

STEP 3
Learning Phase

STEP 4
Enforcement Phase

STEP 5
Ongoing Optimization

Phase I – Known Bad

F5 SILVERLINE MANAGED SERVICES

- Modules
  - Attack Signature Detected
  - Illegal HTTP Status in Response
  - Illegal Method
  - Illegal URL (if disallowed URLs configured)
- Attack Types
  - Command Execution Signatures
  - Cross Site Scripting Signatures
  - Directory Index Signatures
  - HTTP Response Splitting
  - Information Leakage
  - OS Command Injection
  - Path Traversal
  - Remote File Includes
  - SQL Injection
  - Server-Side Code Injection
  - Xpath Injection
  - Information Leakage
  - Forceful Browsing

Phase II - RFC

F5 SILVERLINE MANAGED SERVICES

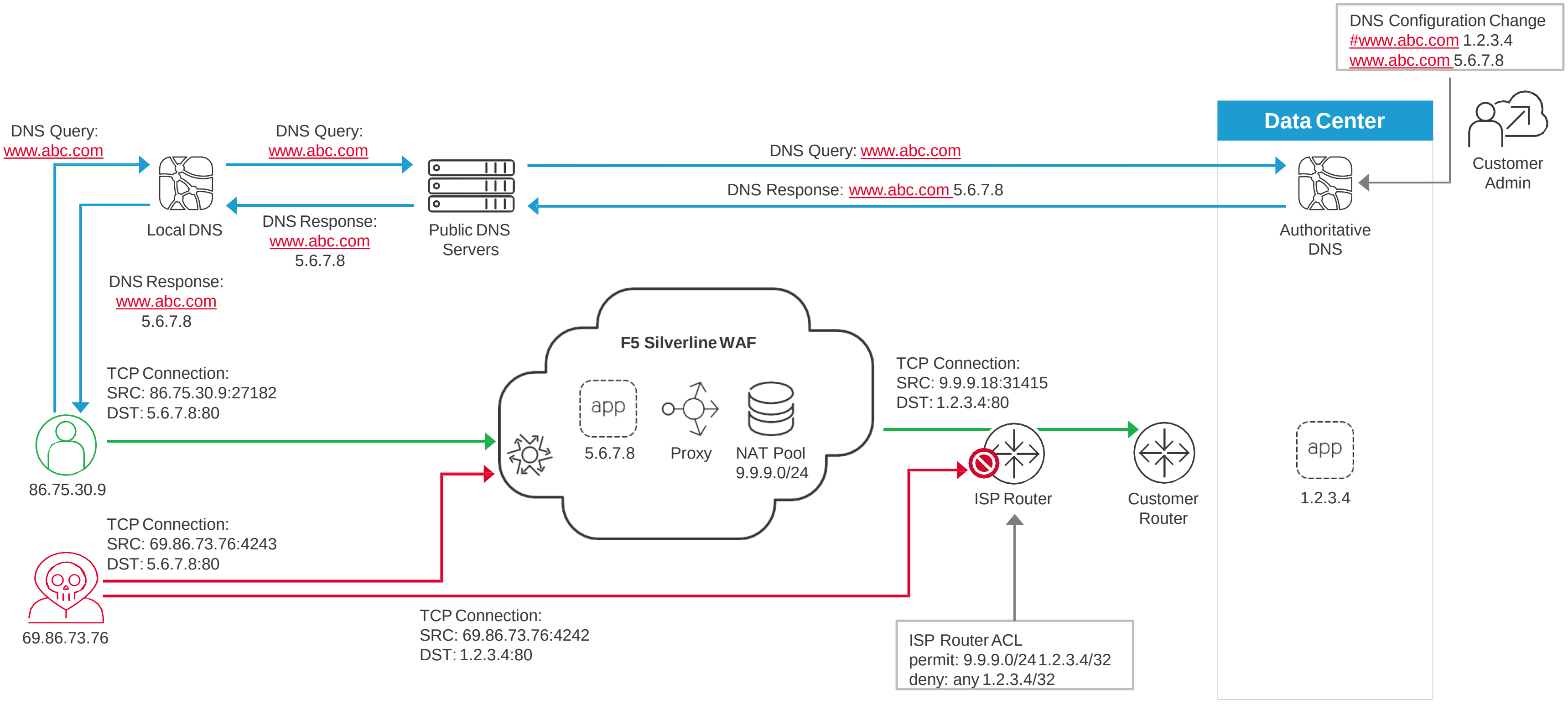
- Modules
  - Cookie not RFC Compliant
  - Disallowed File Upload Content Detected
  - Evasion Technique Detected
  - Failed to Convert Character
  - HTTP Protocol Compliance Failed
  - Request Length Exceeds Defined Buffer Size
  - Mandatory HTTP Header is Missing
- Attack Types
  - Detection Evasion
  - HTTP Parser Attack
  - Abuse of Functionality
  - Parameter Tampering

Phase III – Known Goods

F5 SILVERLINE MANAGED SERVICES

- Modules Tuned
  - Parameter related violations (when configured)
  - Illegal File Type
  - Illegal Redirection Attempt
  - Modified Domain Cookies
  - Illegal URL (for allowed URLs, when appropriate for the application)
  - Malformed JSON data
  - Malformed XML data
- Attack Types
  - Abuse of Functionality
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Forceful Browsing
  - Illegal Redirection
  - Parameter Tampering
  - Path Traversal
  - Predictable Resource Location
  - Remote File Include
  - Server-Side Code Injection
  - Session Hijacking
- Attack Types
  - SQL-Injection
  - Vulnerability Scan
  - Web Scraping
  - XML Parser Attack

F5 Silverline Proxy Configuration



VIRGINIA
IT AGENCY

NTT DATA MESSAGING SERVICES

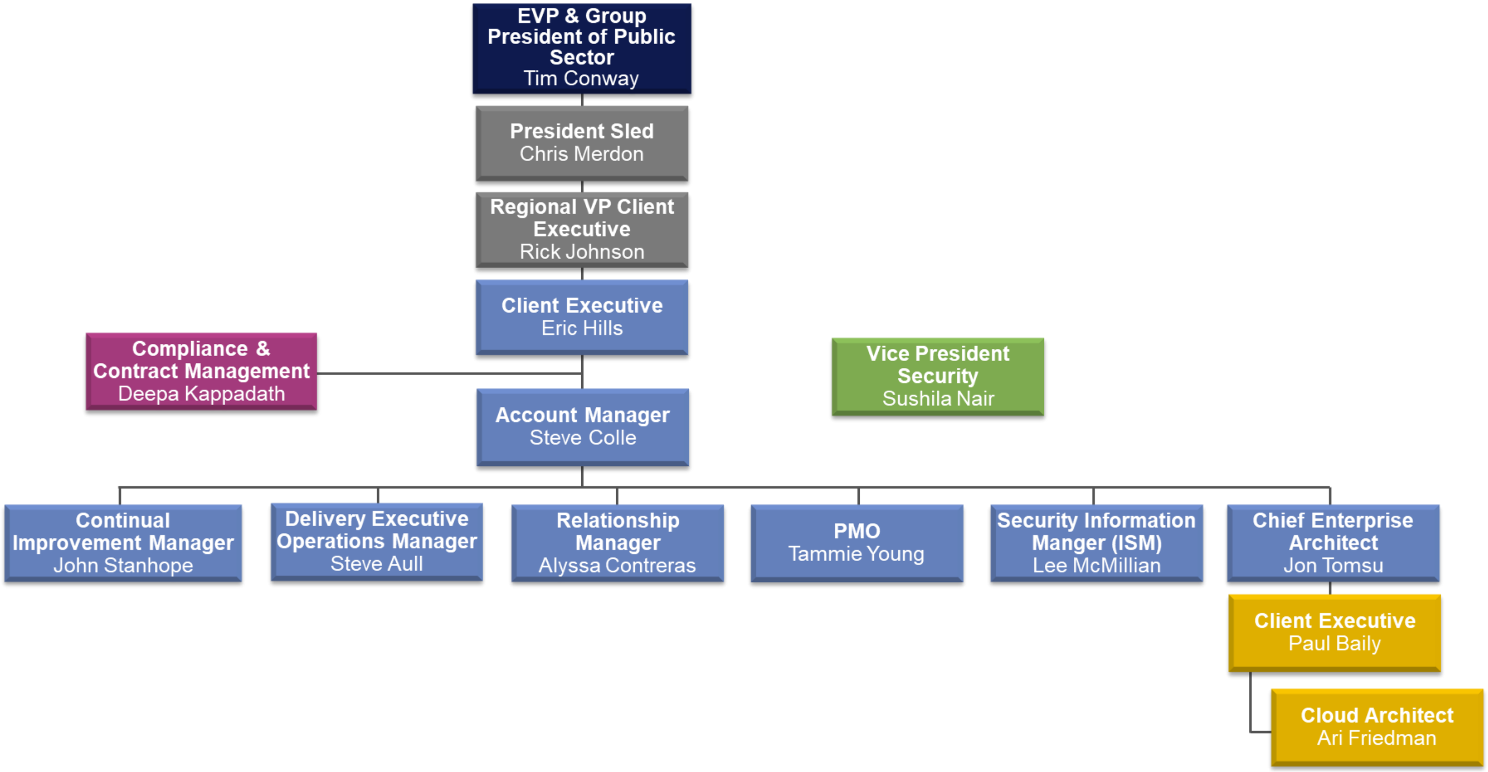
ERIC HILLS, STEVE COLLE & LEE MCMILLIAN

NTT DATA

SEPTEMBER 2021

AGENDA

1. Org Structure
2. Goals & Objectives
3. Messaging Solution
4. Service Overview
5. Transition Timeline
6. Security Improvements
7. Q&A



EVP & Group President of Public Sector
Tim Conway

President Sled
Chris Merdon

Regional VP Client Executive
Rick Johnson

Client Executive
Eric Hills

Compliance & Contract Management
Deepa Kappadath

Vice President Security
Sushila Nair

Account Manager
Steve Colle

Continual Improvement Manager
John Stanhope

Delivery Executive Operations Manager
Steve Aull

Relationship Manager
Alyssa Contreras

PMO
Tammie Young

Security Information Manger (ISM)
Lee McMillian

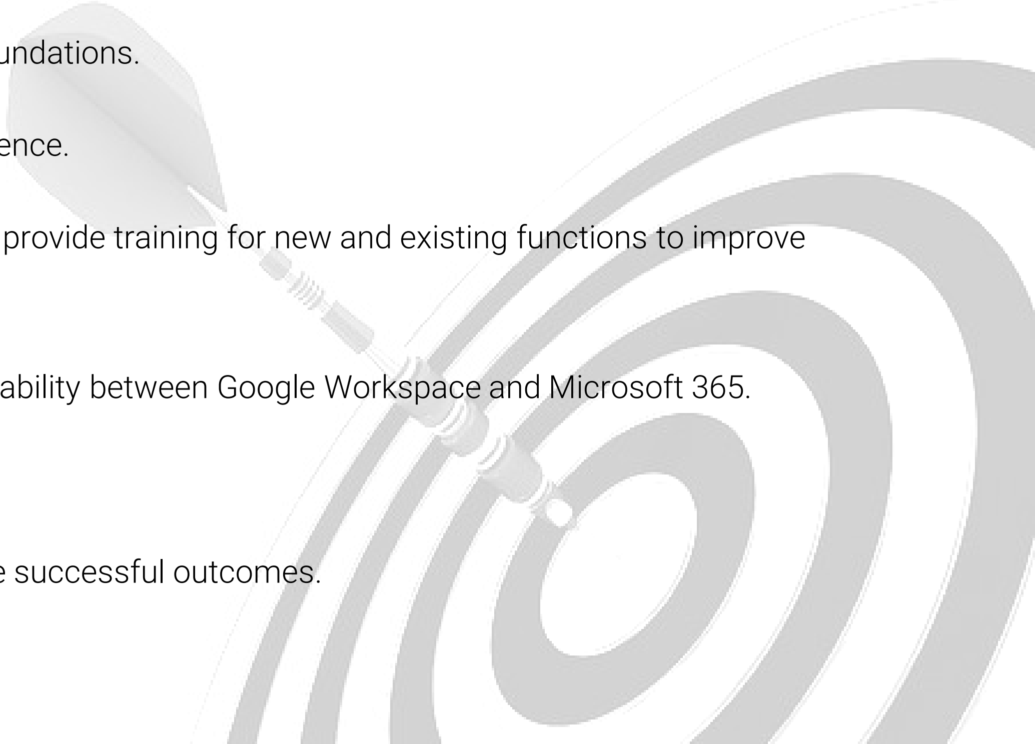
Chief Enterprise Architect
Jon Tomsu

Client Executive
Paul Baily

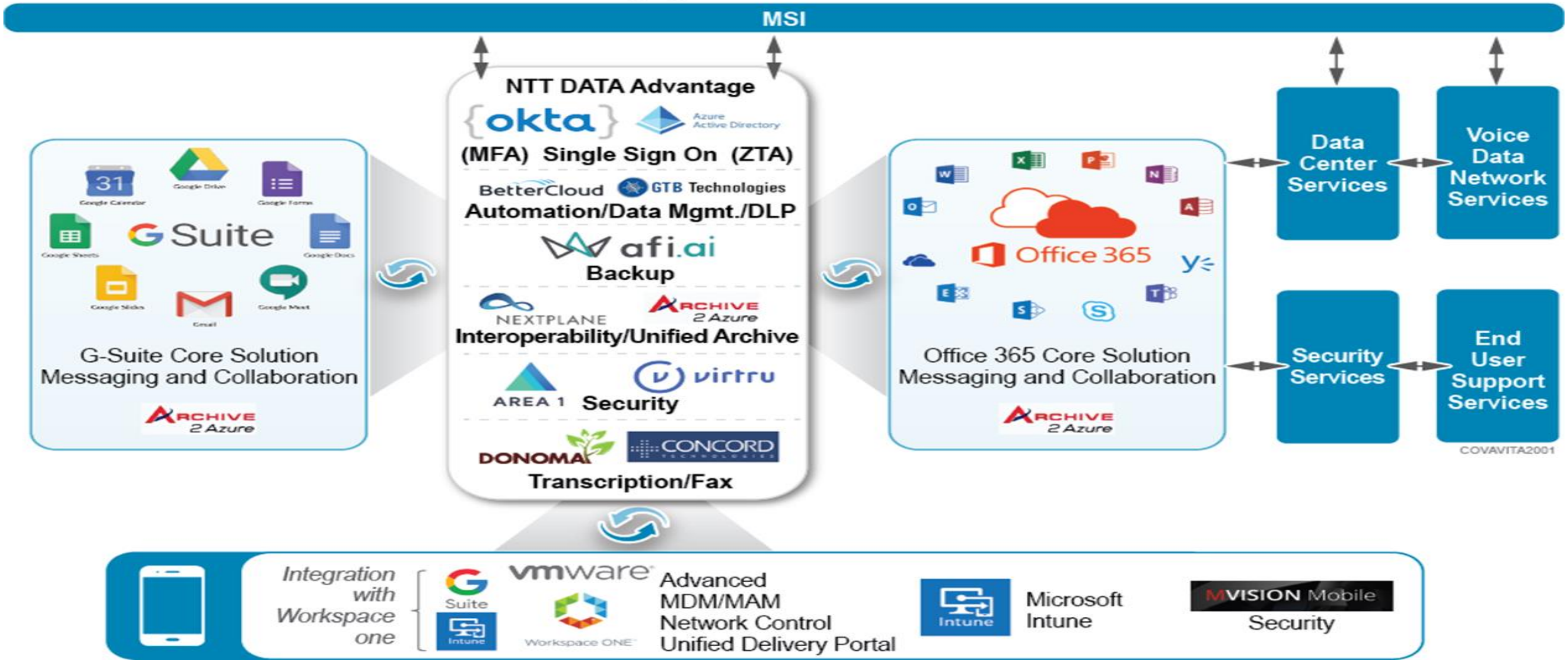
Cloud Architect
Ari Friedman

GOALS AND OBJECTIVES

- Improved product and project delivery using ITIL foundations.
- Solution focused on enhancing the End User experience.
- Identify new functionality as it comes available and provide training for new and existing functions to improve productivity.
- Evolve the current environment to provide interoperability between Google Workspace and Microsoft 365.
- Focus on first call resolution.
- End to end integration within the MSI model to drive successful outcomes.



VITA Messaging Service Architectural Framework



MSI

NTT DATA Advantage

(MFA) Single Sign On (ZTA)

Automation/Data Mgmt./DLP

Backup

Interoperability/Unified Archive

Security

Transcription/Fax

G-Suite Core Solution Messaging and Collaboration

Office 365 Core Solution Messaging and Collaboration

Data Center Services

Voice Data Network Services

Security Services

End User Support Services

Integration with Workspace one

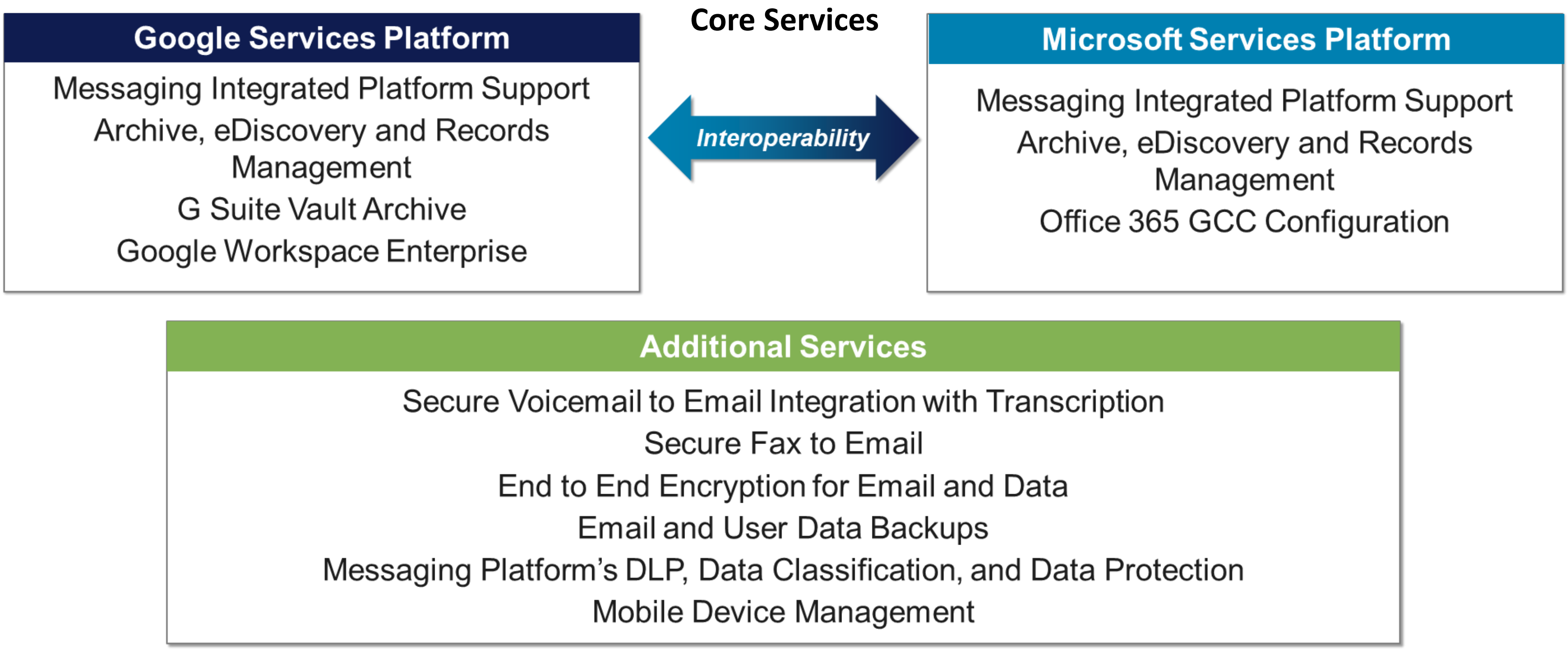
Advanced MDM/MAM Network Control Unified Delivery Portal

Microsoft Intune

Security

COVAVITA2001

MESSAGING SERVICE OVERVIEW



Core Services

Google Services Platform

Messaging Integrated Platform Support
Archive, eDiscovery and Records Management
G Suite Vault Archive
Google Workspace Enterprise

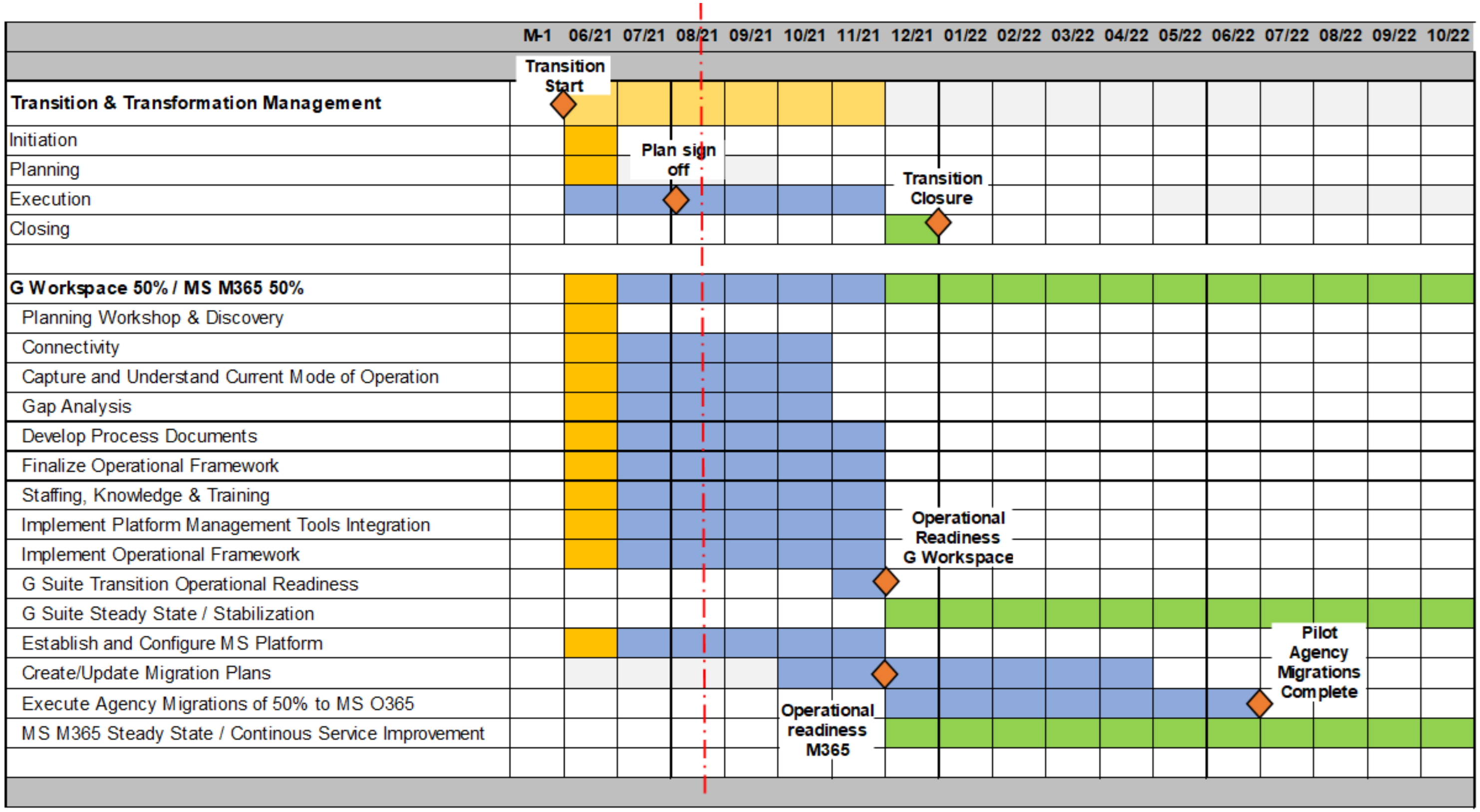
Interoperability

Microsoft Services Platform

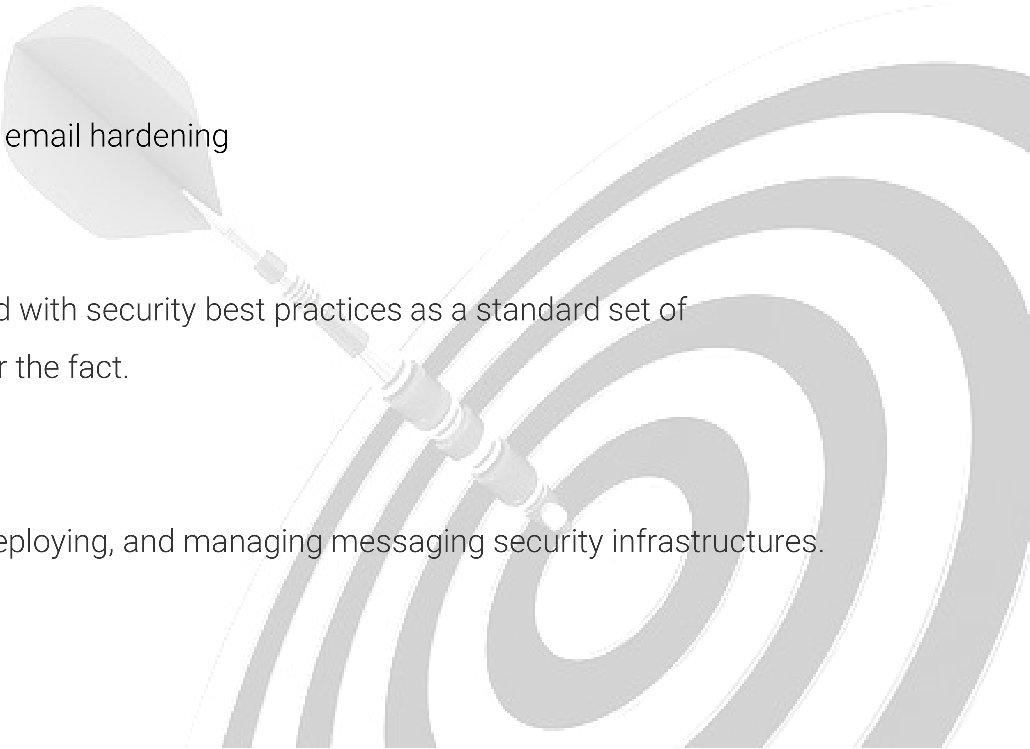
Messaging Integrated Platform Support
Archive, eDiscovery and Records Management
Office 365 GCC Configuration

Additional Services

Secure Voicemail to Email Integration with Transcription
Secure Fax to Email
End to End Encryption for Email and Data
Email and User Data Backups
Messaging Platform’s DLP, Data Classification, and Data Protection
Mobile Device Management



	M-1	06/21	07/21	08/21	09/21	10/21	11/21	12/21	01/22	02/22	03/22	04/22	05/22	06/22	07/22	08/22	09/22	10/22
Transition & Transformation Management	◆ Transition Start	🟨	🟨	🟨	🟨	🟨	🟨											
Initiation		🟧																
Planning		🟧																
Execution		🟦	🟦 ◆ Plan sign off	🟦	🟦	🟦	🟦											
Closing								🟩 ◆ Transition Closure										
G Workspace 50% / MS M365 50%		🟧	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Planning Workshop & Discovery		🟧																
Connectivity		🟧	🟦	🟦	🟦	🟦												
Capture and Understand Current Mode of Operation		🟧	🟦	🟦	🟦	🟦												
Gap Analysis		🟧	🟦	🟦	🟦	🟦												
Develop Process Documents		🟧	🟦	🟦	🟦	🟦	🟦											
Finalize Operational Framework		🟧	🟦	🟦	🟦	🟦	🟦											
Staffing, Knowledge & Training		🟧	🟦	🟦	🟦	🟦	🟦											
Implement Platform Management Tools Integration		🟧	🟦	🟦	🟦	🟦	🟦											
Implement Operational Framework		🟧	🟦	🟦	🟦	🟦	🟦	Operational Readiness G Workspace										
G Suite Transition Operational Readiness							🟦 ◆											
G Suite Steady State / Stabilization								🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Establish and Configure MS Platform		🟧	🟦	🟦	🟦	🟦	🟦								Pilot Agency Migrations Complete			
Create/Update Migration Plans						🟦	🟦 ◆	🟦	🟦	🟦	🟦	🟦						
Execute Agency Migrations of 50% to MS O365						Operational readiness M365		🟦	🟦	🟦	🟦	🟦	🟦	🟦 ◆				
MS M365 Steady State / Continous Service Improvement								🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩



- Email Hardening - Google Cloud Infrastructure
  - Providing security improvements and focus on email hardening
- Native Security Integration
  - The messaging infrastructure is being designed with security best practices as a standard set of features instead of a cumbersome bolt-on after the fact.
- NTT DATA Security Team Expertise
  - Over 25 years of experience with developing, deploying, and managing messaging security infrastructures.

QUESTIONS?

THANK YOU!

TapadhLeat
Koszonom
Murakoze
aDank
BarakAllahuFiik
Grazzi
Grazie
Buznyg
WaadMahadsantahay
ThintKo
Takk
Thank
Mèsi
Chokrane
Kiitos
Blagodaram
Rahmat
Xièxie
Dziakuju
Mauruuru
Matondo
TerimaKasih
Aabhar
Barkal
GratiasAgimus
Mercé
Gracias
Taiku
Tanemirt
Tenki
Aciū
Dankie
Motashakkeram
Dakujem
Merci
You
Spacibo
Danke
Chnorakaloutioun
TänanVäga
Tak
Sagolun
Grandmerce
GratiasAgo
Gràcies
NajisTuke
Hvala
Arigato
Gracie
KopKhunKha
Faleminderit
KamSahHamnida
CámOn
Efharisto
Multumesc
Saha
Nirringrazzjak
Bayarlalaa
Obrigado
Salamat
Gratzias

Voice of Our Clients and Security Trends

VITA ISOAG Meeting

September 1, 2021

Today’s agenda

● CGI Overview

● Voice of Our Clients Overview

● CGI in the Government Industry

● CGI Government Client Insights and Observations

Technology Trends

Security Trends

Summary – [Cyberthreat Defense Report | (ISC)² (isc2.org)]

CGI Overview

CGI at a glance

Founded in 1976

44 years of excellence

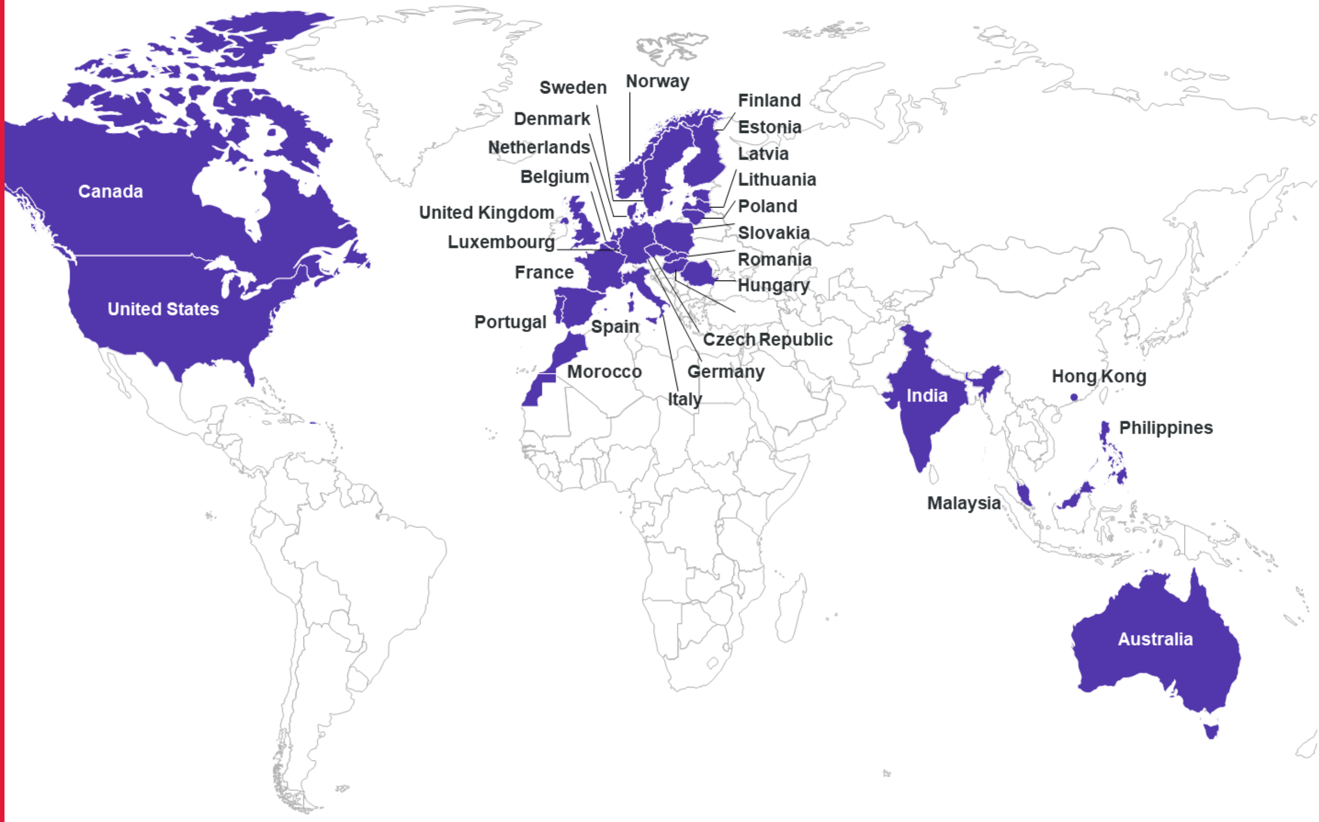
CA$12.2 billion revenue

77,000 consultants

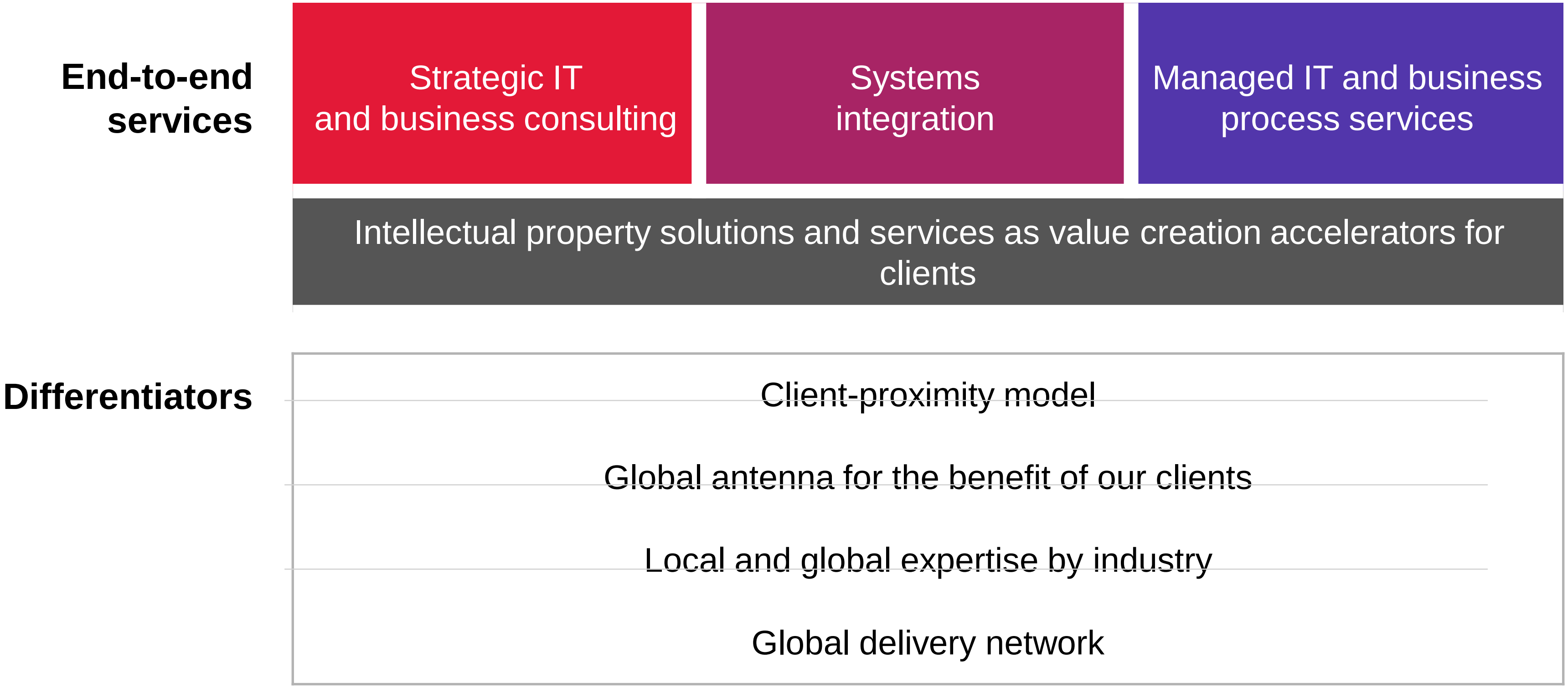
400 locations in 40 countries

5,500 clients benefiting from end-to-end services

IP-based solutions serving 50,000 clients



Range of services and differentiators



End-to-end services

Strategic IT and business consulting

Systems integration

Managed IT and business process services

Intellectual property solutions and services as value creation accelerators for clients

Differentiators

Client-proximity model

Global antenna for the benefit of our clients

Local and global expertise by industry

Global delivery network

CGI’s commitment to the Commonwealth

U.S. head office in Fairfax

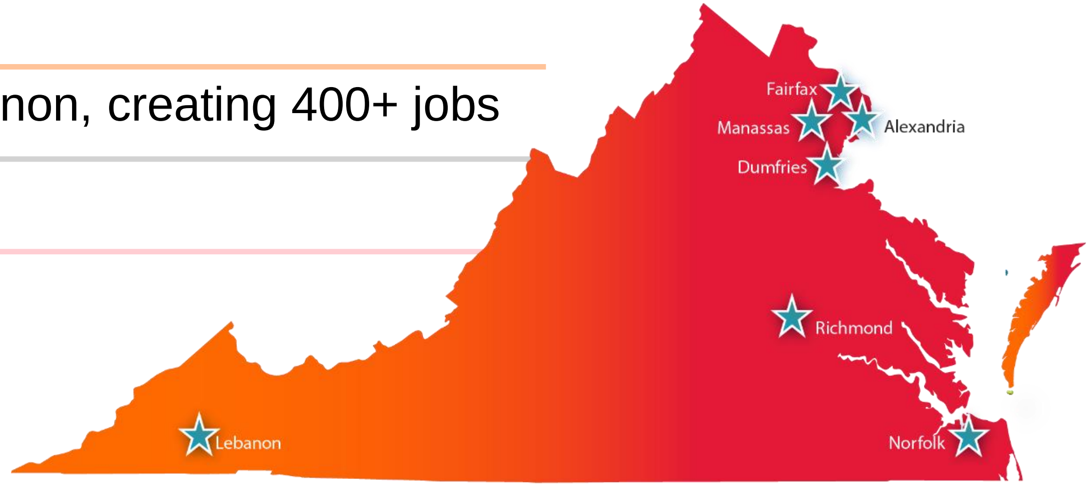
4,200 Virginia-based employees

Downtown Richmond office

On-shore delivery center in Lebanon, creating 400+ jobs

Offices in 7 locations

Long-term economic partnership



CGI in the Commonwealth of Virginia

Power Revenue Management and Tax Collections

Deliver state-wide eProcurement and Transparency via eVA

Agency Database Support

Support / Modernize Retirement Systems

Election Systems Support

Medicaid eHealth Records Incentives

Cloud Migration
Platform Development
Data Analytics
Project Management
App Dev and Management
Advanced Automation
Security Consulting
Database Management

AWS and Azure
Microsoft Dynamics
Salesforce
Tableau
.NET and Java
Ivalua Procurement
Advantage ERP
Tableau

Voice of Our Clients
2021 demographics

Voice of Our Clients

Depth of our insights

Since 2017

7,470
discussions

1M
data points collected

$371B
annual IT spend

In 2021

1,695
discussions

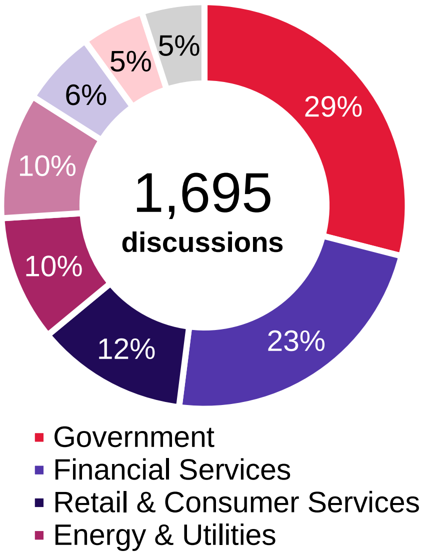
58%
CXOs interviewed

46%
business leaders

54%
IT leaders

7
major regions

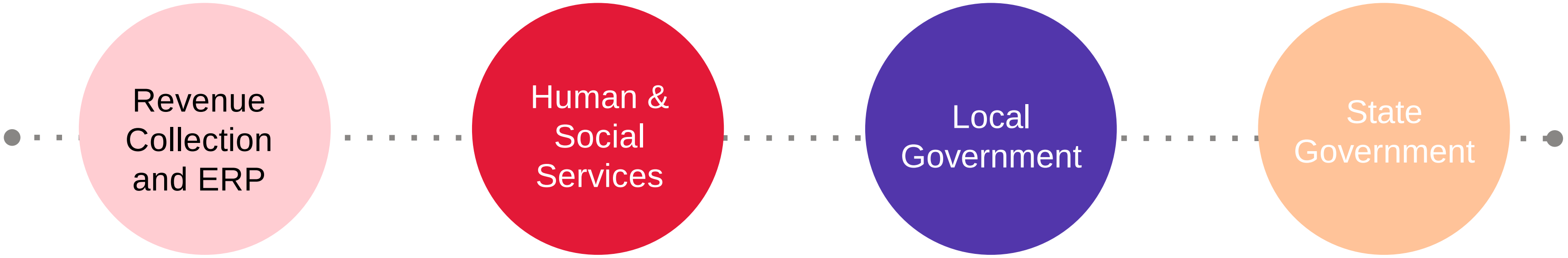
14%
new clients



© 2021 CGI Inc.

CGI in Government

CGI in Provincial & Municipal Government



- **10%** of CGI’s revenue
- Serve **Provincial & Municipal Government** in North America & Europe
- **7,000+ industry experts** across the globe delivering core citizen services for government
- Partner to our top clients for an **average of 15 years**
- **IP** like Advantage ERP, Advantage Revenue and Collections

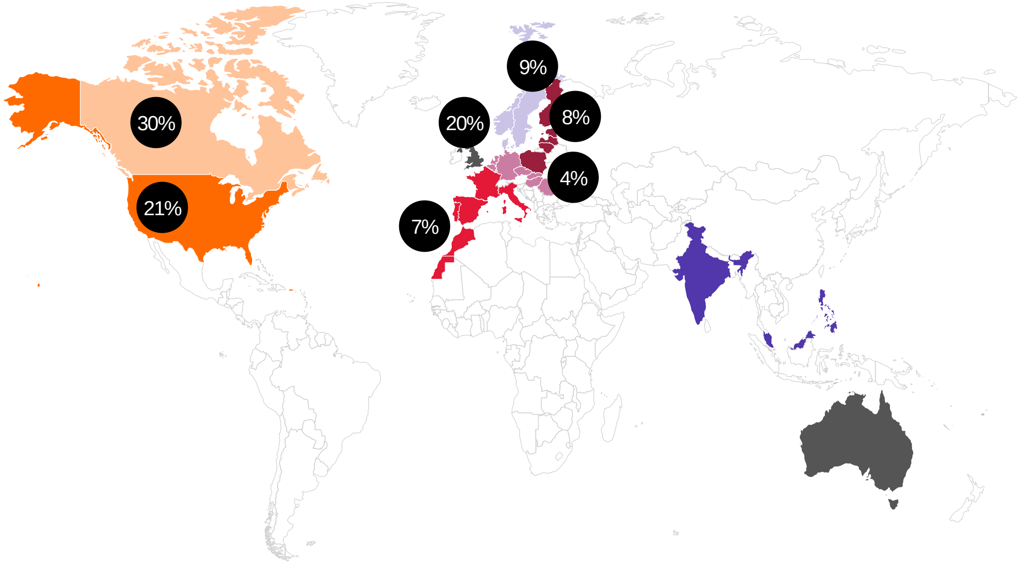
Industry VOC insights

CGI’s Global Antenna

Provincial & Municipal	
52%	Provincial
48%	Municipal

139

Total **interviews**



8 Major Regions

- Asia Pacific
- Canada
- Central & Eastern Europe
- Finland, Poland & Baltics
- Scandinavia
- United States
- UK & Australia
- Western & Southern Europe

62% **CXO** Interviewed

43% **Business** Leaders

57% **IT** Leaders

12% **New** Clients

Business Priorities: Government executive priorities remain the same year over year

By Impact

2020		**2021**		
1	Improve citizen services and experience – 2.0	1	▼	Improve citizen services and experience – 2.2
2	Optimize today's operations and do better for less – 2.5	2	▼	Optimize today's operations and do better for less – 3.2
3	Protect the organization as cybersecurity risks mature – 3.6	3	▲	Protect the organization as cybersecurity risks mature – 3.4
4	Harness the power of data analytics to improve insight – 3.7	4	▲	Harness the power of data analytics to improve insight – 3.7
5	Collaborate across the boundaries of our organization – 4.0	5	▲	Collaborate across the boundaries of our organization – 3.8

▼ ▲ *Indicates rating value change*

Industry Trends: Use of public cloud emerges in top five while workforce challenges drop off – as Government adopts PaaS, SaaS and Cloud solutions retaining certain high tech skills may drop

By Impact

2020		**2021**	
1	Becoming digital organizations to meet increasing citizen expectations – 1.9	1 ▼	Becoming digital organizations to meet increasing citizen expectations – 2.3
2	Protecting through cybersecurity – 2.8	2 ▼	Protecting through cybersecurity – 2.9
3	Coping with budget pressure through IT consolidation and process automation – 2.8	3 ▼	Coping with budget pressure through IT consolidation and process automation – 3.2
4	Assuring regulatory compliance – 3.8	4 ▲	Assuring regulatory compliance – 3.8
5	Aging workforce - challenge of attracting and retaining upcoming talent – 3.9	5 ▼	Increasing use of public and private cloud – 4.0

▼ ▲ *Indicates rating value change*

IT Priorities: Remain the same year over year

By Impact

	2020		2021
1	Digitize and automate business Processes to deliver better citizen service – 1.8	1 ▼	Digitize and automate business processes to deliver better citizen service – 2.4
2	Drive IT modernization to improve Efficiency – 2.5	2 ▼	Drive IT modernization to improve Efficiency – 3.0
3	Protect through cybersecurity – 3.1	3 ▼	Protect through cybersecurity – 3.1
4	Establish effective IT roadmap, governance and management – 3.7	4 ▼	Establish effective IT roadmap, governance and management – 3.8
5	Embrace new and agile IT delivery models (e.g. SaaS and PaaS) – 4.4	5 ▲	Embrace new and agile IT delivery models (e.g. SaaS and PaaS) – 4.2

▼ ▲ *Indicates rating value change*

Digital Transformation Strategy: While digital strategies are in place, few are reporting results

Strategy Producing Results by **Geography**

	Global	Canada	CEE	FPB	Scan	UK/Aus	US CSG	US FED	WSE
VOC 2021	**19%**	12%	50%	14%	27%	21%	18%	NA	25%
VOC 2020	**8%**	NA	NA	14%	NA	13%	17%	NA	NA

Strategy Producing Results by **Sub-Industry**

	Municipal	Provincial
VOC 2021	22%	16%
VOC 2020	14%	2%

36% say that their legacy systems pose a significant challenge to the successful implementation of their digitization strategy (8-10 rank – Q6.5)

37% believe they are more advanced than their peers in leveraging digitization. (8-10 rank – Q6.6)

Significant progress in digital transformation with 84% having a strategy but only 19% producing results. Results are increasing from **8% to 19%** year over year.

Cloud Solutions: More than half of government entities are planning to move 21% of their applications to Cloud solutions

Plan to **Modernize** Application Portfolio

	Less than 20%	21-40%	41-60%	61-80%	More than 80%
Global	27%	23%	16%	7%	11%
North America	30%	21%	16%	5%	14%
Europe	24%	25%	17%	8%	8%

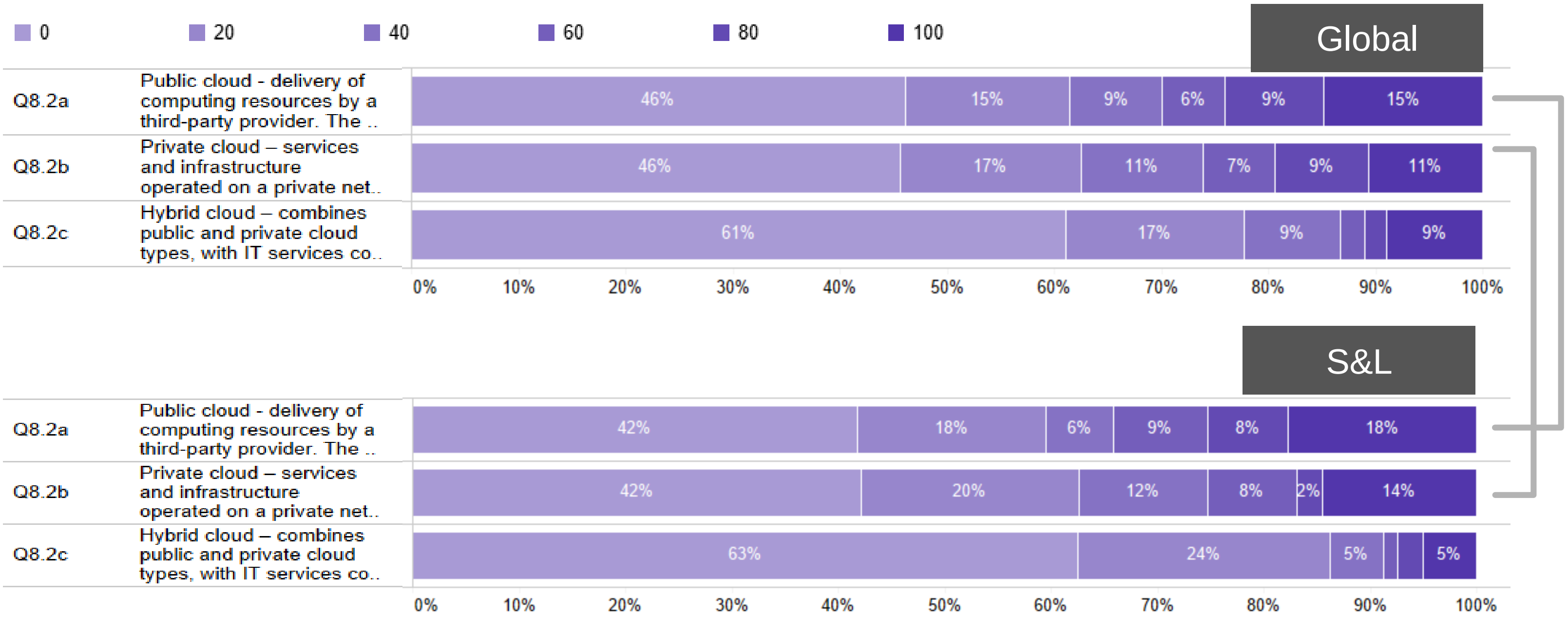
Plan to **Migrate Applications** to the Cloud

	Less than 20%	21-40%	41-60%	61-80%	More than 80%
Global	31%	15%	19%	11%	11%
North America	30%	16%	19%	8%	14%
Europe	32%	14%	19%	14%	8%

Globally **57%** of respondents are planning to modernize at least 21% of their organization’s applications portfolio in the next two years and **56%** are planning to migrate at least 21% of their applications to the cloud

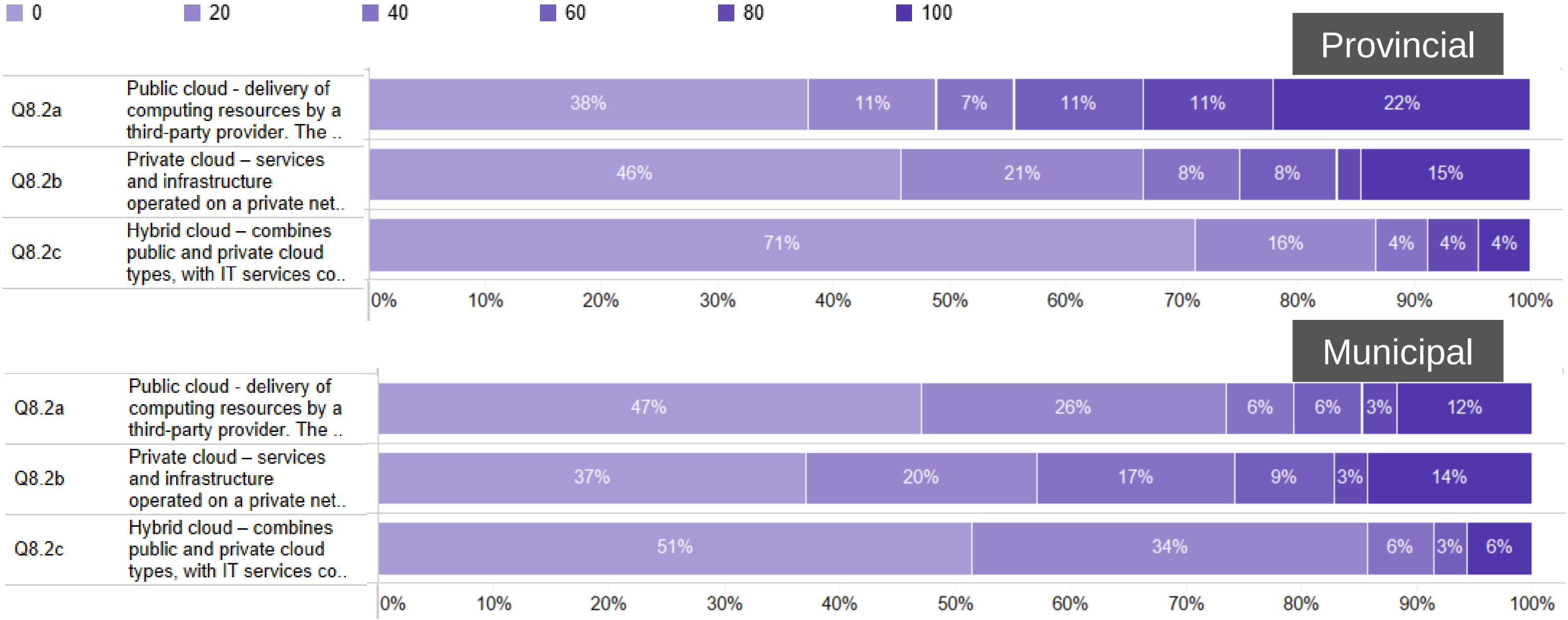
State and Local government clients are more confident to achieve applications migration to public and hybrid cloud in the next 2 years, than global clients overall

For those applications you migrate to the cloud over the next 2 years, what percentage do you expect will be in Public, Private, or Hybrid cloud?



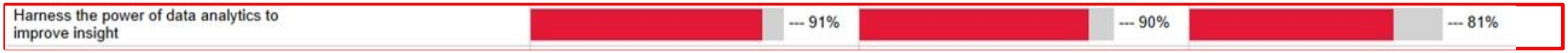
State government clients are more confident to achieve applications migration to public cloud in the next 2 years, with municipal government expectations higher for hybrid

For those applications you migrate to the cloud over the next 2 years, what percentage do you expect will be in Public, Private, or Hybrid cloud?

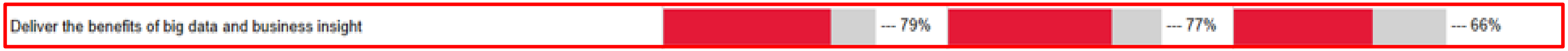


Data analytics increases in prominence 2019-2021 for both business and IT priorities as well as investment in innovation for next 3 years

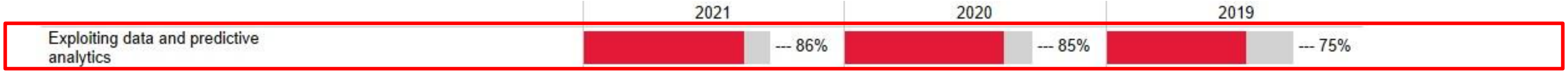
Q2.1a/b: Which priorities continue to be your organization's top business priorities for this year? Does your organization have new business priorities this year?



Q3.1a: Top IT priorities identified, importance ranking, and implementation stage

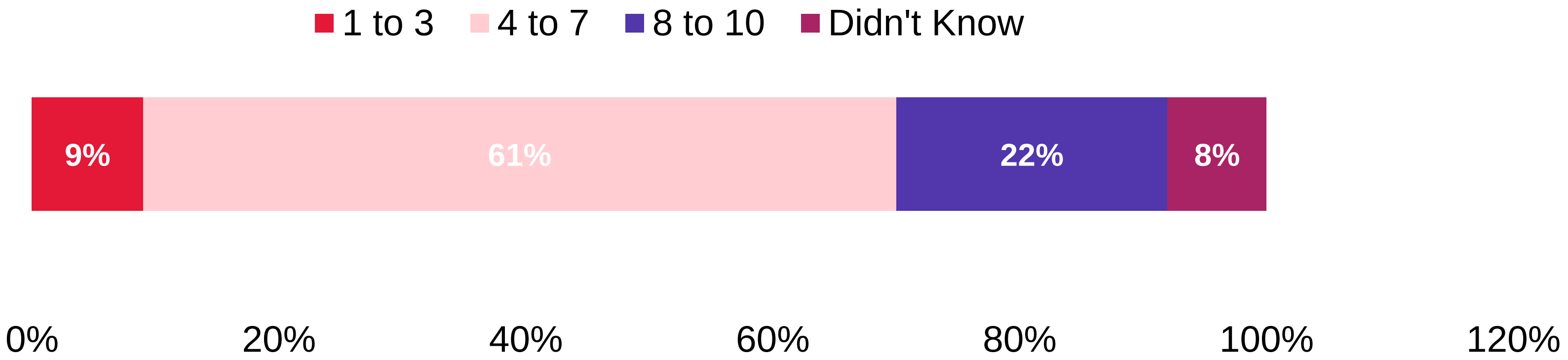


Q5.1a: Looking ahead to the next 3 years, in which areas does your organization plan to invest in innovation?



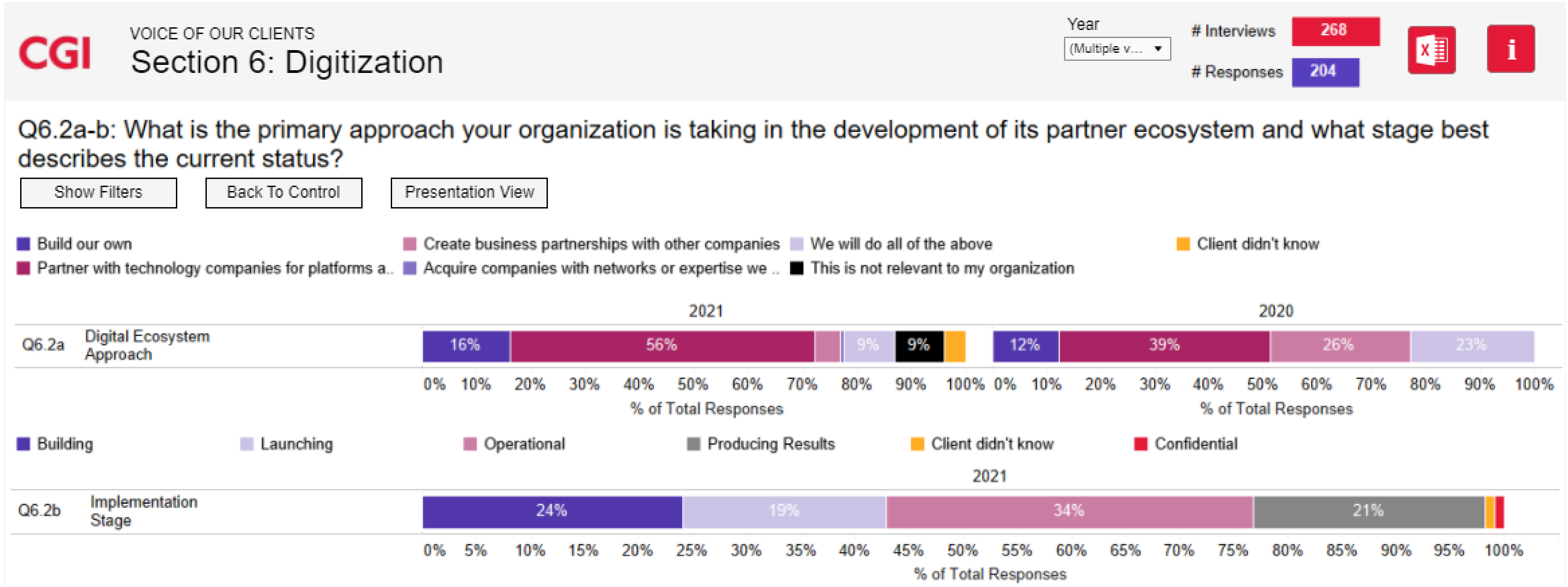
IT Supply Chain: Due to complex and lengthy procurement processes in Europe and North America, 70% percent of government organizations lack agility in technology supply chain

Q3.3: How would you rate the agility of your organization's technology supply chain?



In 2021, **22%** of respondents rated the agility of their organization's technology supply chain as very high (ratings of 8-9-10)

Pandemic has pushed the development of partner ecosystem through collaboration with technology companies (56% in 2021 vs. 39% in 2020) as results were seen by 21% of clients in 2021 vs. 0% in 2020



CGI

VOICE OF OUR CLIENTS

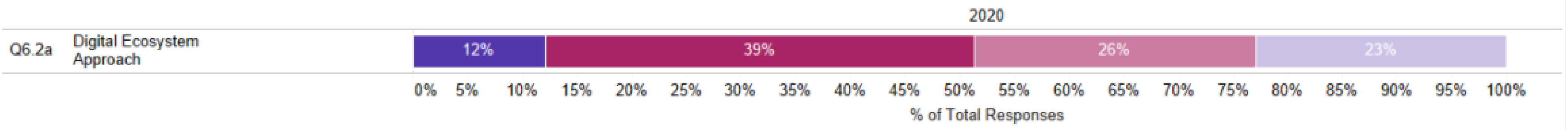
Section 6: Digitization

Year: (Multiple v...

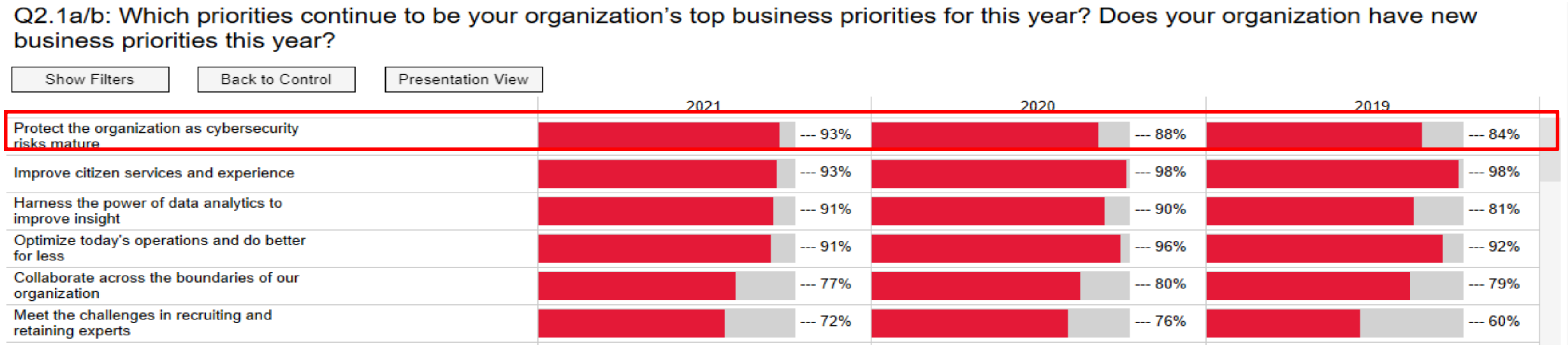
Interviews 268

Responses 204

Q6.2a-b: What is the primary approach your organization is taking in the development of its partner ecosystem and what stage best describes the current status?

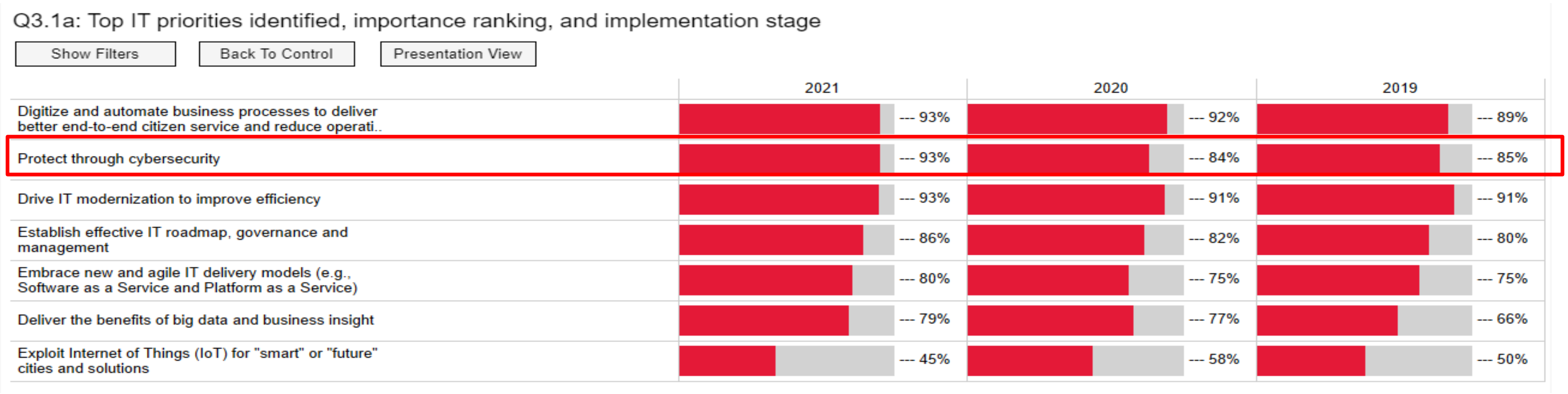


Cybersecurity continues growth in importance when it comes to both business and IT priorities



Q2.1a/b: Which priorities continue to be your organization’s top business priorities for this year? Does your organization have new business priorities this year?

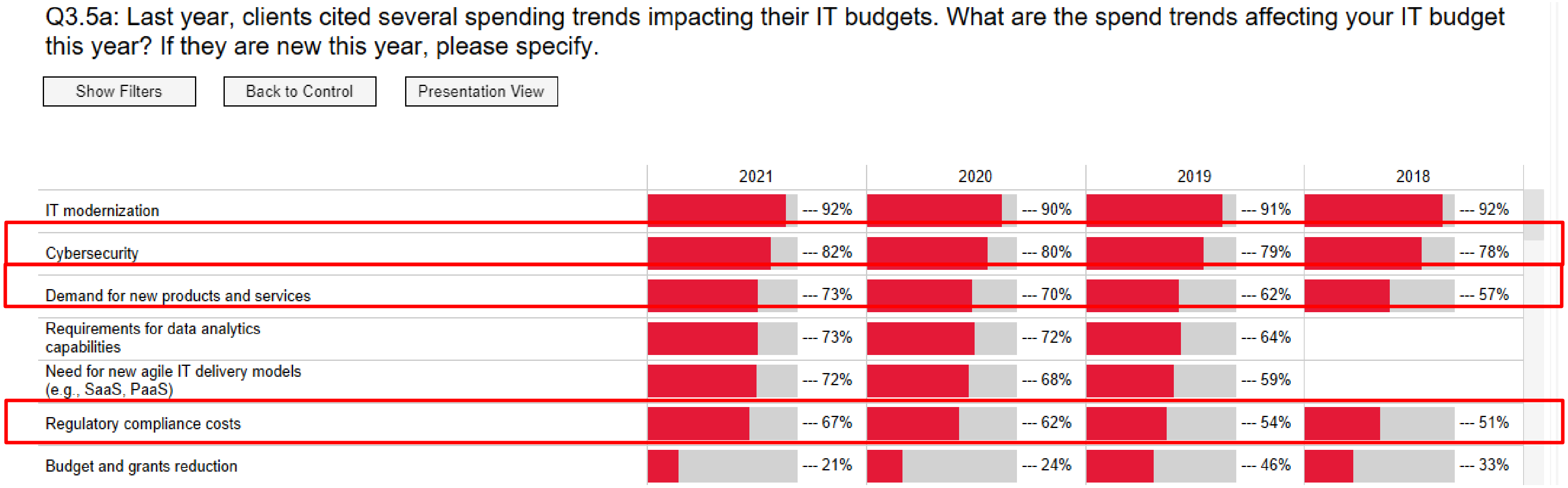
	2021	2020	2019
Protect the organization as cybersecurity risks mature	--- 93%	--- 88%	--- 84%
Improve citizen services and experience	--- 93%	--- 98%	--- 98%
Harness the power of data analytics to improve insight	--- 91%	--- 90%	--- 81%
Optimize today's operations and do better for less	--- 91%	--- 96%	--- 92%
Collaborate across the boundaries of our organization	--- 77%	--- 80%	--- 79%
Meet the challenges in recruiting and retaining experts	--- 72%	--- 76%	--- 60%



Q3.1a: Top IT priorities identified, importance ranking, and implementation stage

	2021	2020	2019
Digitize and automate business processes to deliver better end-to-end citizen service and reduce operati..	--- 93%	--- 92%	--- 89%
Protect through cybersecurity	--- 93%	--- 84%	--- 85%
Drive IT modernization to improve efficiency	--- 93%	--- 91%	--- 91%
Establish effective IT roadmap, governance and management	--- 86%	--- 82%	--- 80%
Embrace new and agile IT delivery models (e.g., Software as a Service and Platform as a Service)	--- 80%	--- 75%	--- 75%
Deliver the benefits of big data and business insight	--- 79%	--- 77%	--- 66%
Exploit Internet of Things (IoT) for "smart" or "future" cities and solutions	--- 45%	--- 58%	--- 50%

Cybersecurity remains high, with demand for new products and services, and regulatory compliance cost are increasingly, impacting the IT budgets of State & Local clients

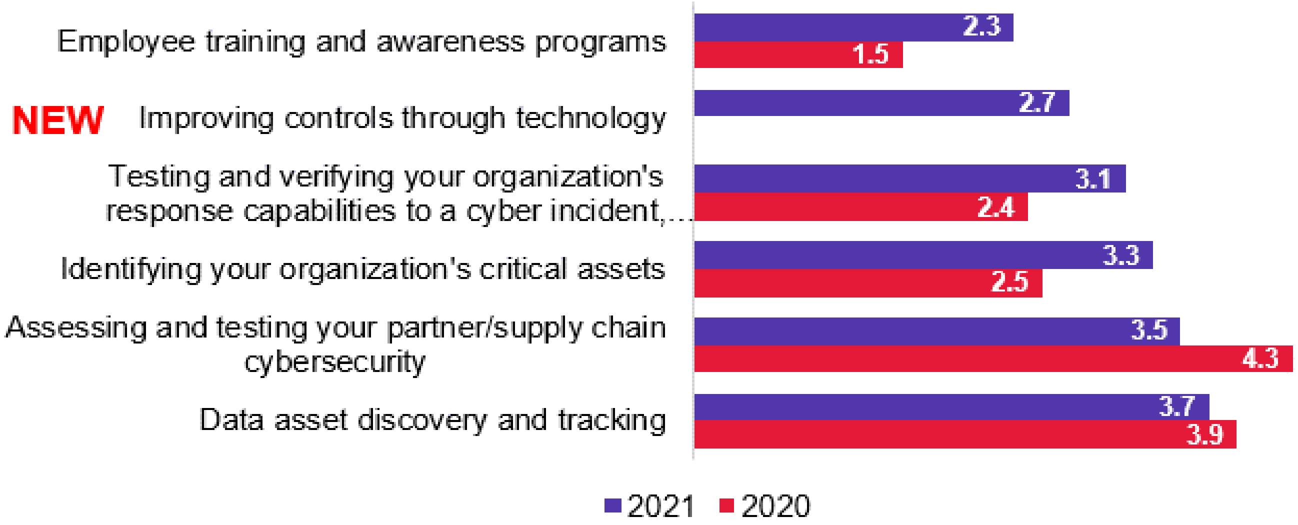


Q3.5a: Last year, clients cited several spending trends impacting their IT budgets. What are the spend trends affecting your IT budget this year? If they are new this year, please specify.

	2021	2020	2019	2018
IT modernization	--- 92%	--- 90%	--- 91%	--- 92%
Cybersecurity	--- 82%	--- 80%	--- 79%	--- 78%
Demand for new products and services	--- 73%	--- 70%	--- 62%	--- 57%
Requirements for data analytics capabilities	--- 73%	--- 72%	--- 64%	
Need for new agile IT delivery models (e.g., SaaS, PaaS)	--- 72%	--- 68%	--- 59%	
Regulatory compliance costs	--- 67%	--- 62%	--- 54%	--- 51%
Budget and grants reduction	--- 21%	--- 24%	--- 46%	--- 33%

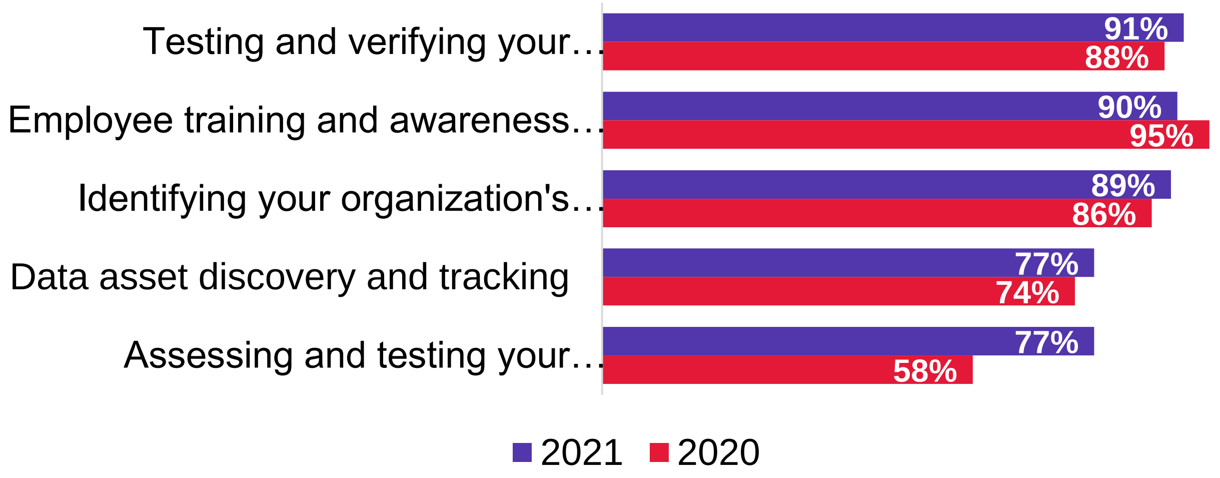
Cybersecurity: highly ranked in both Business and IT Priorities, this year employee training stays as the top ranked cybersecurity element, with improving controls through technology a new addition in 2nd place

How would you rank the importance of these cybersecurity elements to your organization?



Cybersecurity: As security programs mature, while improving controls remains important, **testing grows and training remains high in importance for security assurance and protection**

How would you rank the importance of these cybersecurity elements to your organization?



91% of respondents believe testing and verifying organization’s response capabilities are the core to a successful cybersecurity strategy

CYBEREDGE GROUP

2021 Cyberthreat Defense Report

North America | Europe | Asia Pacific
Latin America | Middle East | Africa

Top Five Insights for 2021 – Cyber Edge Group
Cyberthreat Defense Report | (ISC)² (isc2.org)

Top Five Insights	Summary / Observations
1. Successful Cyber Attacks Make the Biggest Jump in Six Years	*Driven by pandemic conditions, remote work, BYOD, smart phones and Ransomware spikes* *From 62% in 2014 to 86% in 2021.*
2. Rewarding Ransomware payer is good for business (if you are a cyber criminal)	*Criminals reward payers with data 72% of the time resulting increased motivation and funding for more Ransomware. Two-thirds of organizations face Rw.*
3. Adoption of cloud security solutions is rising	*Pandemic conditions sent security professionals looking for easily managed cloud based security tools.*
4. IT security spending increases are slowing	*Similar to CGI findings competing investments in digital, regulatory compliance, new products impact security spend. Budgets down about 5%.*
5. Pessimism is the new normal	*86% surveyed admitted to a cyber breach.* *"There is a shift of focus to detect, terminate and remediate from in-progress attacks."*

Road Ahead– Cyber Edge Group

Cyberthreat Defense Report | (ISC)² (isc2.org)

Road Ahead	Summary / Observations
Security automation, orchestration, and response (SOAR) Integrate, aggregate and accelerate incident response	*Leverage highly automated cloud platforms to integrate security solutions.*
DevSecOps Building security into development lifecycle	*Continuous and systematic testing od development code for vulnerabilities or non-compliance with security policy and standards.*
Browser isolation technology Reduce browser risks on devices	*Technology is improving so larger enterprises are beginning to adopt.*
Continuous security validation Ongoing validation of controls in production	*Launch simulated attacks in production environments to test security controls*
Threat intelligence platforms (TIPs) and services Identify clues about ongoing attacks	*Improvements are being seen by aggregating public threat data to launch searches for threats. 43% planning on acquiring TIPs, biggest focus*

Aaron.Mathes@cgi.com
Mobile (434) 841-5215

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com

Security & Compliance with the Content Cloud

Alok Ojha
VP, Products

Lori LaGuardia
Solutions Engineer

Content is your business

EMPLOYEES

CUSTOMERS

PARTNERS

Everything at work has changed

Distributed teams

Work happens anywhere, anytime, from any app or device

Digital-first

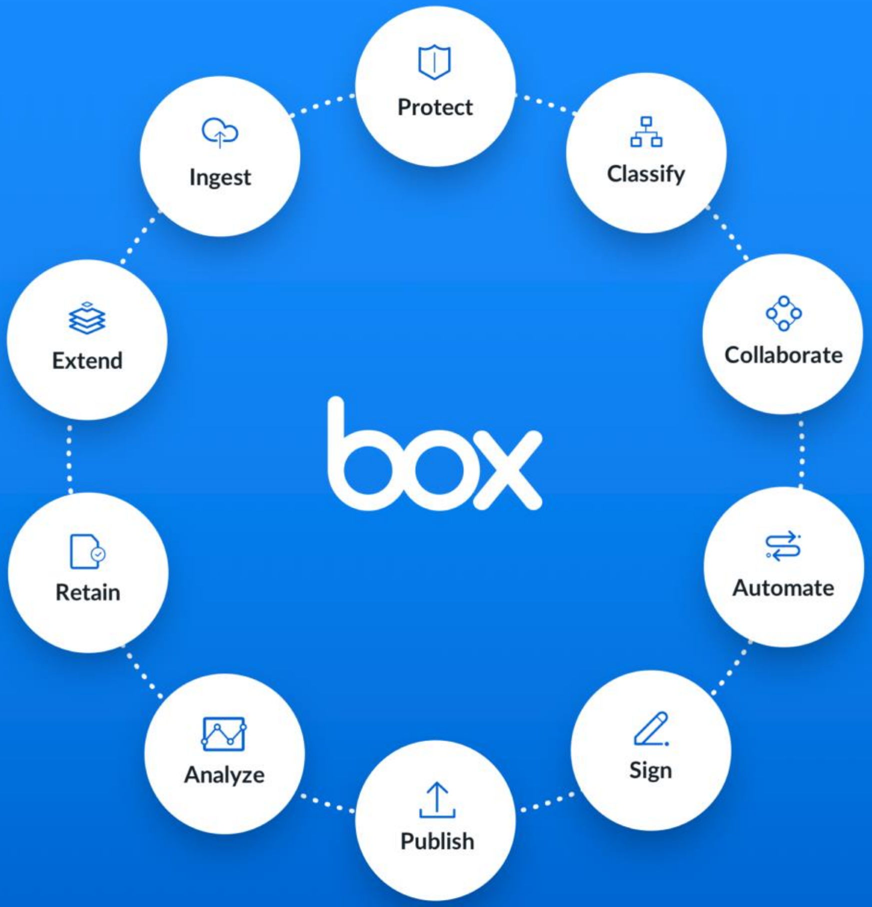
The world is shifting from paper to digital, and from digital to automated

Security and privacy

Data security, privacy, and compliance are critical to collaboration

Welcome to the Content Cloud

One secure platform to manage the entire content journey



Powering content workflows across the enterprise

Finance

Financial operations, audits, and virtual deal rooms

Sales

Sales enablement, client collaboration and onboarding

R&D

Product design and development and supply chain collaboration

Legal

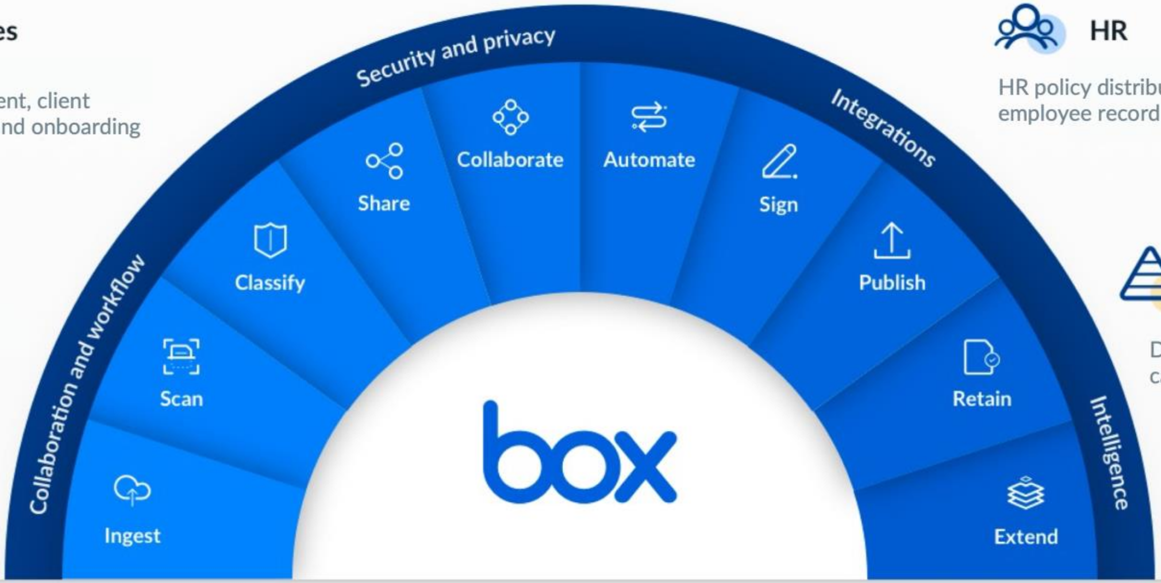
Contract review and approval, and lifecycle management

HR

HR policy distribution and employee record management

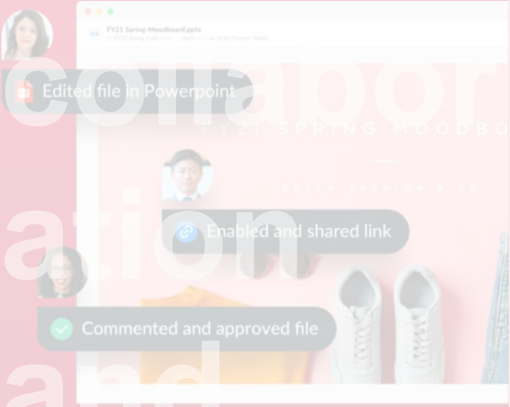
Marketing

Digital asset management and campaign collaboration



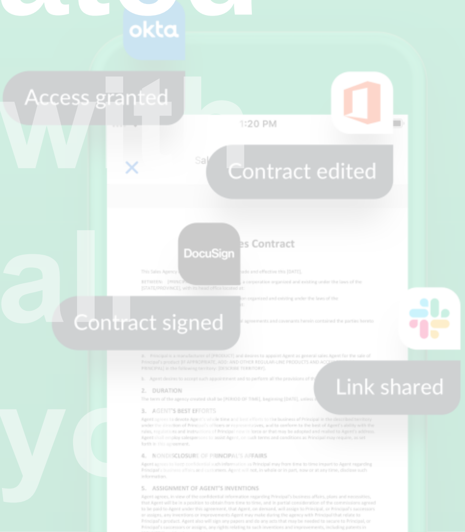
Frictionless security and compliance

Seamless collaboration and workflow



FY21 Spring-Moodboard.pptx
Edited file in Powerpoint
Enabled and shared link
Commented and approved file

Integrated with all your applications



Key challenges our customers are facing

Secure collaboration

Data leak prevention and threat detection

Compliance with industry regulations

Continuous visibility and ease of management

How we solve them

Zero-trust architecture

Core Security

- Secure Sharing
- User Authentication
- Device Trust
- Application Controls

Leak prevention and threat detection

Box Shield

- Auto-Classification
- Smart Controls
- Anomaly Detection
- Malware Detection

Compliance and content lifecycle management

Compliance Products

- Box Governance
- Box Zones
- Box GxP
- Box KeySafe

Enterprise Administration

Continuous visibility

Industry certifications

WEBCOR

Medtronic

USAA

box

SHIELD

Your content holds the keys to your business

Banking

- Client data
- Financial records

Life Sciences

- Drug formulas
- Clinical trial data

Media and Entertainment

- Unreleased albums
- Movie scripts

Professional Services

- Customer data
- Contracts

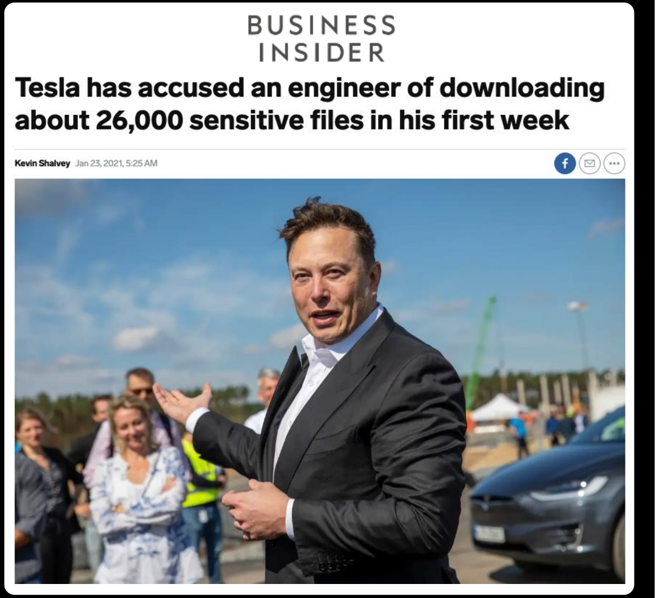
Retail

- New product launch
- Retail site details

Technology

- M&A documents
- Technical designs

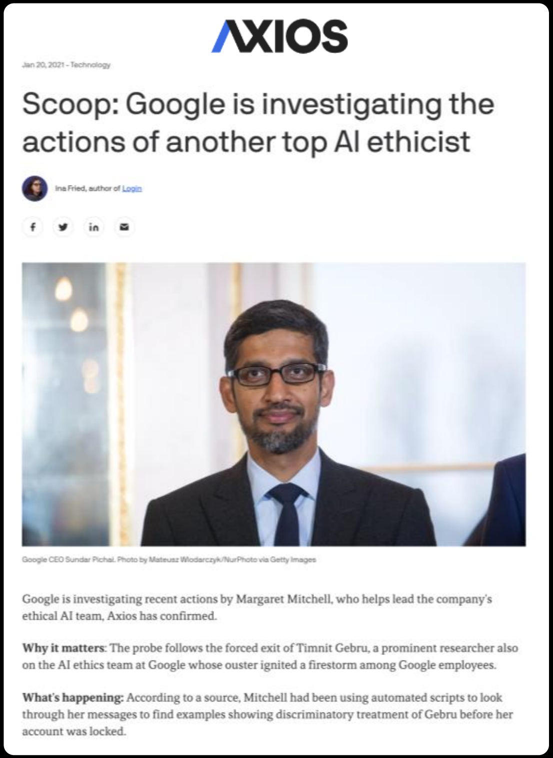
Data breaches and malware breakouts are on a rise



BUSINESS INSIDER

Tesla has accused an engineer of downloading about 26,000 sensitive files in his first week

Kevin Shalvey Jan 23, 2021, 5:25 AM



AXIOS

Jan 20, 2021 - Technology

Scoop: Google is investigating the actions of another top AI ethicist

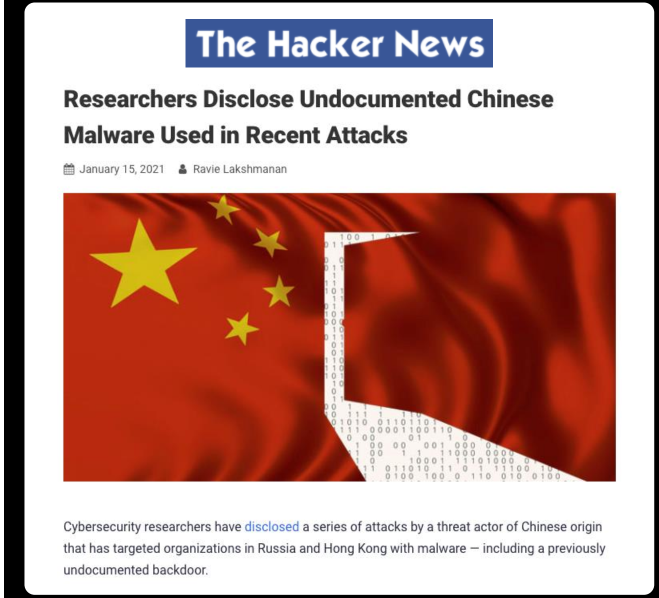
Ina Fried, author of Login

Google CEO Sundar Pichai. Photo by Mateusz Wlodarczyk/NurPhoto via Getty Images

Google is investigating recent actions by Margaret Mitchell, who helps lead the company's ethical AI team, Axios has confirmed.

Why it matters: The probe follows the forced exit of Timnit Gebru, a prominent researcher also on the AI ethics team at Google whose ouster ignited a firestorm among Google employees.

What's happening: According to a source, Mitchell had been using automated scripts to look through her messages to find examples showing discriminatory treatment of Gebru before her account was locked.



The Hacker News

Researchers Disclose Undocumented Chinese Malware Used in Recent Attacks

January 15, 2021 Ravie Lakshmanan

Cybersecurity researchers have disclosed a series of attacks by a threat actor of Chinese origin that has targeted organizations in Russia and Hong Kong with malware — including a previously undocumented backdoor.

SolarWinds Compromise

December 13th 2020

KrebsonSecurity

In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

SolarWinds Hack Could Affect 18K Customers

December 15, 2020 122 Comments

The still-unfolding breach at network management software firm **SolarWinds** may have resulted in malicious code being pushed to nearly 18,000 customers, the company said in a legal filing on Monday. Meanwhile, **Microsoft** should soon have some idea which and how many SolarWinds customers were affected, as it recently took possession of a key domain name used by the intruders to control infected systems.

On Dec. 13, SolarWinds acknowledged that hackers had inserted malware into a service that provided software updates for its **Orion** platform, a suite of products broadly used across the U.S. federal government and Fortune 500 firms to monitor the health of their IT networks.

solarwinds
CrowdSec
The open-source & free massively multiplayer firewall: Respond to attacks & share signals across thecommunity.
Learn more
Akamai

Colonial Pipeline Attack

May 7th 2021

THE WALL STREET JOURNAL.

TO THE MOON PODCAST

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

Biden's Executive Order

May 12th 2021

THE WHITE HOUSE

Administration Priorities COVID-19 Briefing Room Español MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

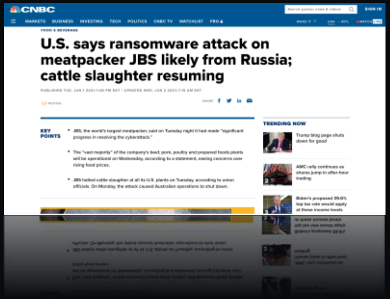
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more

Meatpacker JBS Cyberattack

June 1st 2021



CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST PRO

SIGN IN

FOOD & BEVERAGE

U.S. says ransomware attack on meatpacker JBS likely from Russia; cattle slaughter resuming

PUBLISHED TUE, JUN 1 2021 [illegible] PM EDT | UPDATED WED, JUN 2 2021 [illegible] AM EDT

REUTERS

KEY POINTS

- JBS, the world's largest meatpacker, said on Tuesday night it had made "significant progress in resolving the cyberattack."
- The "vast majority" of the company's beef, pork, poultry and prepared foods plants will be operational on Wednesday, according to a statement, easing concerns over rising food prices.
- JBS halted cattle slaughter at all its U.S. plants on Tuesday, according to union officials. On Monday, the attack caused Australian operations to shut down.

TRENDING NOW

1 Trump blog page shuts down for good

2 AMC rally continues as shares jump in after-hour trading

3 Biden's proposed 39.6% top tax rate would apply at these income levels

The average cost of a malware attack on a company is $2.6 million.

SOURCE: Accenture

IT needs to minimize these data leakage risks

Accidental leakage

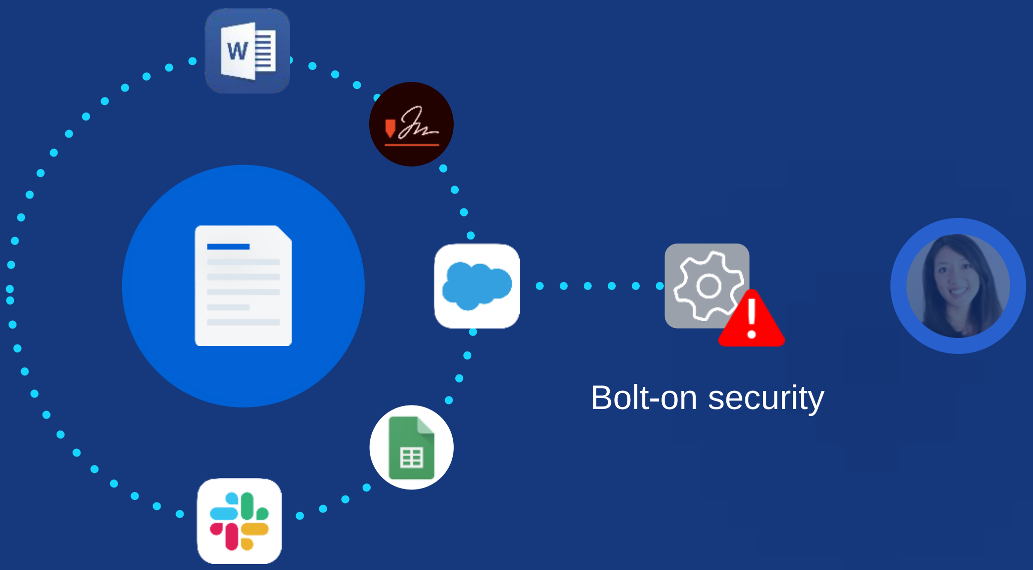
Public shared links
Accidental collaboration invites
Use of unmanaged devices

Content-centric threats

Anomalous downloads
Suspicious user sessions
Malware and ransomware

Customers are dissatisfied with existing solutions

Traditional content security solutions impede user productivity



Frictionless security is

Built-in

Precise controls that
don’t inhibit work

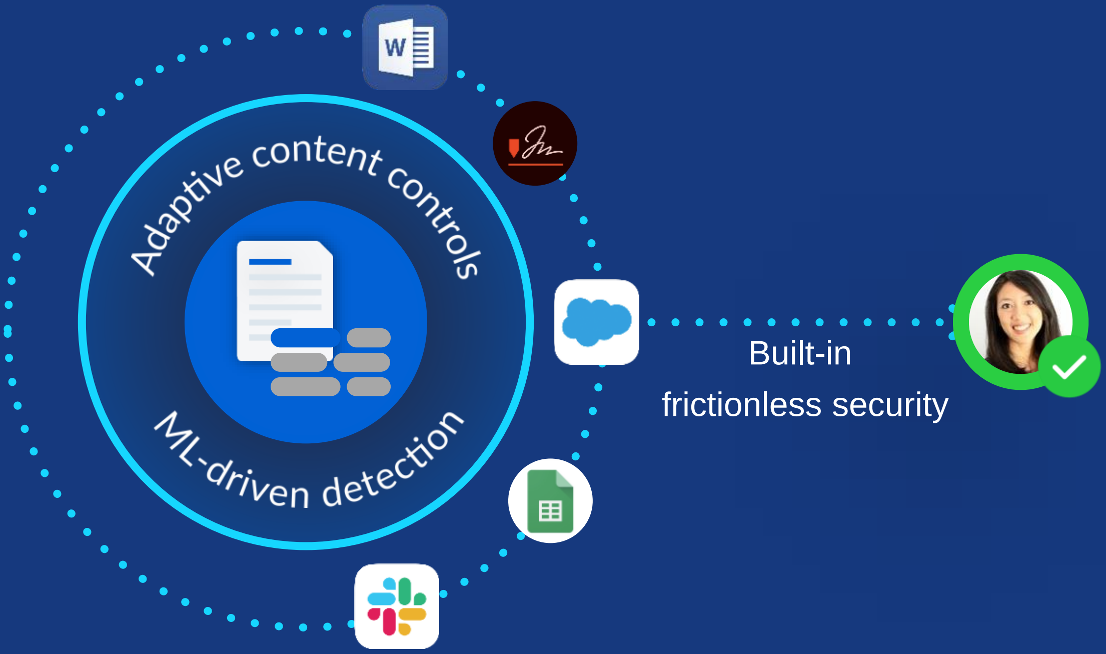
Transparent

Remain compliant
without adding friction

Empowering

Enable employees
to safeguard data

Reimagine security with the Content Cloud



Box Graph (ML/AI)

Scalable Metadata

Unified Content Store

Best-of-breed Integrations

Content-centric risks to solve

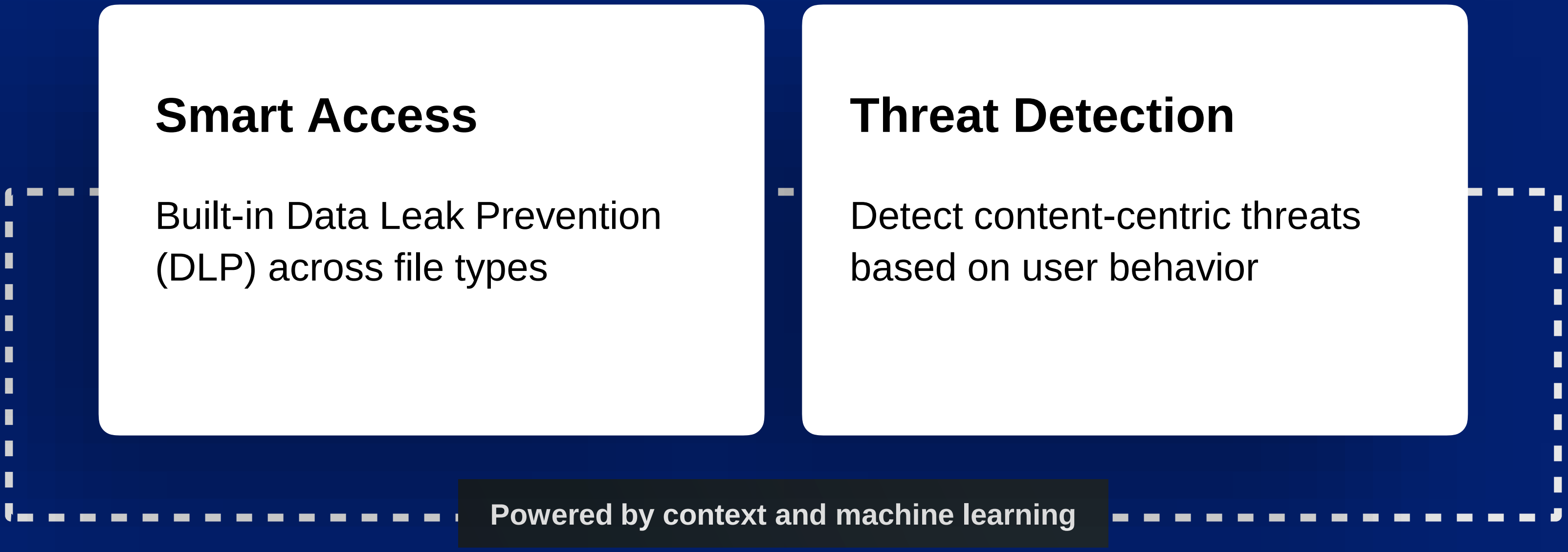
Accidental leakage

Public shared links
Accidental collaboration invites
Use of unmanaged devices

Content-centric threats

Anomalous downloads
Suspicious user sessions
Malware and ransomware

box SHIELD



Smart Access

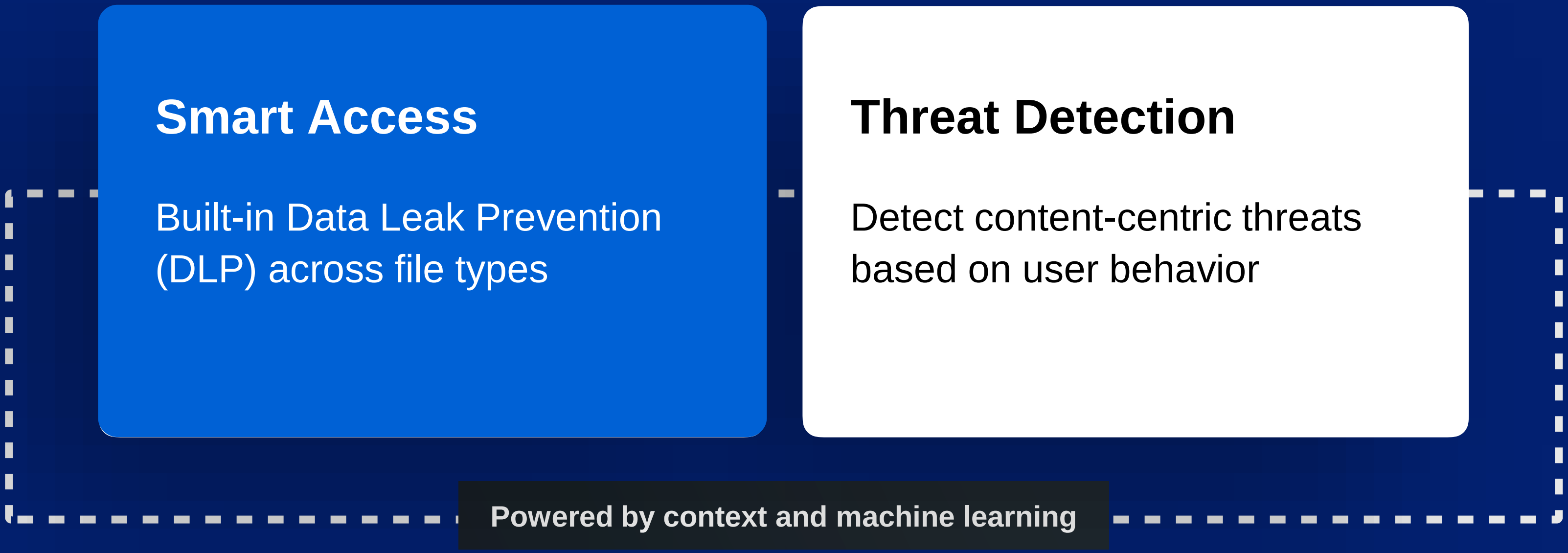
Built-in Data Leak Prevention (DLP) across file types

Threat Detection

Detect content-centric threats based on user behavior

Powered by context and machine learning

box SHIELD



Smart Access

Built-in Data Leak Prevention (DLP) across file types

Threat Detection

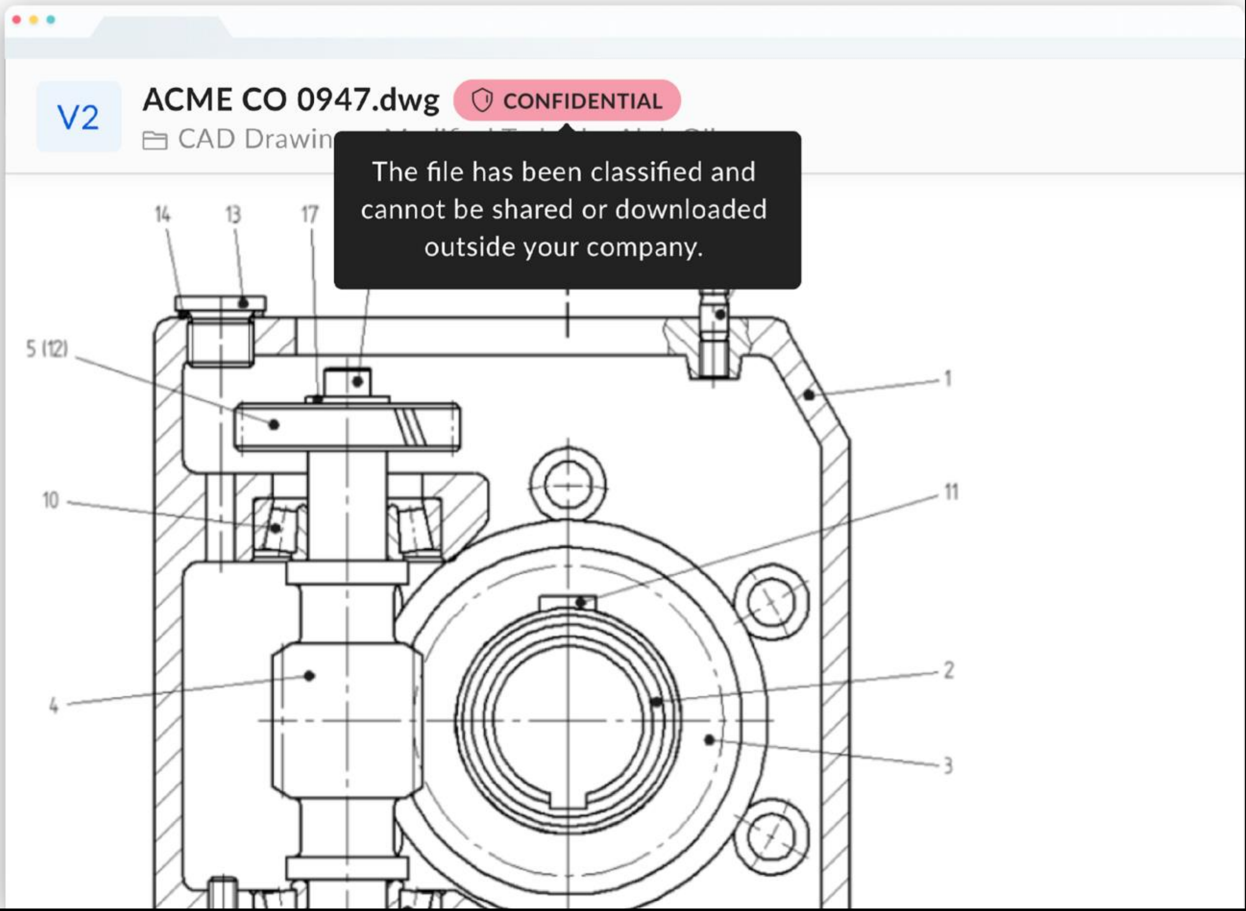
Detect content-centric threats based on user behavior

Powered by context and machine learning

Shield: Smart Access

Prevent data leaks with frictionless content controls

- Create and manage custom classification labels
- Classify content manually or automatically
- Enforce classification-based security policies



V2

ACME CO 0947.dwg

CONFIDENTIAL

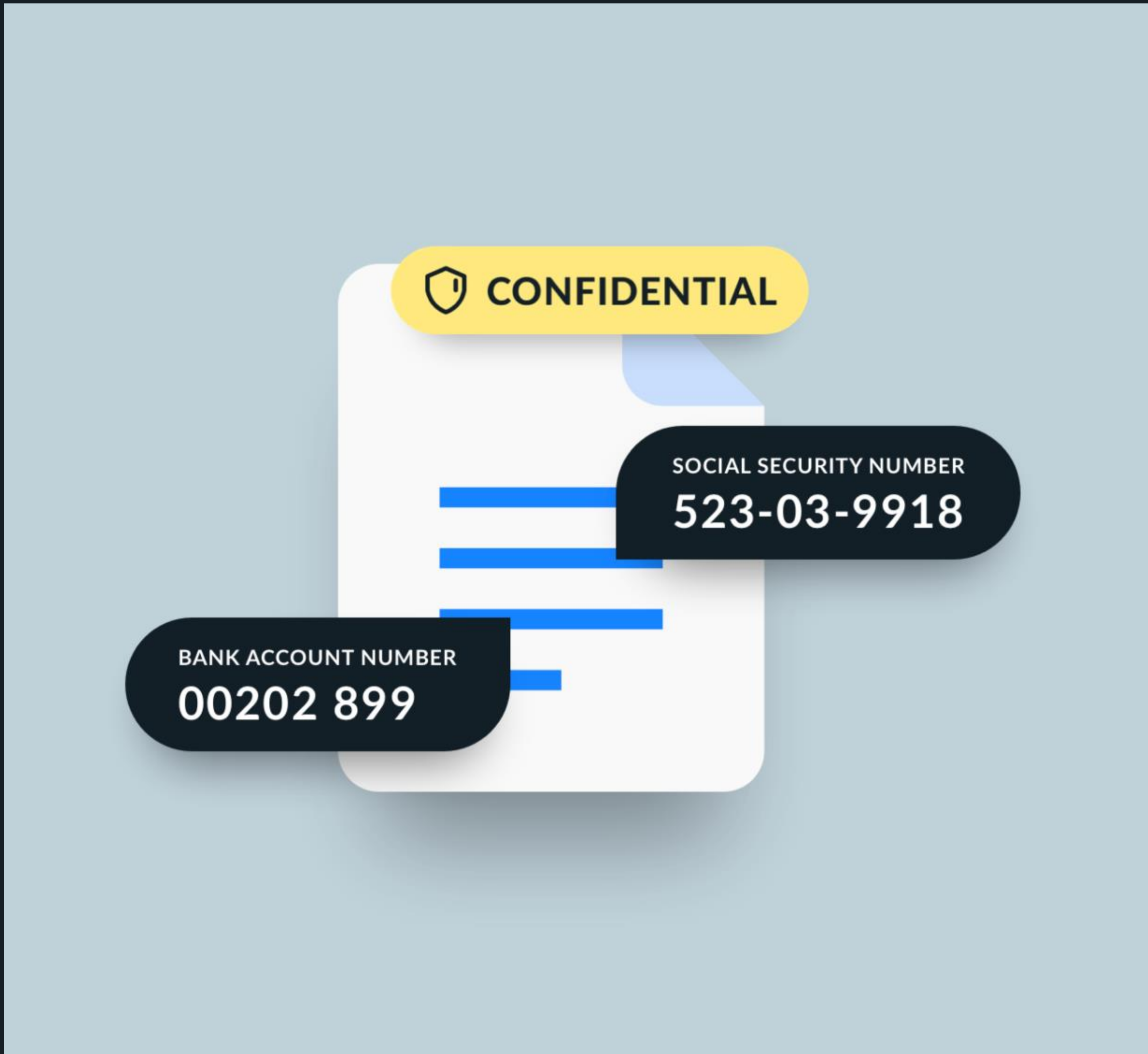
CAD Drawin

The file has been classified and cannot be shared or downloaded outside your company.

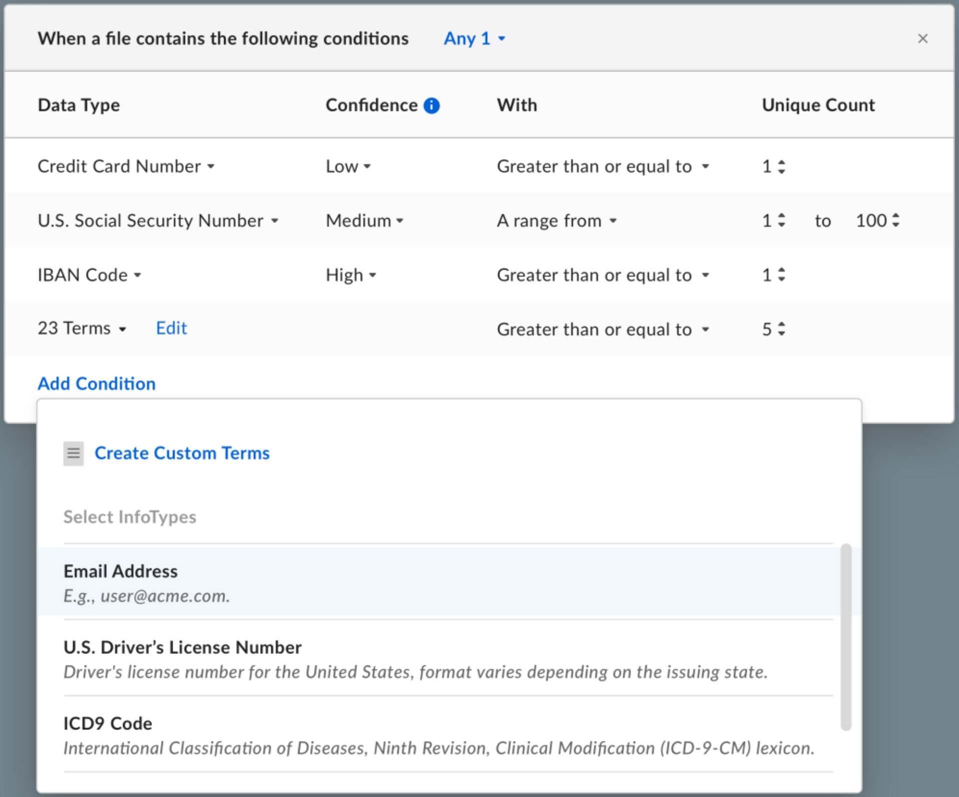
Automated Classification

Automatically classify files based on what's inside files

- Define classification policy
- Detect PII
- Detect custom-terms
- Classify by file type



Define flexible classification policies to detect sensitive data



When a file contains the following conditions Any 1 ▾ ×

Data Type	Confidence ⓘ	With	Unique Count
Credit Card Number ▾	Low ▾	Greater than or equal to ▾	1 ⬍
U.S. Social Security Number ▾	Medium ▾	A range from ▾	1 ⬍ to 100 ⬍
IBAN Code ▾	High ▾	Greater than or equal to ▾	1 ⬍
23 Terms ▾ Edit		Greater than or equal to ▾	5 ⬍

Add Condition

Create Custom Terms

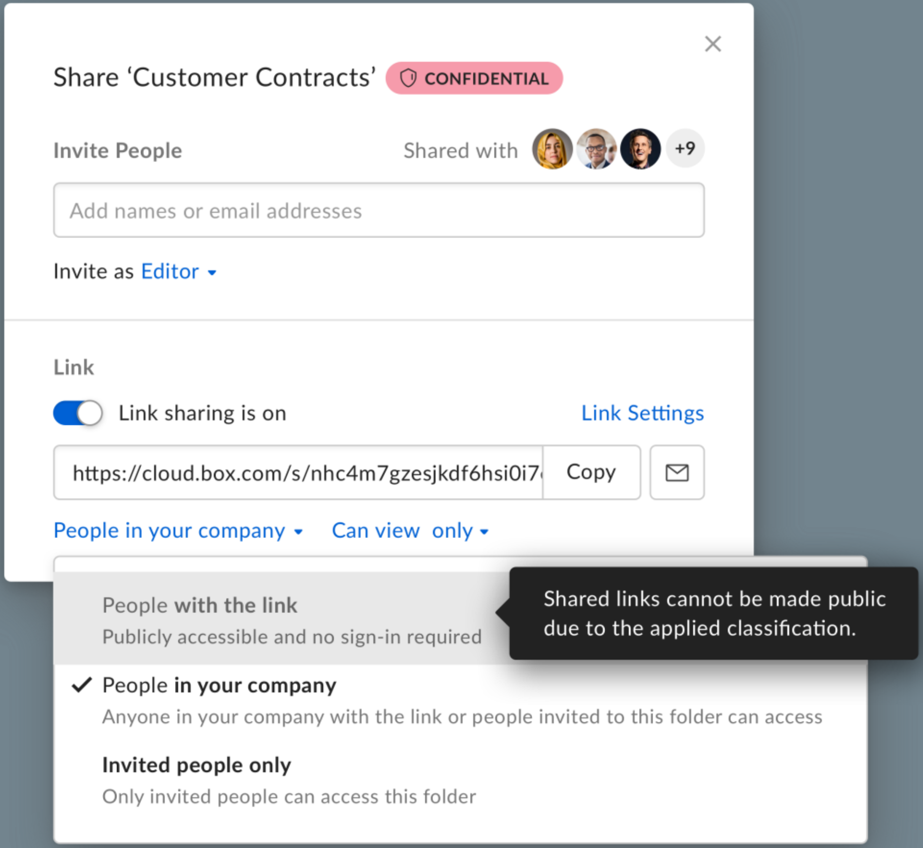
Select InfoTypes

Email Address
E.g., user@acme.com.

U.S. Driver's License Number
Driver's license number for the United States, format varies depending on the issuing state.

ICD9 Code
International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) lexicon.

Shield then prevents data leaks in real time



Share 'Customer Contracts' CONFIDENTIAL

Invite as Editor ▾

Link

Link sharing is on

https://cloud.box.com/s/nhc4m7gzesjkdf6hsi0i7

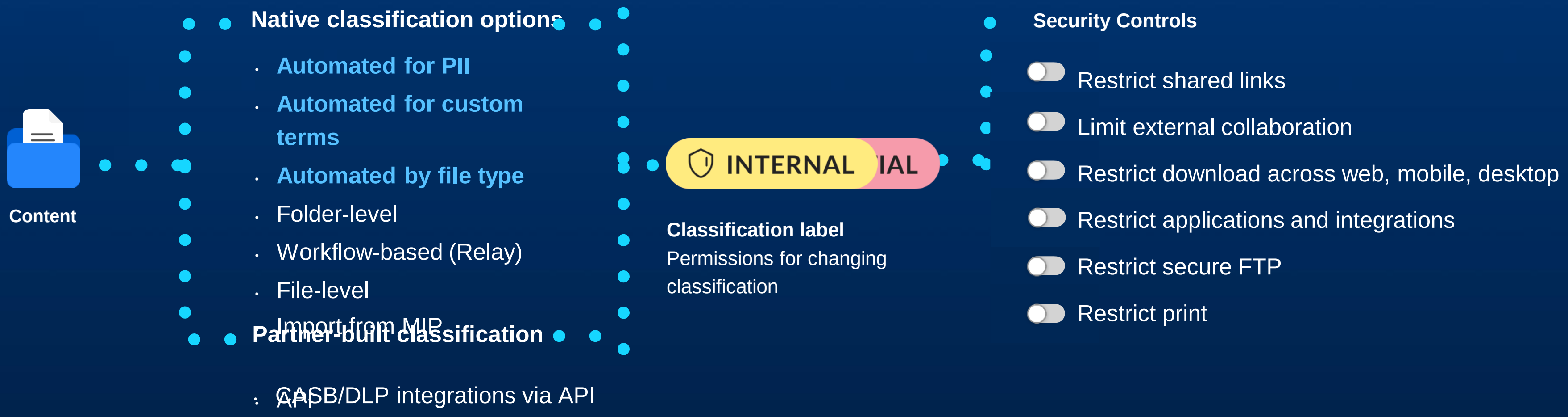
People in your company ▾ Can view only ▾

People with the link
Publicly accessible and no sign-in required

Shared links cannot be made public due to the applied classification.

✓ People in your company
Anyone in your company with the link or people invited to this folder can access

Invited people only
Only invited people can access this folder



Content

Native classification options

- Automated for PII
- Automated for custom terms
- Automated by file type
- Folder-level
- Workflow-based (Relay)
- File-level
- Import from MIP

Partner-built classification

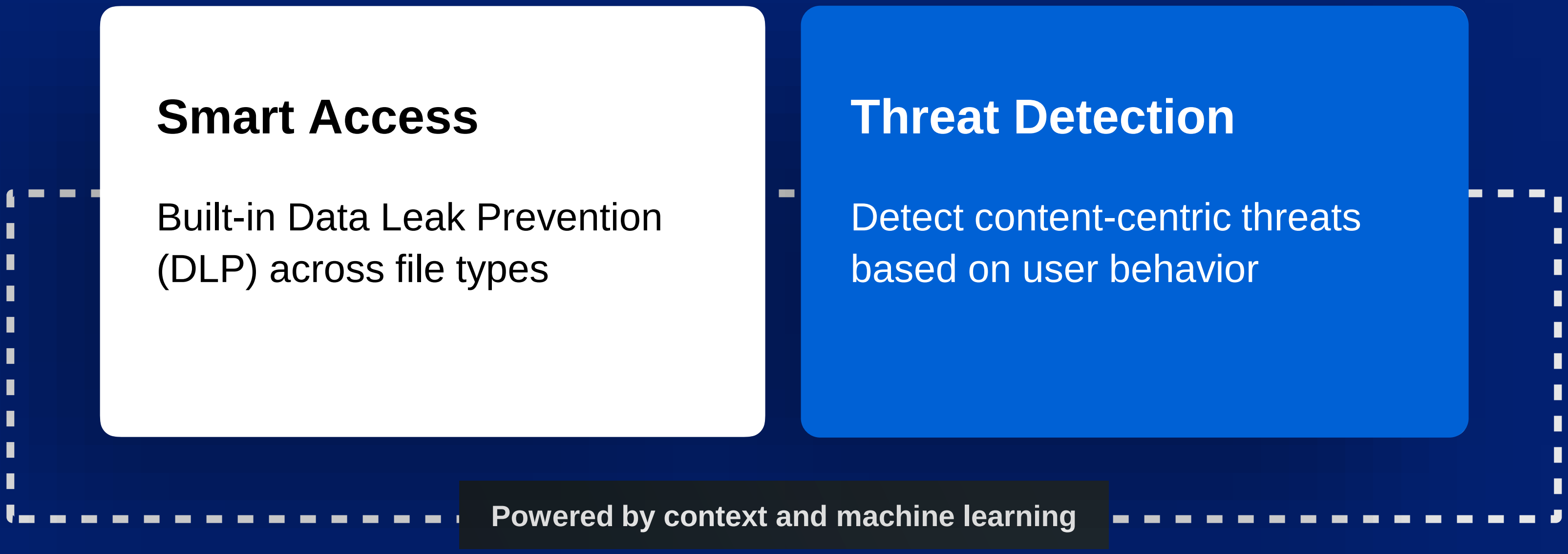
- CASB/DLP integrations via API
- API

Classification label
Permissions for changing classification

Security Controls

- Restrict shared links
- Limit external collaboration
- Restrict download across web, mobile, desktop
- Restrict applications and integrations
- Restrict secure FTP
- Restrict print

box SHIELD



Smart Access

Built-in Data Leak Prevention (DLP) across file types

Threat Detection

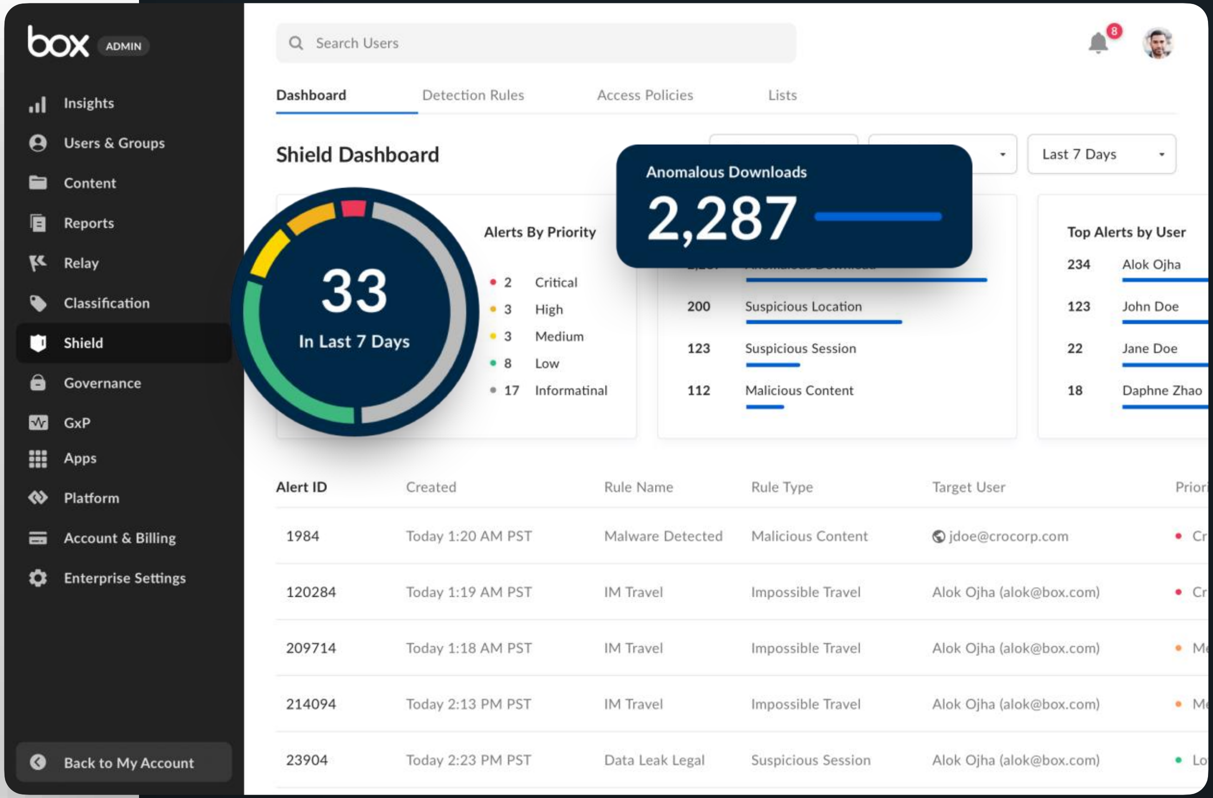
Detect content-centric threats based on user behavior

Powered by context and machine learning

Anomaly detection

Detect risky behaviors and alert security teams

- Flag anomalous download behaviors
- Identify content access via suspicious sessions
- Discover content access from risky locations



Shield Dashboard

33
In Last 7 Days

Anomalous Downloads
2,287

Alerts By Priority

● 2	Critical
● 3	High
● 3	Medium
● 8	Low
● 17	Informational

200	Suspicious Location
123	Suspicious Session
112	Malicious Content

Top Alerts by User

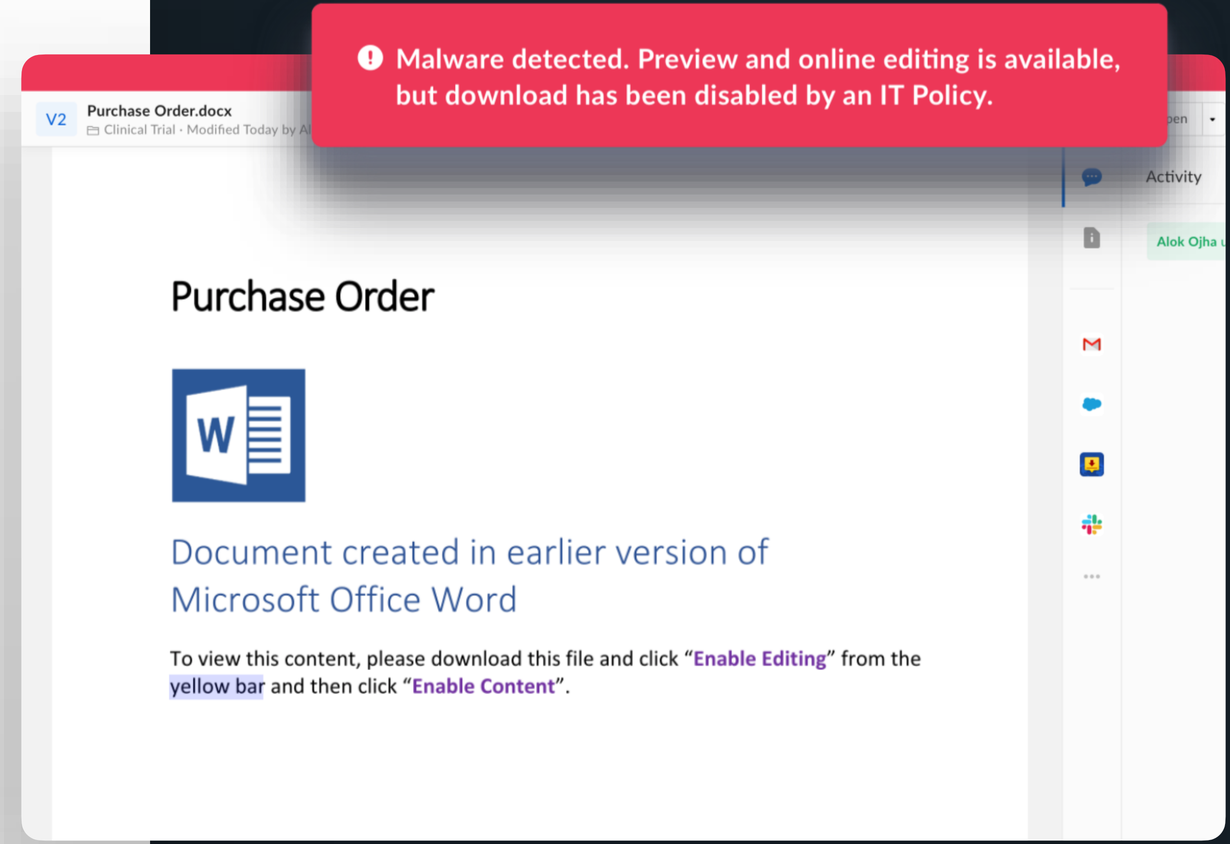
234	Alok Ojha
123	John Doe
22	Jane Doe
18	Daphne Zhao

Alert ID	Created	Rule Name	Rule Type	Target User	Prior
1984	Today 1:20 AM PST	Malware Detected	Malicious Content	jdoe@crocorp.com	● Cr
120284	Today 1:19 AM PST	IM Travel	Impossible Travel	Alok Ojha (alok@box.com)	● Cr
209714	Today 1:18 AM PST	IM Travel	Impossible Travel	Alok Ojha (alok@box.com)	● Me
214094	Today 2:13 PM PST	IM Travel	Impossible Travel	Alok Ojha (alok@box.com)	● Me
23904	Today 2:23 PM PST	Data Leak Legal	Suspicious Session	Alok Ojha (alok@box.com)	● Lo

Malware detection

Detect and prevent spread of malicious content

- Alert security teams
- Restrict download and sync
- Allow end-users to preview and online edit

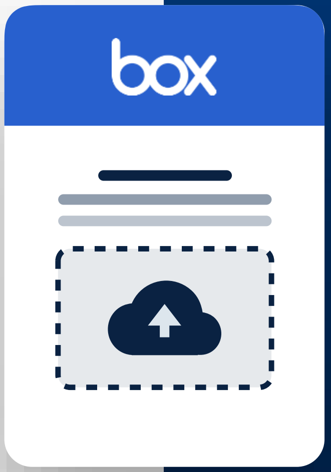


Malware detected. Preview and online editing is available, but download has been disabled by an IT Policy.

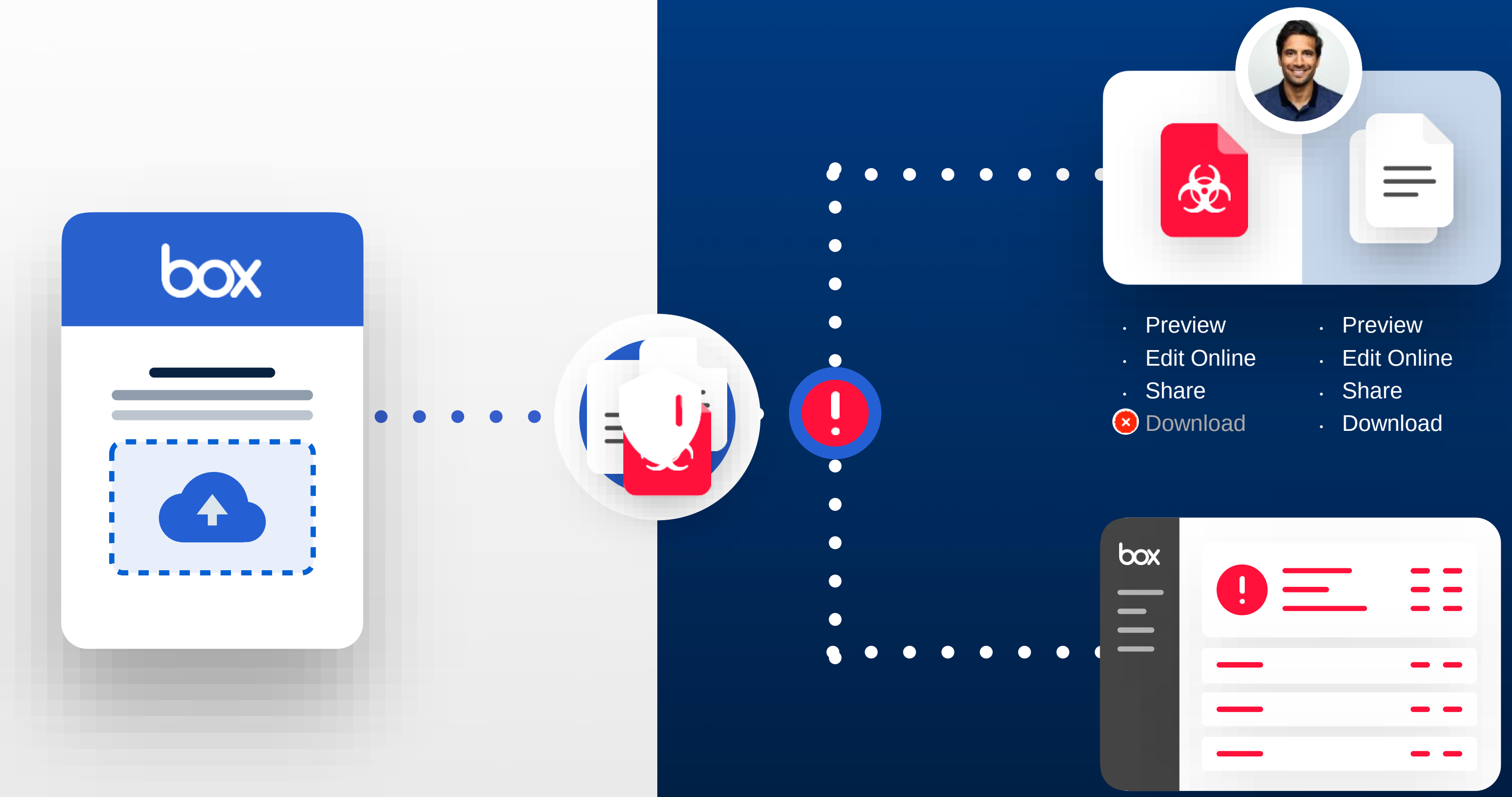
Purchase Order

Document created in earlier version of Microsoft Office Word

To view this content, please download this file and click “**Enable Editing**” from the yellow bar and then click “**Enable Content**”.


box

box



- Preview
- Edit Online
- Share
- ☒ Download

- Preview
- Edit Online
- Share
- Download

View Alert in Shield Dashboard
(forward to SIEMs like Splunk)

As a result, reduced risk while speeding up the business

Alex, Director of IT and Security

Outcome: Reduced risk of data leaks and fines

Improved posture by securing PII and IP with built-in controls, while meeting standards such as FINRA, ISO 27018, SEC 17a-4

Kim, VP and Head of Client Advisory

Outcome: Improved satisfaction and shortened process

Shortened end-to-end onboarding process from 3 weeks to 3 days, which improved client satisfaction and engagement

Thank You!

Helping our customers protect their content

FY22 roadmap summary

Core security

- Groups for Admin Policy
- Vector-based watermarking
- Device Trust 3.0
- 2FA Authentication app support
- External 2FA management and recovery

Box Shield

- MIP integration
- Auto-classification Improvements
- Access Policy monitoring mode
- Ethical wall
- Malware deep scan
- More security controls

Compliance products

- Retention performance improvements
- Event-driven retention
- Modifiable retention
- GxP sandbox testing
- GxP test coverage
- FedRamp High certification

Enterprise administration

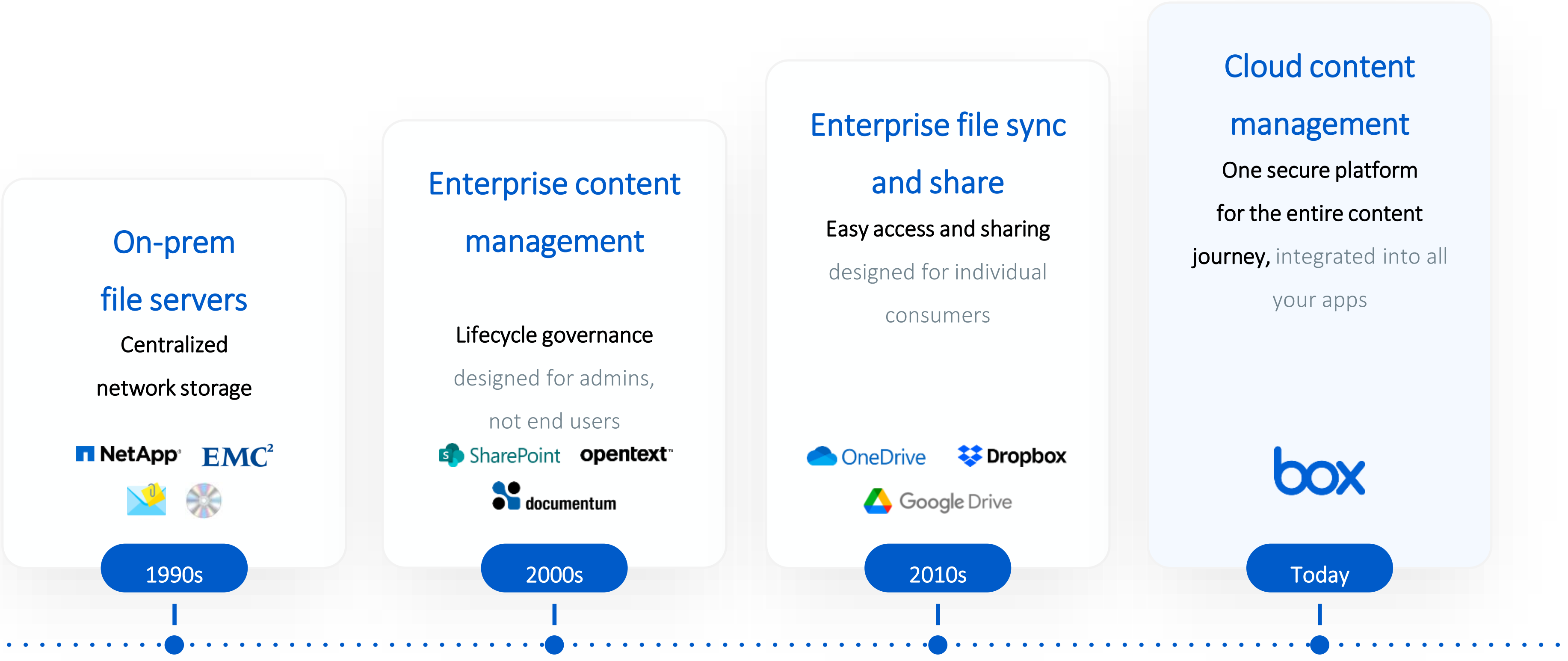
- 99.9% report success rate
- What’s New: message center
- Domain verification
- Managed Users redesign
- Scheduled reports

Content is at the heart of all work

But our most valuable content is locked in silos

File shares and email	Content management	Personal storage and sharing	Communication apps	Line-of-business apps
✉	SharePoint	OneDrive	Microsoft Teams	servicenow
EMC^2	opentext™	Google Drive	zoom	Adobe
NetApp®	documentum	Dropbox	slack	salesforce

Every tech shift has changed how we manage content



On-prem file servers

Centralized network storage

NetApp EMC²

1990s

Enterprise content management

Lifecycle governance designed for admins, not end users

SharePoint opentext documentum

2000s

Enterprise file sync and share

Easy access and sharing designed for individual consumers

OneDrive Dropbox Google Drive

2010s

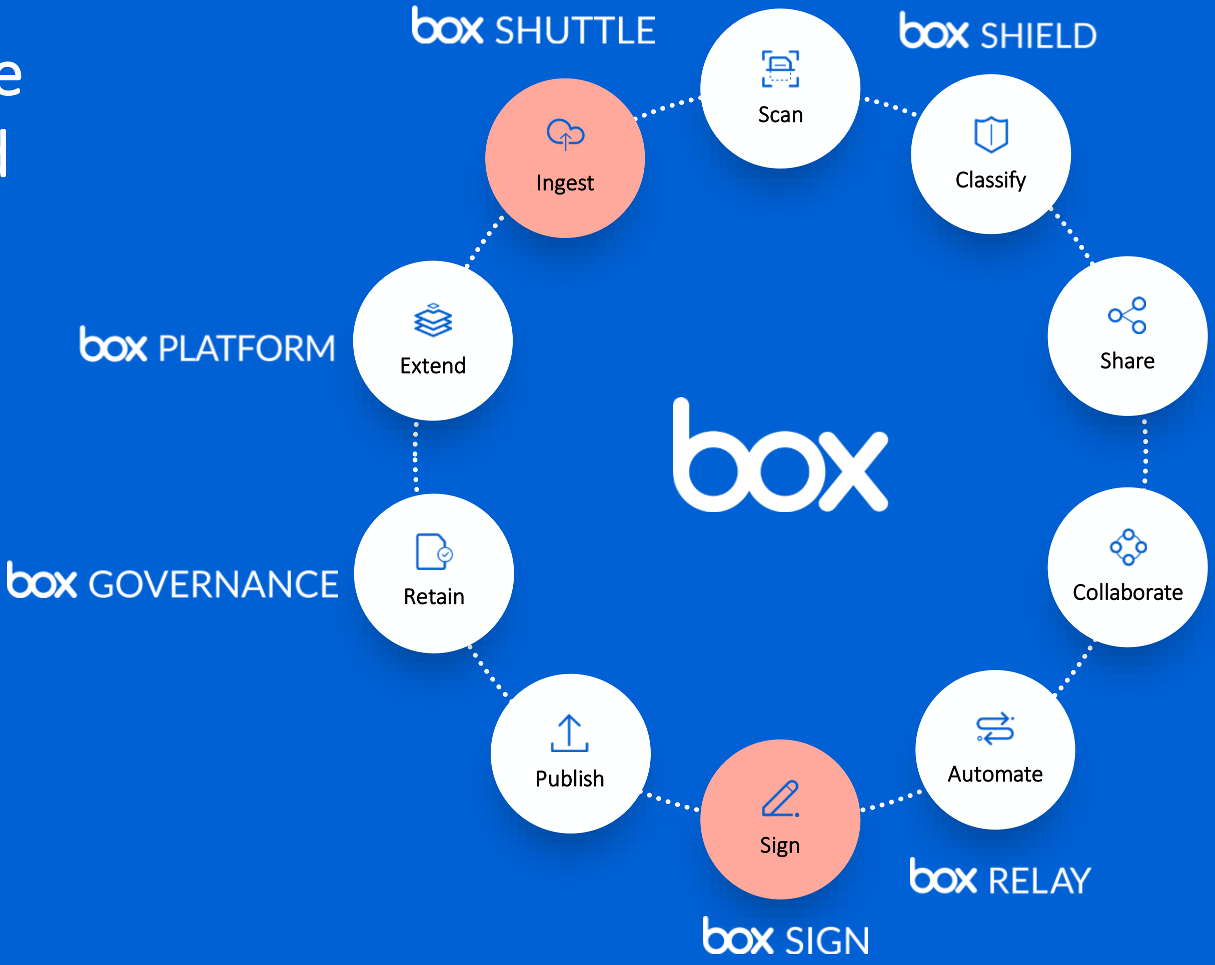
Cloud content management

One secure platform for the entire content journey, integrated into all your apps

box

Today

Completing the Content Cloud



Sign

box SIGN

Secure, seamless e-signatures where your content lives

Native e-signatures

Available from right within the Box Content Cloud, and extensible via APIs

Included in your subscription

E-signatures for the entire organization, no matter the department or industry

Secure and compliant

Industry-leading Box security and compliance baked in

Ingest

box SHUTTLE

Accelerate your migration to the Content Cloud

Any system

Cloud and on-premises connectors to move content from any source

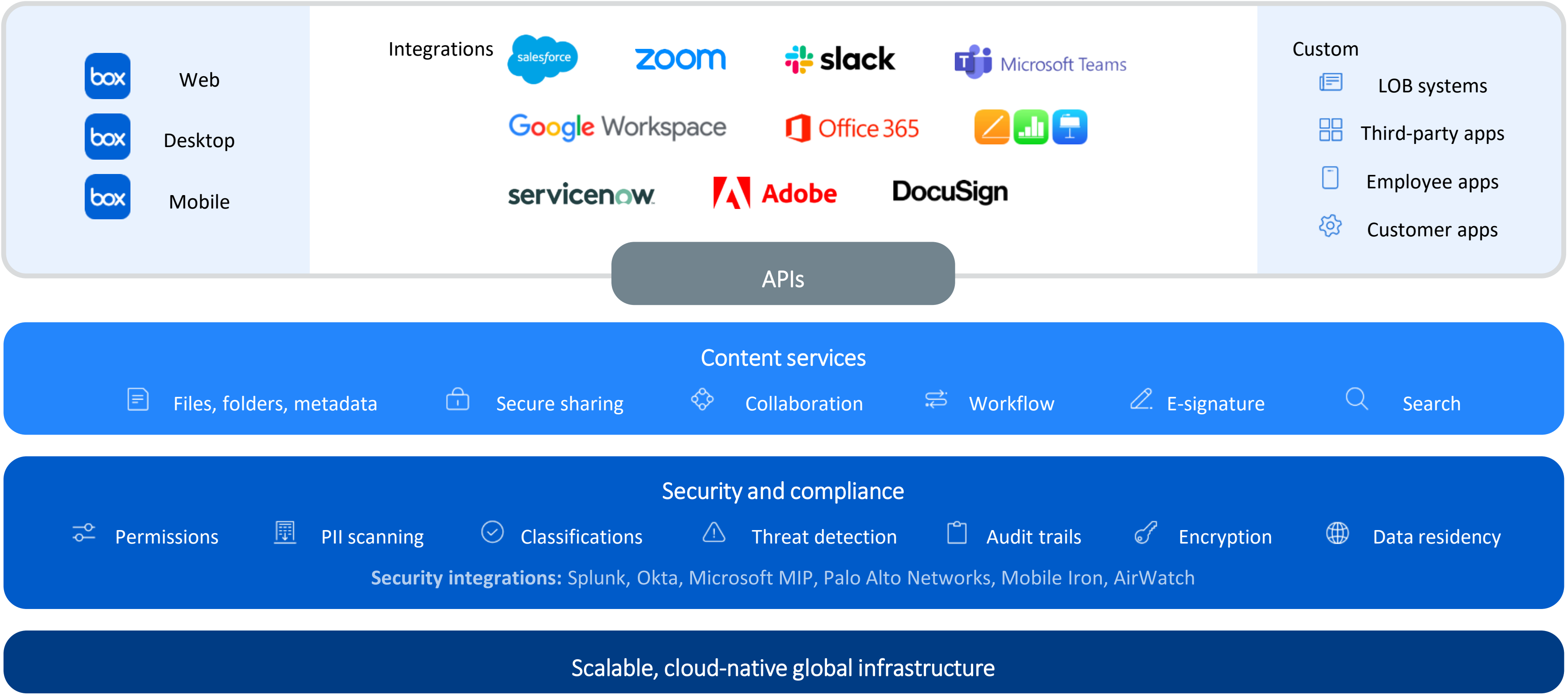
Content intelligence

Maintain internal and external permissions, version history, and metadata

Move quickly

Move dozens of terabytes per day with automatic API and network optimization

The industry-leading cloud content platform



box Web

box Desktop

box Mobile

Integrations: salesforce, zoom, slack, Microsoft Teams, Google Workspace, Office 365, servicenow, Adobe, DocuSign

Custom
- LOB systems
- Third-party apps
- Employee apps
- Customer apps

APIs

Content services

Files, folders, metadata · Secure sharing · Collaboration · Workflow · E-signature · Search

Security and compliance

Permissions · PII scanning · Classifications · Threat detection · Audit trails · Encryption · Data residency

Security integrations: Splunk, Okta, Microsoft MIP, Palo Alto Networks, Mobile Iron, AirWatch

Scalable, cloud-native global infrastructure

Box Industry Compliance Posture

ISO 27001

Global standard for information security and systems control

ISO 27018

Cloud service provider standard for handling Personally Identifiable Information (PII)

SOC-1 & SOC-2 Type II Reports

Third-party reports covering security, availability and confidentiality principles

FINRA/SEC 17a-4

Enables compliance with SEC 17a-4 for broker/dealer recordkeeping

PCI Data Security Standard

Compliant with DSS requirements for storing cardholder information as a service provider

HIPAA and HITECH

Trusted platform for PHI, PHRs and medical research

GxP Validation

Enables qualification of Box to store clinical, lab & manufacturing content

Box Privacy Posture

Privacy Shield

Compliant with requirements for collection, use & retention of personal information transferred from EU to US

Binding Corporate Rules

Cross border transfer mechanism approved by GDPR.

Approval by UK ICO, Spanish & Polish DPAs for Box as data processor and controller

APEC CBPR and PRP

Certification with the APEC cross border privacy requirements in the Asia-Pacific region

Box Global Government Compliance Posture

FedRAMP

US Federal program for security assessment, authorization, and monitoring of cloud services

Export Control

Compliant with ITAR/EAR regulations

C5

Cloud Computing Compliance Controls Catalogue. German govt. backed attestation by the Federal Office for Information Security

DoD Cloud SRG

Security Requirements Guide for Cloud Use in the Department of Defense

G-Cloud Framework

Approved for sharing official data in UK

IRS 1075

Requirements for storing Federal Tax Information (FTI)

box

Thank you

Upcoming events

ISO/AITR APPROVERS LIST

Please verify the ISO/AITR Approver's List for your agency. This list verifies who has the authority to approve KSE tickets. The list can be obtained by opening a ticket with the VCCC or contacting your CAM or BRM.

It is very important that if there is a change of ISO, AITR or other designated approver within your agency, your list should be updated accordingly. This will avoid any delays in approving any critical tickets that are outstanding.

VIRGINIA MANAGEMENT FELLOWS

The Virginia Management Fellows program deploys people, knowledge, skills, and experience preparing Fellows for permanent positions in the Commonwealth’s state agencies.

The Virginia Management Fellows Program falls under the Department of Human Resources. Individuals in this program rotate between selected state agencies every six months for two years.

If a Virginia Management Fellow is assigned to your agency, please verify they have completed Security Awareness Training either with DHRM or the agency they were previous assigned to. This will avoid duplication of training.

Please contact sarah.frame@dhrm.virginia.gov to verify training or if you have additional questions.

LET'S GET READY FOR:

CYBERSECURITY AWARENESS MONTH 2021

CYBERSECURITY AWARENESS MONTH 2021

Cybersecurity Awareness Month is fast approaching so let’s start planning our activities now. Below are the weekly themes for the month.

Week 1: Be Cyber Smart
Take simple actions to keep our digital lives secure.
Week 2: Fight the Phish!
Highlight the dangers of phishing attempts—which can lead to ransomware or other malware attacks—and how to report suspicious emails.
Week 3: Explore. Experience. Share.
Celebrate National Initiative for Cybersecurity Education’s (NICE) Cybersecurity Career Awareness Week and the global cybersecurity workforce, as well as host our own CISA hiring fair and highlight the varying educational tools CISA has.
Week 4: Cybersecurity First
Explore how cybersecurity and staying safe online is increasingly important as our world continues to operate virtually for so much of work and play.

CYBERSECURITY AWARENESS MONTH SPEAKER REQUESTS

If you would like to request a CISA speaker to participate in your Cybersecurity Awareness Month event, please complete a DHS Speaker Request Form and email it to CISA.speakers@hq.dhs.gov.

https://www.dhs.gov/publication/dhs-speaker-request-form

LITMOS TRAINING UPDATE

SANS will be conducting updated LITMOS content training for those agencies who are using the LITMOS platform under the VITA ISO Services license. Our license has been renewed for another year. Training will be on September 9th @10a via GoToMeeting. Invites have been sent out.

All agency administrators should attend.

If you have questions prior to the meeting, contact tina.gaines@vita.virginia.gov.

government technology
COVITS
VIRTUAL
SEPTEMBER 8 2021

SEPTEMBER IS ORIENTATION

September 30 from 1 to 3 pm

Required of all primary ISOs and anyone interested in the COV ISO certification at least once every 2 years.

Contact Marlon Cole to register.

https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e2bbb3be5081c70928bf8ce29b96d6cd6

OCTOBER ISOAG

October 6, from 1 to 4

Presenters:

CISecurity : NCSR Survey
CSRM Presenters (various)

This meeting is mandatory for primary ISOs. If you cannot attend, please let us know who at your agency will attend in your place.

VASCAN2021

Securing New Ways to Work

WHEN: OCTOBER 7 AND OCTOBER 8

WHERE: VIRGINIA COMMONWEALTH UNIVERSITY (IN PERSON)

COST: CONFERENCE ONLY $150

CONFERENCE AND TRAINING $400
(CONFERENCE $150 + TRAINING $250)

TRAINING: LINUX FORENSICS

REGISTRATION LINK:
HTTPS://VASCAN.VCU.EDU/CONFERENCE-REGISTRATION/

VIRGINIA IT AGENCY

THANK YOU FOR ATTENDING!