VIRGINIA
IT AGENCY

JULY ISOAG MEETING

VIRGINIA
IT AGENCY

- JOHN JOSEPH & DR. VAHID HEYDARI
- JASON ROBINSON
- BART SLOWIK
- JEFF SCHEICH
- DR. PETER AIKEN & LORNE JOSEPH
- ERIC TAYLOR
- UPCOMING EVENTS
- ADJOURN


Obtego Cyber
No hype. Just hide.
OBTEGO CYBER

What's the Problem?

You can't keep your attack surface from being found. Then ransomware spreads after they find you.

"My fundamental problem is the attack surface is a sitting duck. Adversaries can find it - anytime. Attack it - anytime."

- Brian Jackson, President and COO, Abacus Technologies

What's the Solution?

"Zero Trust +" technology that hides the attack surface on the perimeter (no open ports) *and* limits the spread of ransomware inside networks.

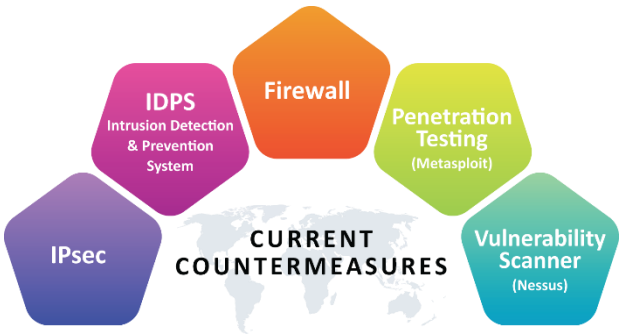
A New Layer of Security

NEW

CURRENT

YOUR IP ADDRESS

Obtego Cyber adds a new, light layer of security.



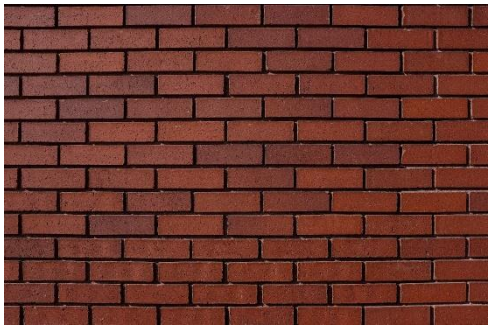
98.96.50.134

Problems with current Zero Trust Network Access (ZTNA) solutions

- *Attack Surface is not hidden – still a sitting duck*
- *Only as secure as the protocol used for HTTPS*
- *Any vulnerability gives full access to servers*
- *Reduced performance*

The Attack Surface: Obtego vs Zero Trust from an Attacker's Perspective

Obtego Secure Remote: Hides



$ nmap -p0-65535 50.19.51.201 -T5:
Host is up (0.0015s latency).
All 65536 scanned ports on ec2-50-19-51-201.compute-1.amazonaws.com (50.19.51.201) are filtered

ZTNA: Reduces

```
nmap -T4 -A -v [redacted]
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http nginx
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: nginx
```

Super Micro-Segmentation (Prevent Malware Lateral Movement)

- **VPN:** Remote users have access to the **entire LAN**
- **Micro-Segmentation:** Limit remote users to **a Subnet**
- **Obtego:** Limit remote users to **a Single App on a Single Server**

	VPN	Obtego
Number of **accessible ports** by a remote user	**600**	**1**

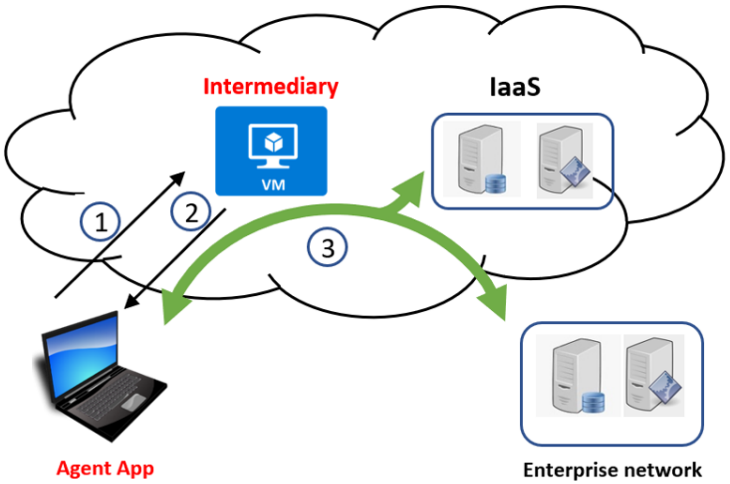
Assumptions:
- Number of devices inside the LAN: 50
- Number of connected remote users: 10
- Number of open ports per each device: 10

Can This Be Implemented?

Is Deployment Flexible?	Yes. Light software.
Are use cases relevant?	This technology works on fixed *and* mobile devices (from phones to medical devices to drones and more).
Does it work on IPv4 or IPv6?	Our first product hides the IPv4 attack surface. Our next product will hide the attack surface of 4 and 6.
Does it disrupt existing environments?	No rip-and-replace. We are an overlay to your existing environment, with no disruption to existing operations.

OBTEGO CYBER

Obtego Secure Remote Solution Framework



1	Authentication Request
2	List of Authorized Applications
3	Data Communication via Intermediary

Obtego Solution vs Status Quo

	VPNs	Zscaler	Obtego
Provides principle of least privilege	✗	✓	✓
Does not change the IP of users	✗	✓	✓
Helps prevent lateral movement of ransomware (Remote user only has access to a specific port on a specific server instead of all ports of all network devices)	✗	✓	✓
Supports SMB (sharing access to files etc.)	✓	✗	✓
Hides the Attack Surface (no open TCP or UDP ports!)	✗	✗	✓
Does not sacrifice performance	✗	✗	✓

Meet Obtego Cyber

Dr. Vahid Heydari (CTO) created our technology, which has been recognized by Sandia National Laboratories, IEEE, and others.

John Joseph IV (CEO) directs a business incubator and has cofounded/advised numerous startups.

Argonne NATIONAL LABORATORY

International conference ICCWS on Cyber Warfare & Security

Sandia National Laboratories

MACH37

RAPID REACTION Technology Office

21ST COLLOQUIUM FOR INFORMATION SYSTEMS SECURITY EDUCATION

AGC PARTNERS

OBTEGO CYBER

OBTEGO CYBER

Customers Want

Shorter attack windows

Diversified defense strategies

Peace of mind

Customers Told Us

As part of the newest MACH37 cohort, we spoke with over 60 potential customers to validate the problem and product/market fit.

*"It's a whole lot harder to **rob a moving car** than one just sitting there."*

Hayden Strickland
VP of Technology
Magnolia River Services, Inc.

*"I like the idea that **people wouldn't be able to see my server**."*

Stacey Nicholson
President
CNR Insurance, Inc.

*"The notion that people can't find what they're attacking is a **very attractive value proposition**."*

Jitendra Puri
Former CIO/CTO
Colombian Securities Exchange

OBTEGO CYBER

OBTEGO CYBER

Go To Market

Enterprise	SMB	Highly Regulated	IoT/5G
Direct/Channel	*Channel*	*Licensing*	*OEM / Embedded*
		• SCADA/ICS • Healthcare • Aerospace + Defense • Autonomous Tech	• Routers • Carriers/ISP • Infrastructure

Revenue Models

- **Subscription fees**
- **Revenue splits with strategic partners**
- **Licensing for specific verticals**

Other Solutions:

Assume A Sitting Duck Attack Surface + Ransomware Spread

- Traditional network barriers (firewall, IDS)
- Identity and Access Management
- Compliance
- Incident Response
- Penetration
- Zero Trust
- Deception/Virtualization (honeypots, etc.)
- SDP/SDN
- Limiting the attack surface

Obtego Cyber:

We Hide The Attack Surface + Limit Ransomware Spread

WE HIDE THE ATTACK SURFACE, CREATING A POLYMORPHIC PERIMETER.

Stealth-Mode Milestones

Patents Issued
(3rd issued 2021)

Demos Underway

Early Adopters Committed

Approached for Scale Up Opportunities

Early Adopter Feedback

- ✓ Ease of use “fantastic "
- ✓ Admin portal looked “easy to administrate” – very important
- ✓ Key point - the ability to isolate the user only to what they need on the network is a great, great piece – the technology can limit access to one service on our server as opposed to giving access to the entire network
- ✓ The speed is “amazing”

Product Development Roadmap

- **Gen 1: “Zero Trust +” technology that**
  - **Hides the attack surface**
  - **Limits the spread of ransomware**

- **Gen 2: Isolate internal attackers**

OBTEGO CYBER

OBTEGO CYBER

Questions?

Obtego Cyber

No hype. Just hide.

Auspex Labs Inc.

July ISOAG Meeting

Jason Robinson
Chief Executive Officer

Revised 07/10/2021

Auspex Labs Inc.

Applied Data Science in the Domain of Cybersecurity

Auspex Observatory™

Auspex Observatory™ is a user-friendly network observability / visualization platform that collects a broad scope of telemetry from common agents and logging mechanisms. This telemetry provides the vectors to detect threats as they begin, giving your organization the ability to prevent damage before it disrupts your business.

Professional Services:

Compliance

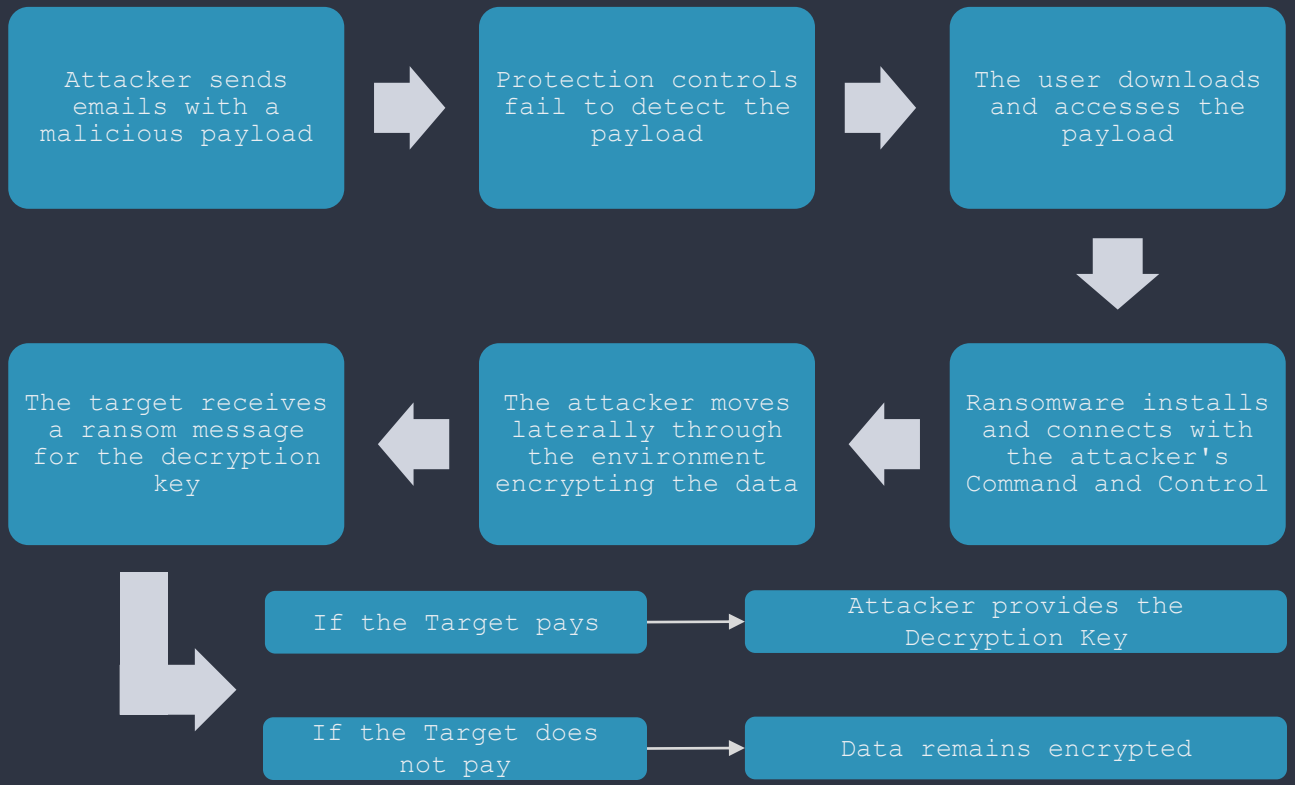
Penetration Testing

Threat Intelligence

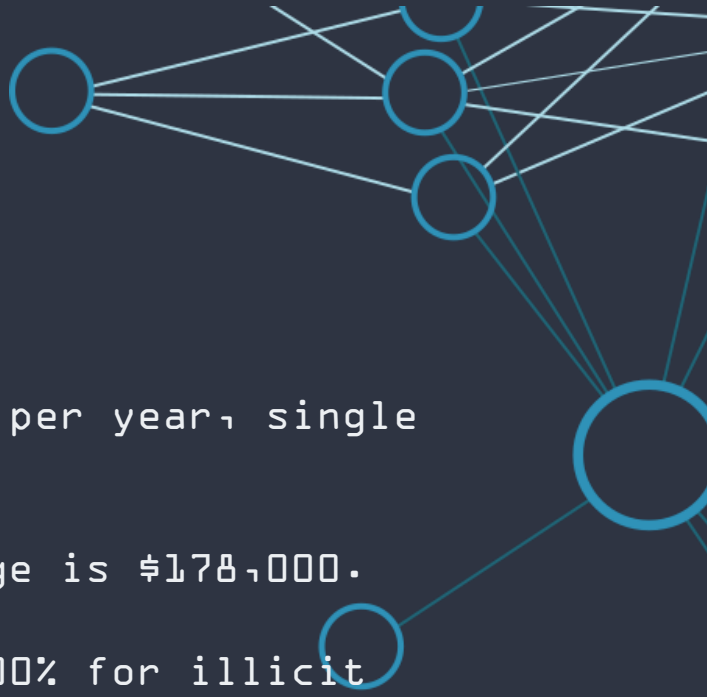
Static Code Analysis

Anatomy of a Breach

Ransomware Workflow



Why Ransomware?



- Ransomware Kits cost less than $100.
- Extremely low risk; less than 100 arrests per year, single digit convictions.
- 18.3% of attacks result in payouts, average is $178,000.
- Profit margin of 65,000% compared to 12,000% for illicit drugs.
- Double extortion for exfiltraited data, average is $234,000.
- Estimated harm caused in 2020: $20 Billion.

Should You Pay?

No, you shouldn’t.

- 80% of Organizations that pay are compromised again.
- Only 8% of Organizations that pay recover all of their data.
- 29% recover less than half of their data.
- Recovery costs for those who pay are on average twice as high as those who don't pay.
- It is increasingly consider unethical to pay.

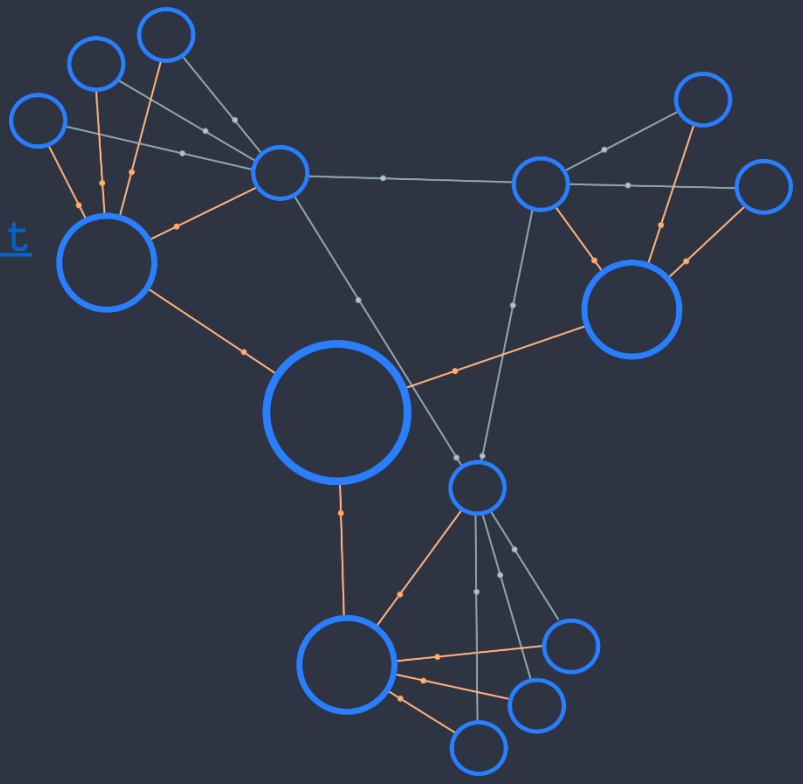
FBI's Tips for Avoiding Ransomware

- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
- Back up data regularly and double-check that those backups were completed.
- Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
- Create a continuity plan in case your business or organization is the victim of a ransomware attack.

Auspex Labs' Ransomware Advice

- Maintain a Blackhole Hosts File https://github.com/StevenBlack/hosts
- Configure Russian as a secondary language

These two actions will protect your systems over 90% of the time.



Ransomware Detection

The earlier that Ransomware is detected, the easier it is to mitigate. Network Observability tools make this task practical.

The key points of detection:

- Communication with Command and Control
- Detection of Lateral Movement in your Network
- Data Flowing Out of Your Environment
- Infected Hosts Encrypting Centralized Files

Questions?

Thank you!

Auspex Labs Inc.

jason.robinson@auspex-labs.com

540.860.0772

www.auspex-labs.com

SylLab

Security and compliance – simplified

Data Privacy Simplified

SylLab Systems provides embedded compliance for enterprise data security through its technology.

Problem

EXPENSIVE	DIFFICULT
Costs • **Security** • **Compliance and Non-compliance** • **Maintenance**	Complexity • **Cryptography is difficult to implement** • **Regulations are changing** • **Slow to implement**

EQUIFAX Lack of Encryption - $2 billion

Marriott Stolen Cryptographic Keys - $ 1 billion

Solution

Secure your data and stay compliant for a fraction of the cost!

AFFORDABLE

Save $100K and more on security and compliance

Pay as you grow your business

Save on expensive maintenance

FAST

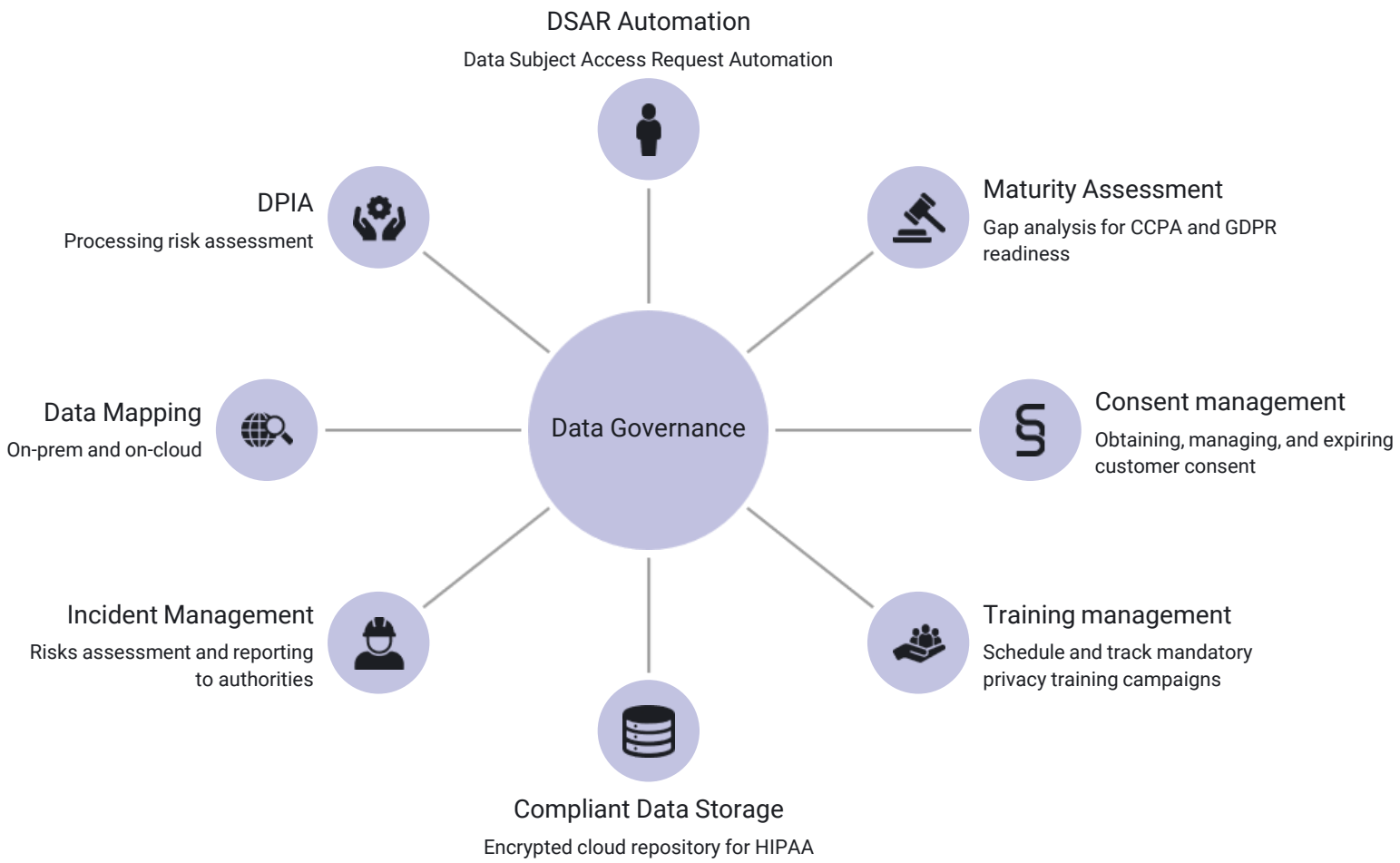
Built-in cryptography and security

Zero to low code deployment

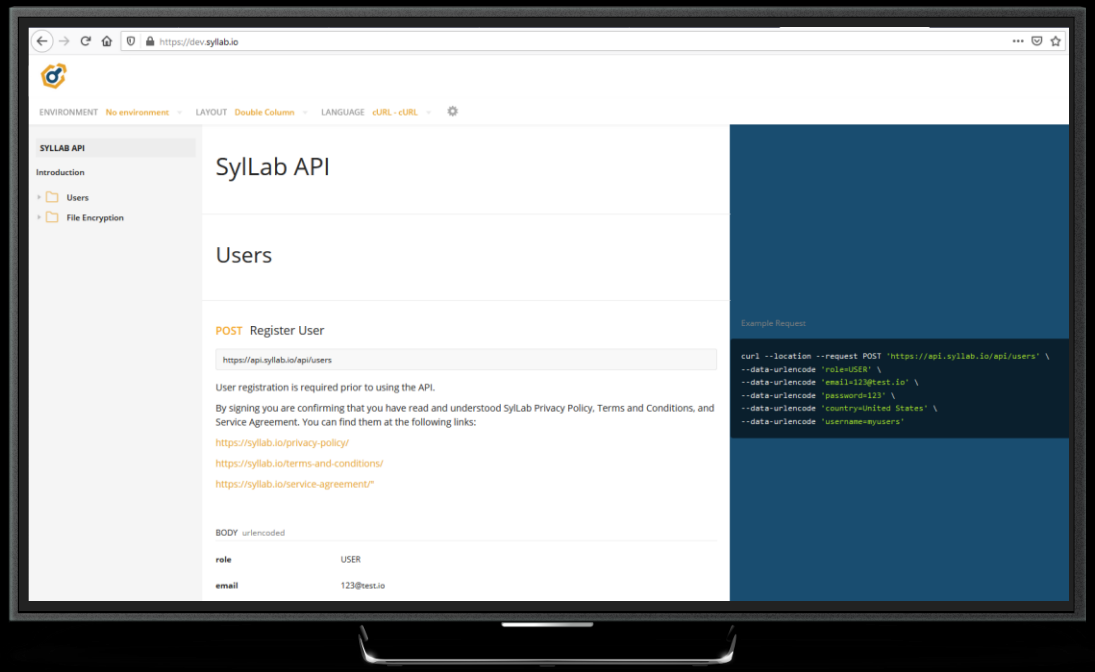
One-click compliance

WordPress Plugin (starting from) **$5.99 /m**

SylLab API **$60 /m + $0.18 API call**

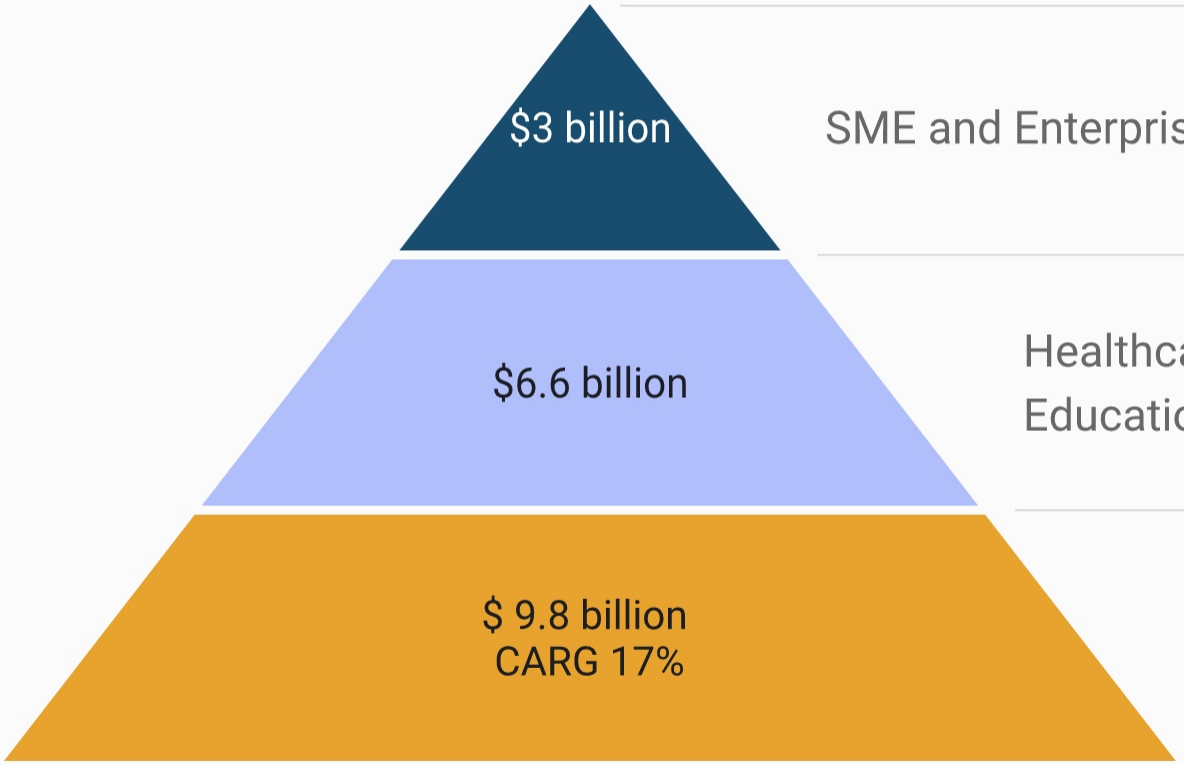

DSAR Automation
Data Subject Access Request Automation
DPIA
Processing risk assessment
Maturity Assessment
Gap analysis for CCPA and GDPR readiness
Data Mapping
On-prem and on-cloud
Data Governance
Consent management
Obtaining, managing, and expiring customer consent
Incident Management
Risks assessment and reporting to authorities
Training management
Schedule and track mandatory privacy training campaigns
Compliant Data Storage
Encrypted cloud repository for HIPAA

SylLab



1. Sensitive data stored securely
2. Low code HIPPA, CCPA, PDPA, GDPR, FINRA compliance
3. Granular Encryption and high-grade security

Bottom's Up Market Sizing



SME and Enterprise

Healthcare, Insurance, Fintech, Education, Government

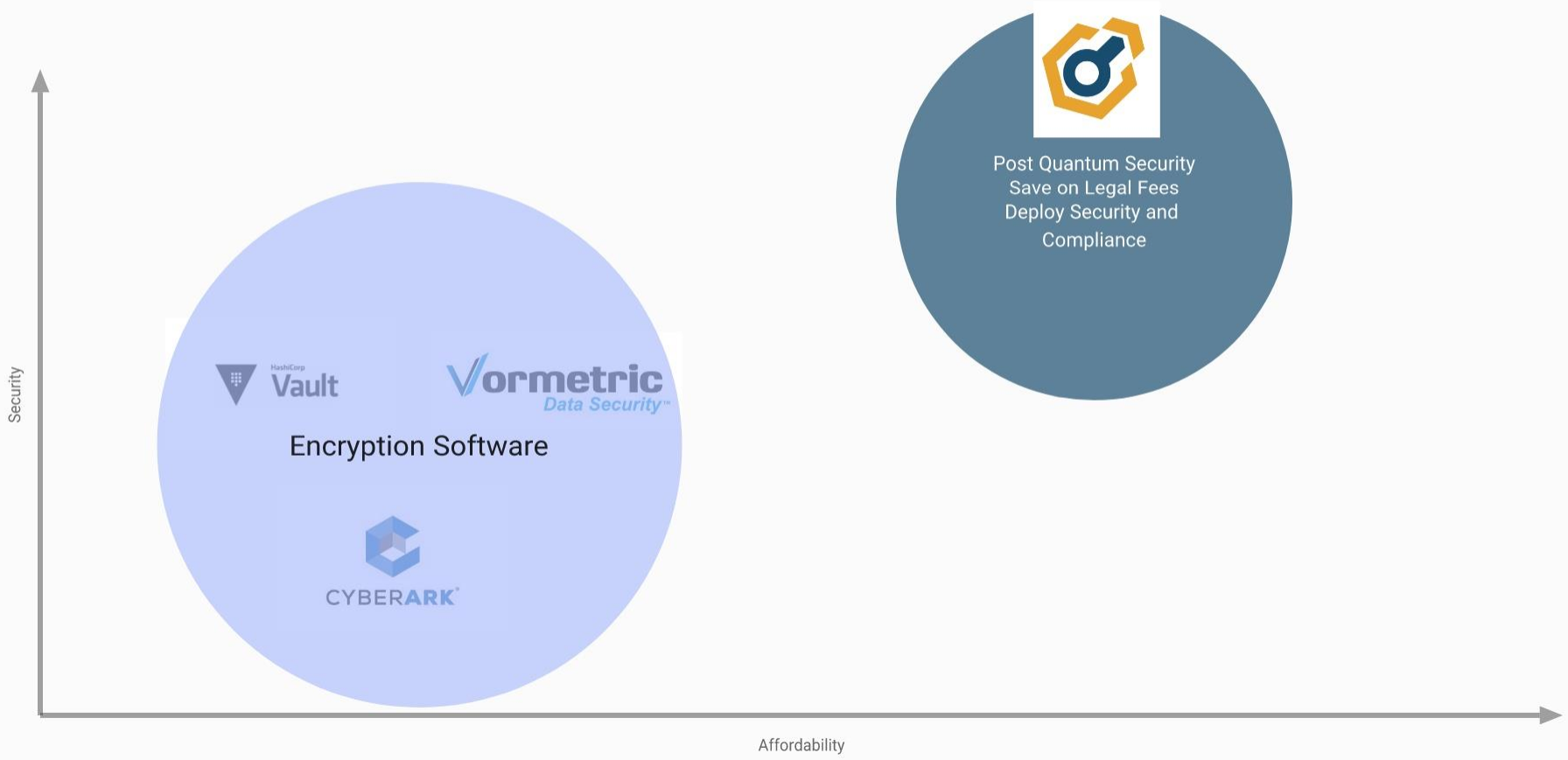
Encryption Management Solutions (*Technavio)

1. The market will nearly double in next 4 years*
2. Increase in digitization = data vulnerability
3. The regulations are changing and becoming more complex
4. SMEs don't have tools and budget to catch up

Why Now?

*Technavio

What Sets Us Apart



Our Team

Bart Slowik

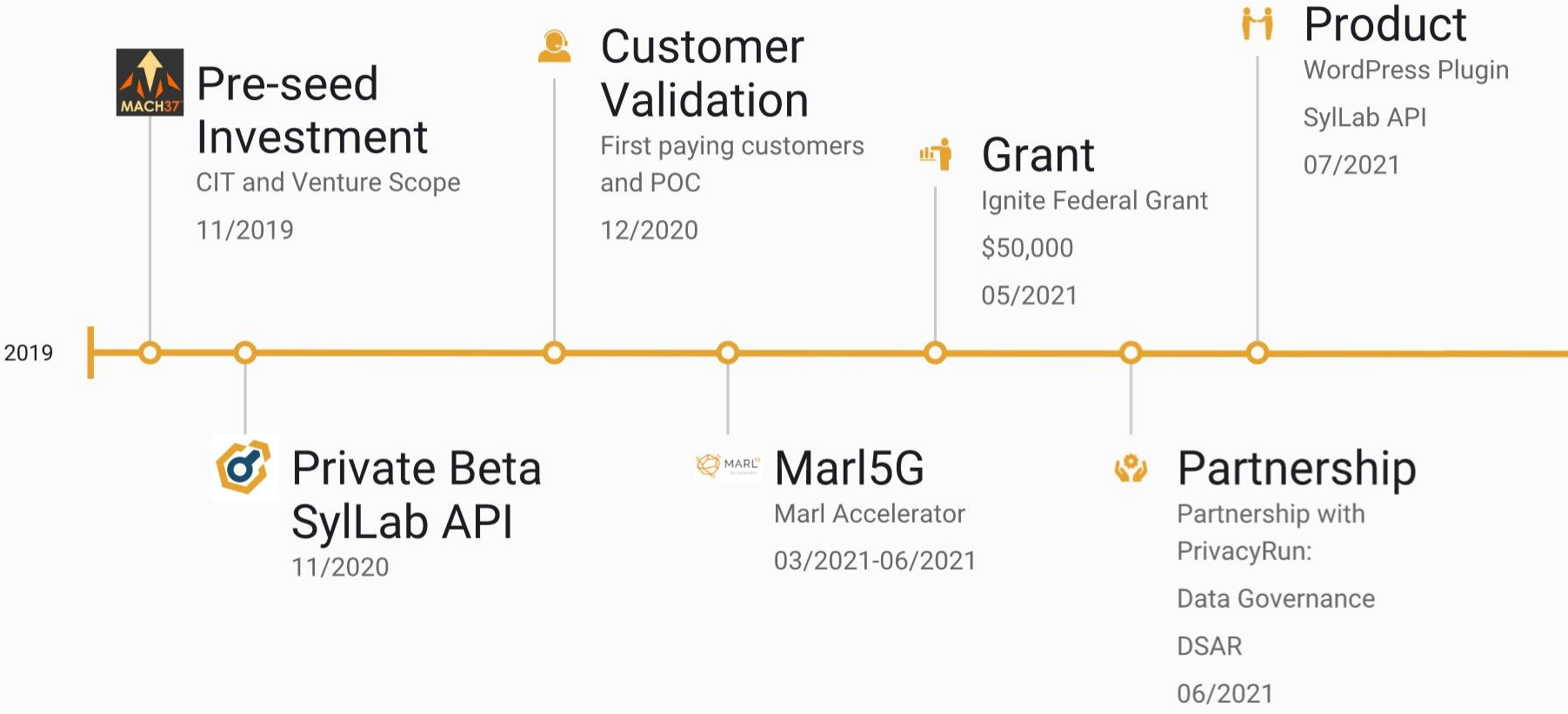
CEO

MIT Cybersecurity, Thomson Reuters

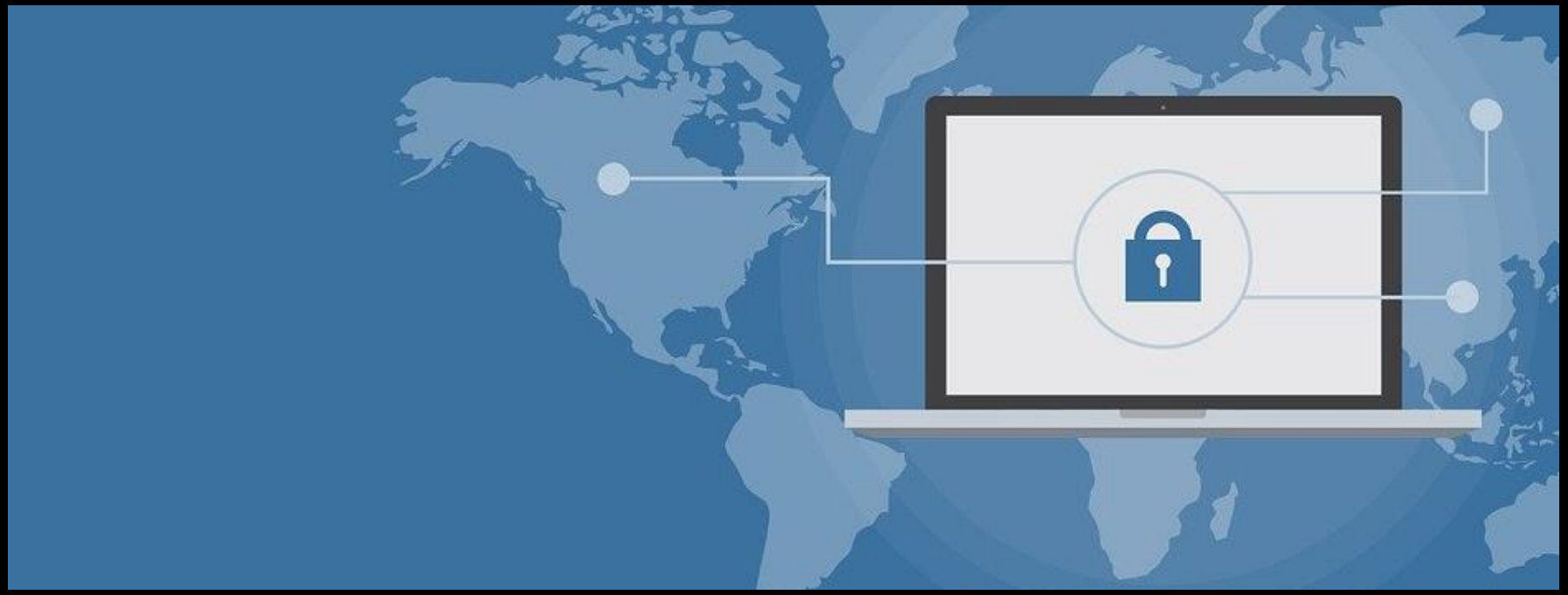
Ph.D Ramses Fernandez Valencia

Cryptographer

Ph.D in Mathematics, Applied Cryptographer

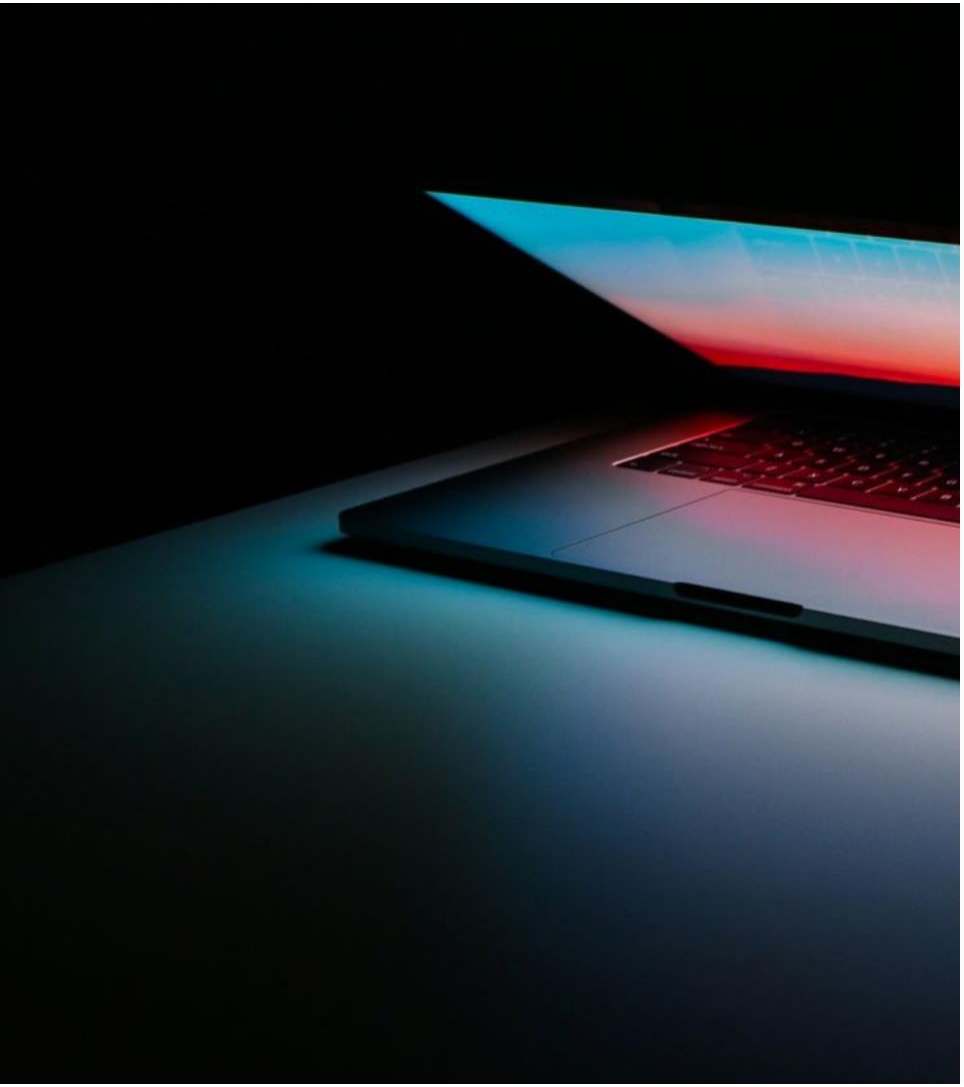

2019
Pre-seed Investment
CIT and Venture Scope
11/2019
Private Beta SylLab API
11/2020
Customer Validation
First paying customers and POC
12/2020
Marl5G
Marl Accelerator
03/2021-06/2021
Grant
Ignite Federal Grant
$50,000
05/2021
Partnership
Partnership with PrivacyRun:
Data Governance
DSAR
06/2021
Product
WordPress Plugin
SylLab API
07/2021

The Ask



Client introduction

CISOs that face privacy regulations and want to stream-line the process



Bart Slowik

CEO/ SylLab Systems, Inc.

bart@syllab.io

contact@syllab.io

syllab.io

VIRGINIA IT AGENCY

APPLICATION INTEGRATION SERVICES (AIS)

VITA SECURE GATEWAY

JEFF SCHEICH, AIS SERVICE OWNER
PRASHANT DIXIT, PROJECT MANAGER

JULY 14, 2021

What is VITA secure gateway?

- VITA secure gateway (VSG) service provides security and integration for Commonwealth of Virginia (COV) websites, applications and services.

- VSG is based on the IBM DataPower® multi-channel gateways that deliver security, control, integration and optimized access to a full range of on-premise and cloud workloads.

- The service includes solution design and implementation by the VITA application integration services (AIS) team. The AIS team has expertise with many COV agencies and collaborates with customers to implement the best solutions based on customer needs.

- The VSG service utilizes enterprise-grade gateways to securely connect within the QTS datacenter, to cloud and external vendors. Customers benefit with secure websites, applications and services all at cost effective rates.

Key features

- Secured API proxy – The VSG service increases productivity and improves outcomes for teams involved in API-led innovation efforts. The service provides security and proxy services for your enterprise APIs (REST/SOAP). Security policies are custom-defined and enforced with minimal developer coding required. The result is reduced coding effort for the customer and a common industry standard security policy is enforced across all services.

- Web application proxy - The VSG service provides additional security with an Internet/DMZ presence for your web application, regardless of where it resides in the network.

- Secure shell file transfer protocol (SFTP) proxy services - The VSG service offers SFTP and file transfer protocol secure (FTPS) proxy services, thereby enabling secure integrations and file transfers between third-party vendors (inside or outside the COV network) and customer SFTP server instances.

- Insights and troubleshooting – The VSG service includes an operations dashboard that provides centralized troubleshooting and real-time operational visibility. The result is faster problem determination and operational resiliency.

How does the secured application programming interface (API) proxy help in my agency applications developed using APIs?

Agency has coded a REST API in their application. In order to secure this API call, VSG is used to enforce lightweight directory access protocol (LDAP) authentication of the user who is requesting the data. Once the request is authenticated and authorized, the request is allowed access to call the service and return the data.

How does the Web Application Proxy help in my agency's application development efforts?

Agency has many web applications residing on a secure server. Most web applications are for agency internal use but the public website needs to be accessible from the internet. Instead of purchasing another server/instance in the DMZ, VSG can be utilized to proxy this request to the backend server in a secured manner.

How can my agency leverage the capabilities provided by the SFTP proxy services?

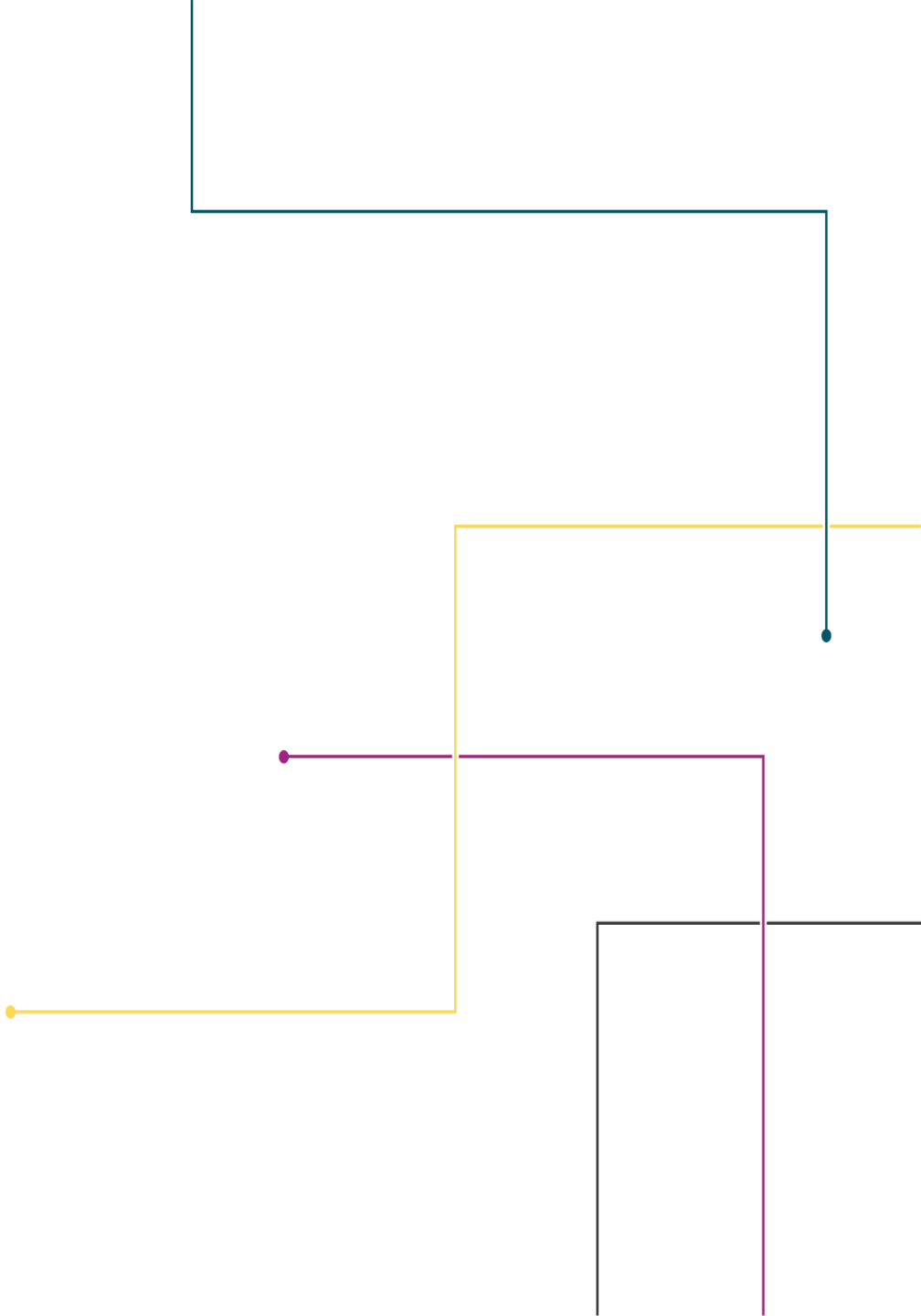
Agency creates an application on an enterprise service bus that processes data received via external vendors. VSG is able to proxy this secure shell file transfer protocol (SFTP) request through the DMZ, allows the external vendor to communicate directly to the SFTP server installed on the enterprise service bus, and transfers the data directly to the server.

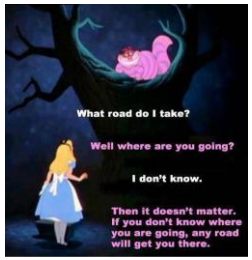
How does the insights and troubleshooting toolset benefit my agency?

Agency creates a service that VSG is protecting through mutual Secure Sockets Layer (SSL) authentication. They have a new client who is trying to get access, but the service is denying the request. By logging into this application, they are able to see debug logs of the transaction. By accessing this information, they are able to quickly and easily determine that they are passing the “wrong” certificate in the request, and debug the problem.

QUESTIONS?

Thank you!





"If you don't know where you are going, any road will get you there."
- Lewis Carroll

paiken@plusanythingawesome.com+1.804.382.5957

Presented jointly by:

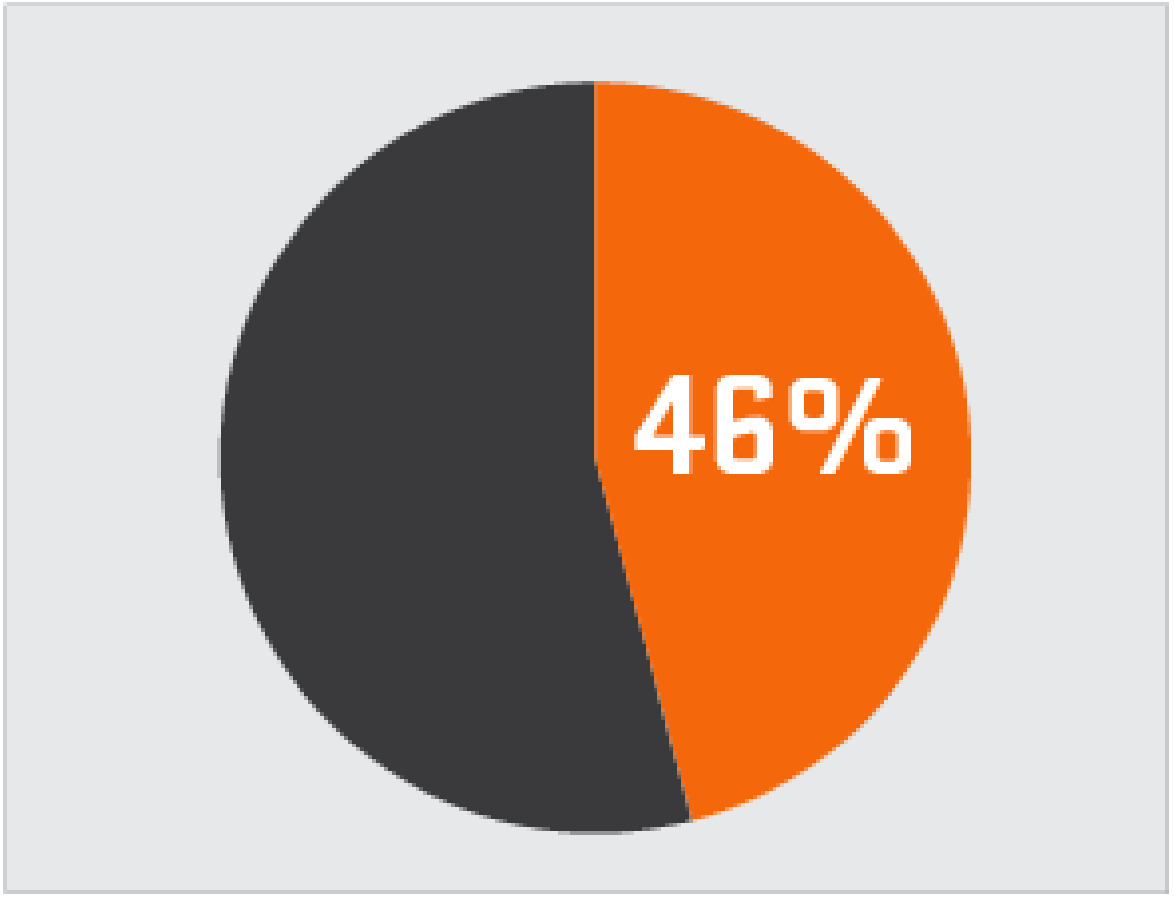
Lorne O. Joseph
Founder, eGRC.COM

Peter Aiken
Founder, Anything Awesome

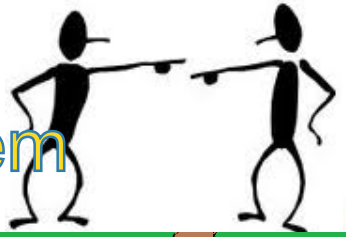
NEWS FLASH!

46% of companies report they made an inaccurate business decision based on bad or outdated data. Bad data leads to bad business decisions. Companies need to be careful that their data is sound – especially when dealing with investors.

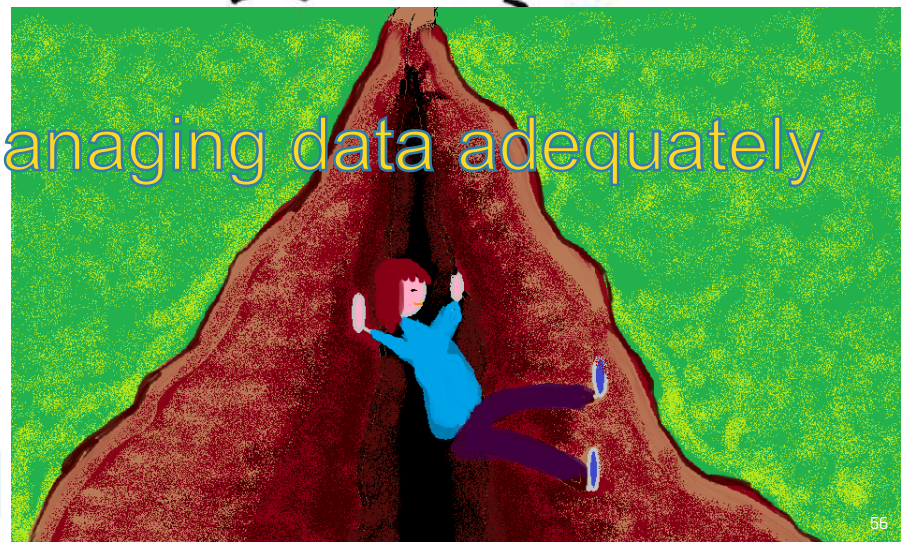
Like Comment Share



s problem



anaging data adequately



Business Challenge

Poor results

Business Challenge

Business Challenge

Business Process

IT System

IT System

Business Challenge

Business Process

IT Process

IT Process

Business System

Business Challenge

Business Challenge

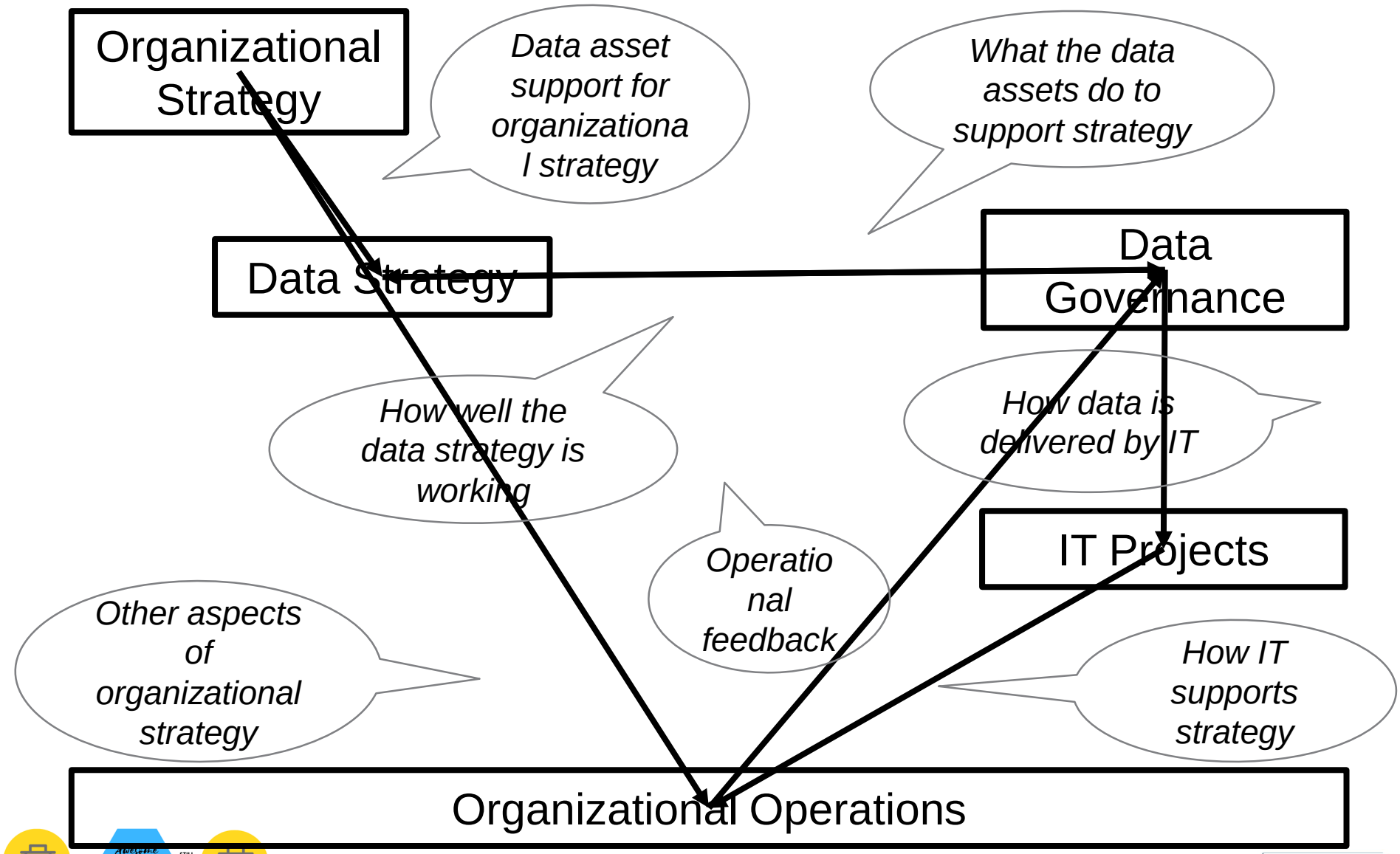
Business Challenge

Business Challenge

- "Putting structure around how organizations align IT strategy with business strategy, ensuring that companies stay on track to achieve their strategies and goals, and implementing good ways to measure IT's performance.
- It makes sure that all stakeholders' interests are taken into account and that processes provide measurable results.
- Framework should answer some key questions, such as how the IT department is functioning overall, what key metrics management needs and what return IT is giving back to the business from the investment it's making." *CIO Magazine* (May 2007)

IT Governance Institute, 5 areas of focus:

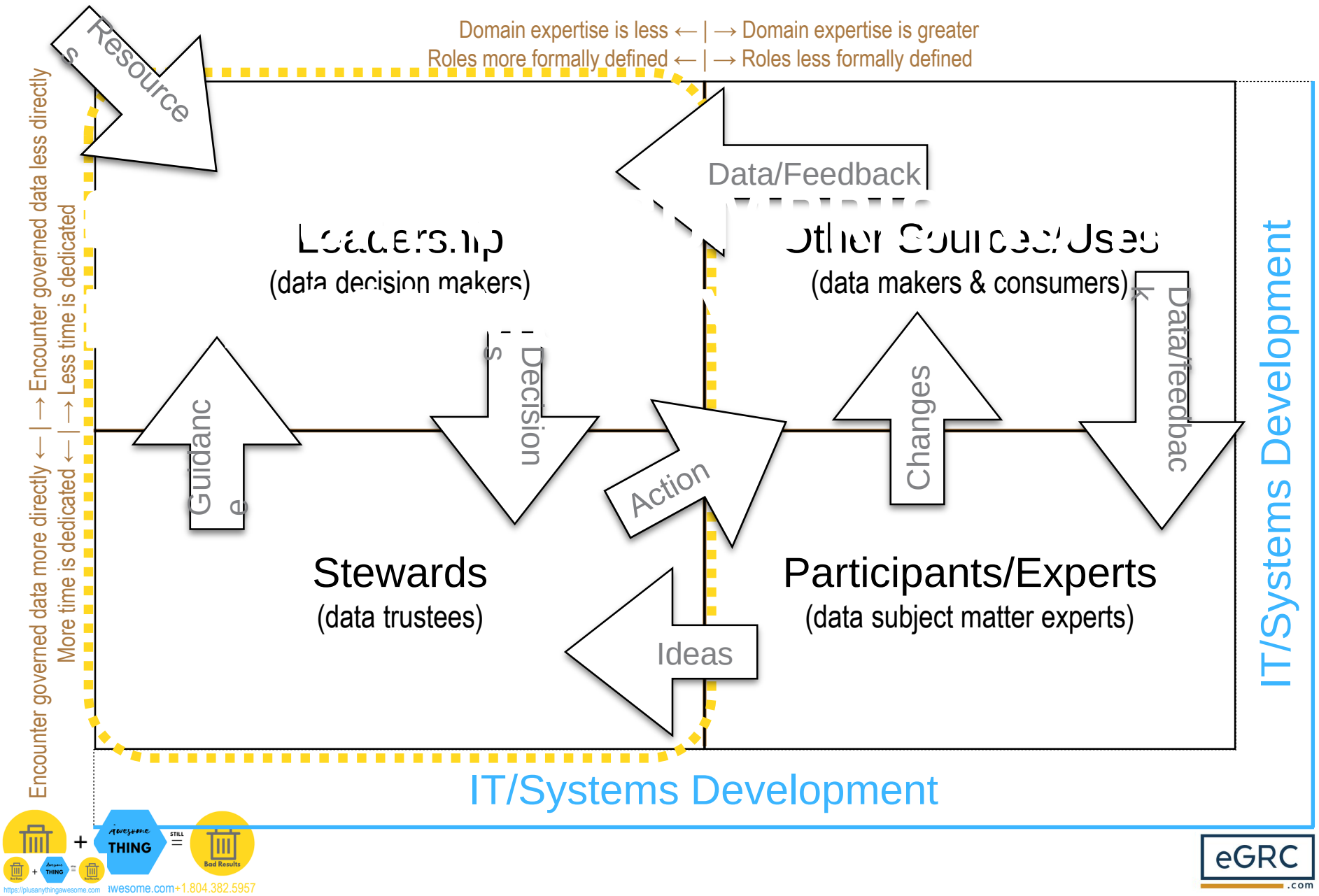
- Strategic Alignment
- Value Delivery
- Resource Management
- Risk Management
- Performance Measures

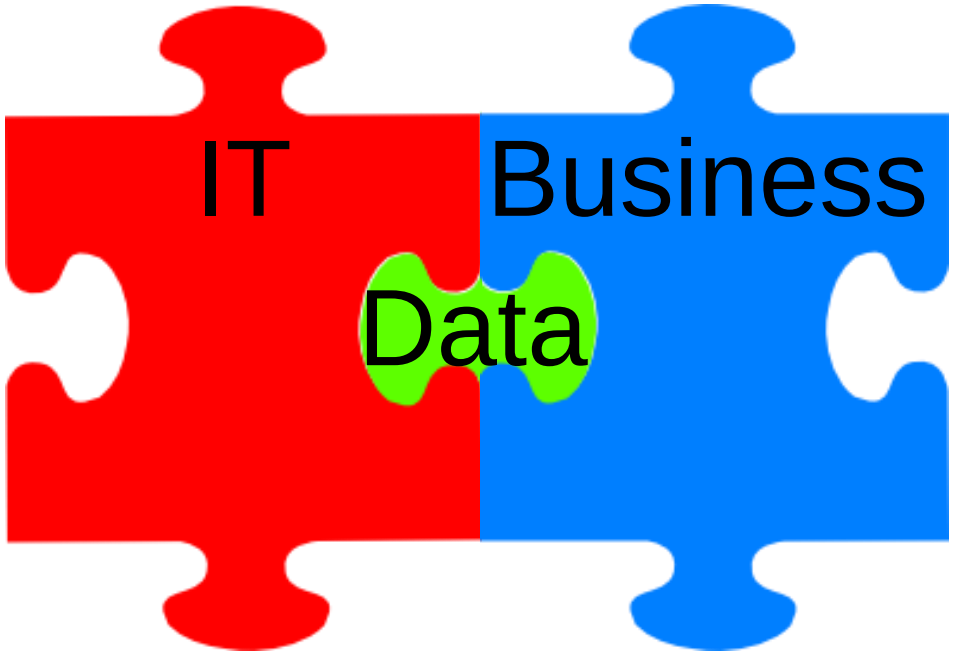


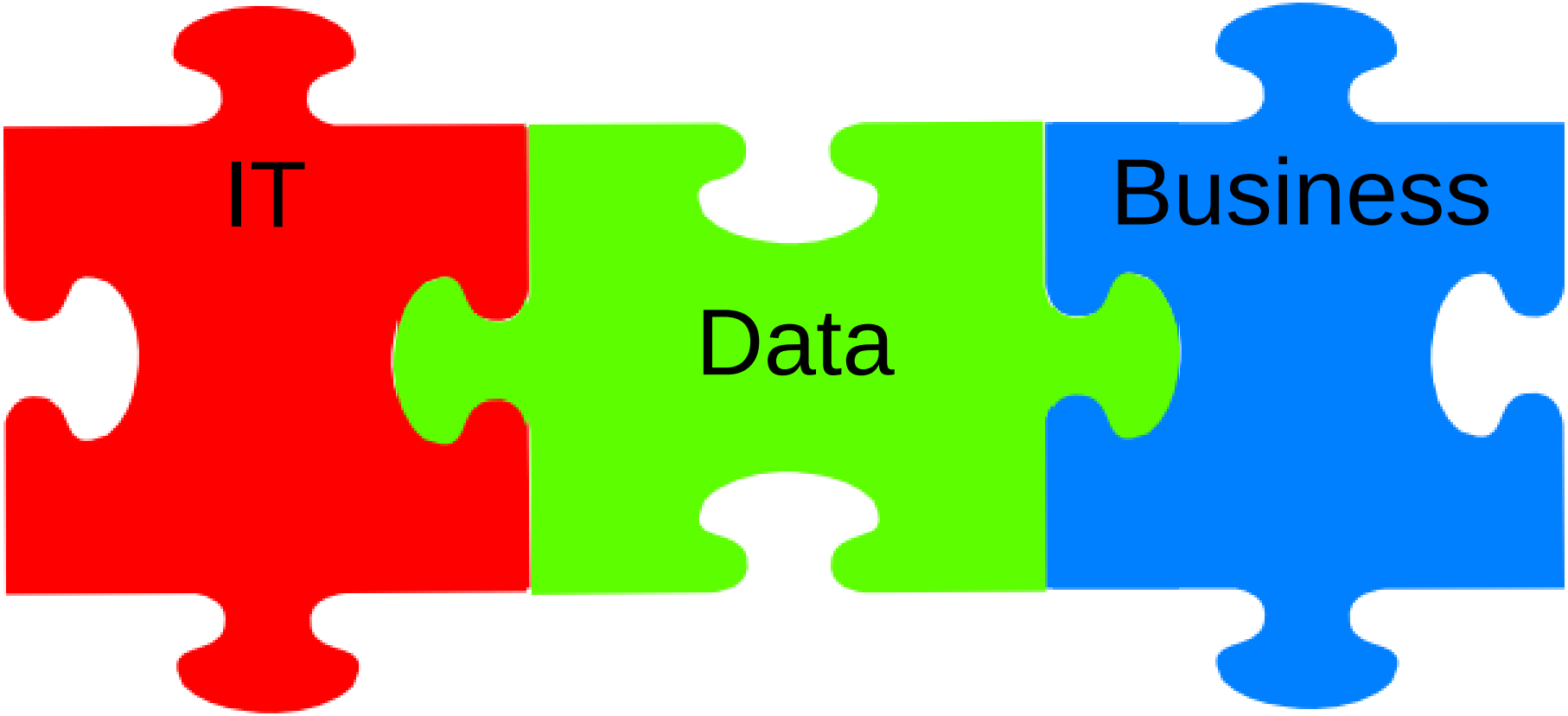
A system of ideas for guiding analyses

A means of organizing project data

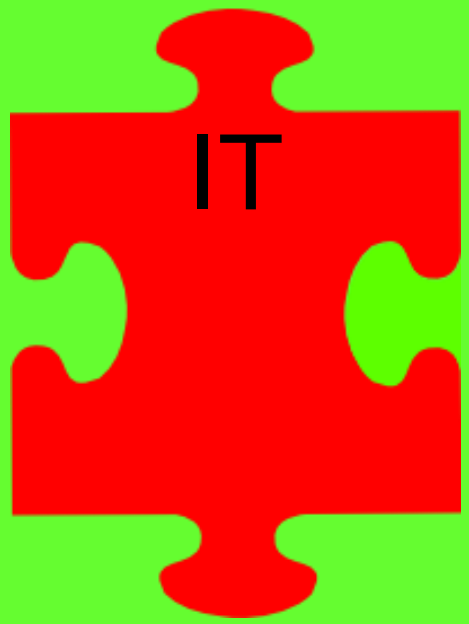
Priorities for data decision making







THE REAL STATE OF DATA



Data

Need for DG is increasing

Increase in data volume

Lack of practice improvement

DG must be driven by a data strategy complimenting organizational strategy

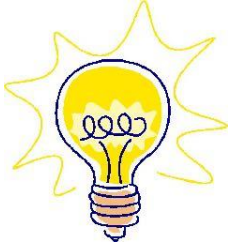
DG Strategy #1: Keep it practically focused like Asset Data required for Vuln Mgmt

DG Strategy #2: Implement DG (and data) as a program not a project

DG Strategy #3: Gradually add ingredients

Learn the value of stories/storytelling

Questions?



Thank + You!

from

Bad Data → Awesome THING STILL = Bad Results

&

eGRC.com

Websites

The Data Administration Newsletter (TDAN)–*http://www.TDAN.com*

DM Review Magazine–www.dmreview.com. Note: www.dmreview.com is now www.information-management.com.

EIM Insight, published by The Enterprise Information Management Institute–
http://eiminstitute.org

SearchDataManagement.com white paper library–
http://go.techtarget.com/r/3762877/5626178

Thomas, Gwen. Alpha Males and Data Disasters: The Case for Data Governance. Brass Cannon Press, 2006. ISBN-10: 0-978-6579-0-X. 221 pages.

Data Governance Book

Bloem, Jaap, Menno van Doorn, and Piyush Mittal. Making IT Governance Work in a Sarbanes-Oxley World. John Wiley & Sons, 2005. ISBN 0-471-74359-3. 304 pages.

Compliance Book

Benson, Robert J., Tom Bugnitz, and Bill Walton. From Business Strategy to IT Action: Right Decisions for a Better Bottom Line. John Wiley & Sons, 2004. ISBN 0-471-49191-8. 309 pages.

IT Governance Institute. Control Objectives for Information and related Technology (CobiT©). www.isaca.org/cobit

Lutchen, Mark. Managing IT as a Business: A Survival Guide for CEOs. John Wiley & Sons, 2003. ISBN 0-471-47104-6. 256 pages.

Maizlish, Bryan and Robert Handler. IT Portfolio Management Step-By-Step: Unlocking the Business Value of Technology. John Wiley & Sons, 2005. ISBN 0-471-64984-8. 400 pages.

Van Grembergen, Wim and Steven Dehaes. Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value. Springer, 2009. ISBN 0-387-84881-5, 360 pages.

Van Grembergen, Wim and Steven Dehaes. Implementing Information Technology Governance: Models, Practices and Cases. IGI Publishing, 2007. ISBN 1-599-04924-3, 255 pages.

Van Grembergen, Wim and Steven Dehaes. Strategies for Information Technology Governance. IGI Publishing, 2003. ISBN 1-591-40284-0. 406 pages.

Weill, Peter and Jeanne Ross. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, 2004. ISBN 1-291-39253-5. 288 pages.

VIRGINIA
IT AGENCY

ENTERPRISE ENDPOINT SECURITY

ENDPOINT SECURITY
MANAGED DETECTION AND RESPONSE

ERIC TAYLOR

JULY 14, 2021

VITA & Atos will soon be replacing certain elements provided by the McAfee security tool suite with the CrowdStrike Falcon platform. CrowdStrike will be deployed to all endpoints and servers. The CrowdStrike platform will **improve** the following VITA services **without** impacting existing operations:

- Desktop-managed host intrusion protection, firewall and antivirus
- Server-managed firewall and antivirus
- Server-managed host intrusion protection
- Security incident management
- Security monitoring, log management and analysis

What are the benefits of CrowdStrike?

- The CrowdStrike platform provides better protection through artificial intelligence-enabled solutions.
- It has the ability for computer systems to perform tasks that normally require human intelligence; this will enhance the cybersecurity operators with instant and holistic visibility.
- CrowdStrike brings better performance of operating systems and agency applications. The cloud-native solutions eliminate complexity, simplify deployment and provide consistent solutions regardless of environment or location
- Dramatically decreasing performance impact of a endpoint security solution
- Deployed in a single agent.

- CrowdStrike Falcon provides all core EPP capabilities in a single agent, with customers appreciating the low resource utilization.
- An easy-to-use management console and simplified deployment experience add to the high rating for market understanding and innovation.
- CrowdStrike has a strong reputation in the market as the single solution for endpoint security for organizations looking to consolidate their EPP and EDR agents/solutions
- CrowdStrike has a customer base that is highly targeted by attackers. As a result, it has consistently adapted early to shifts in attack techniques. It achieved positive results in the MITRE phase two evaluations with consistent identification of tactics and techniques.

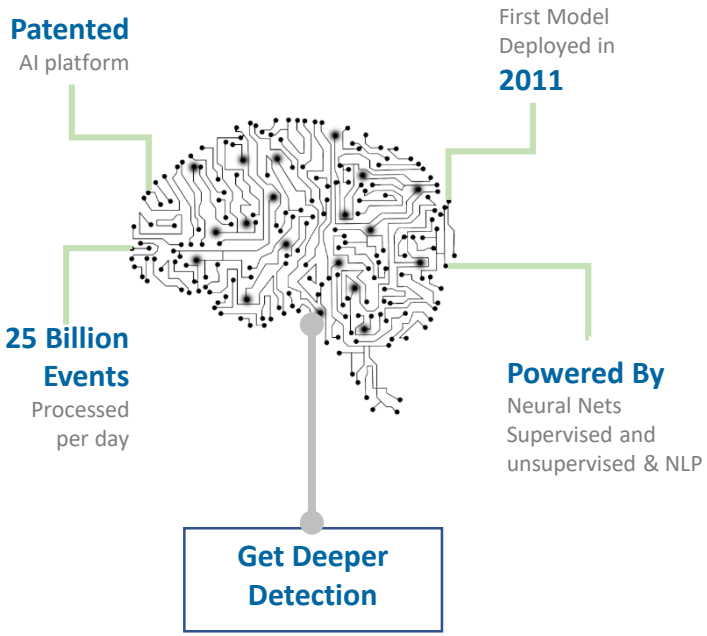
Source: Gartner (May 2021)

- This will be a phased approach by agency with the intention to onboard all assets of an agency together. De-installation of McAfee components will take place during the CrowdStrike deployment process
- “Crowdstrike has worked great for us and has also solved an existing issue that was long running , **kudos to this effort and the product that now we are even ready to have our agency leadership use the product and utilize the benefits.** Again we have the highest visibility stakeholders at VADOC including the CIO and the Deputy CIO along with agency leadership now which will use the product and undoubtedly help champion the effort when VITA/CSRM decide to scale this enterprise wide. ” --- **Kartik Yadav**

- VITA & Atos will soon be replacing all elements provided by the McAfee security monitoring suite (SIEM) with the Atos MDR platform – (formally – Paladion AIsaac)
- Atos MDR platform, known as AIsaac, will bring efficiencies in Security Operations Monitoring and Response.
- The AIsaac platform was developed by Paladion, a top tier MDR provider. Paladion was acquired by Atos in 2020
- Paladion Recognized as Winner of Microsoft's 2020 Most Innovative AI Solution
  - Paladion was honored among top businesses who have taken early strides in Artificial Intelligence and have demonstrated business impact implementing innovative technology
- The deployment will replace the current log collector agent on servers for the Atos MDR agent

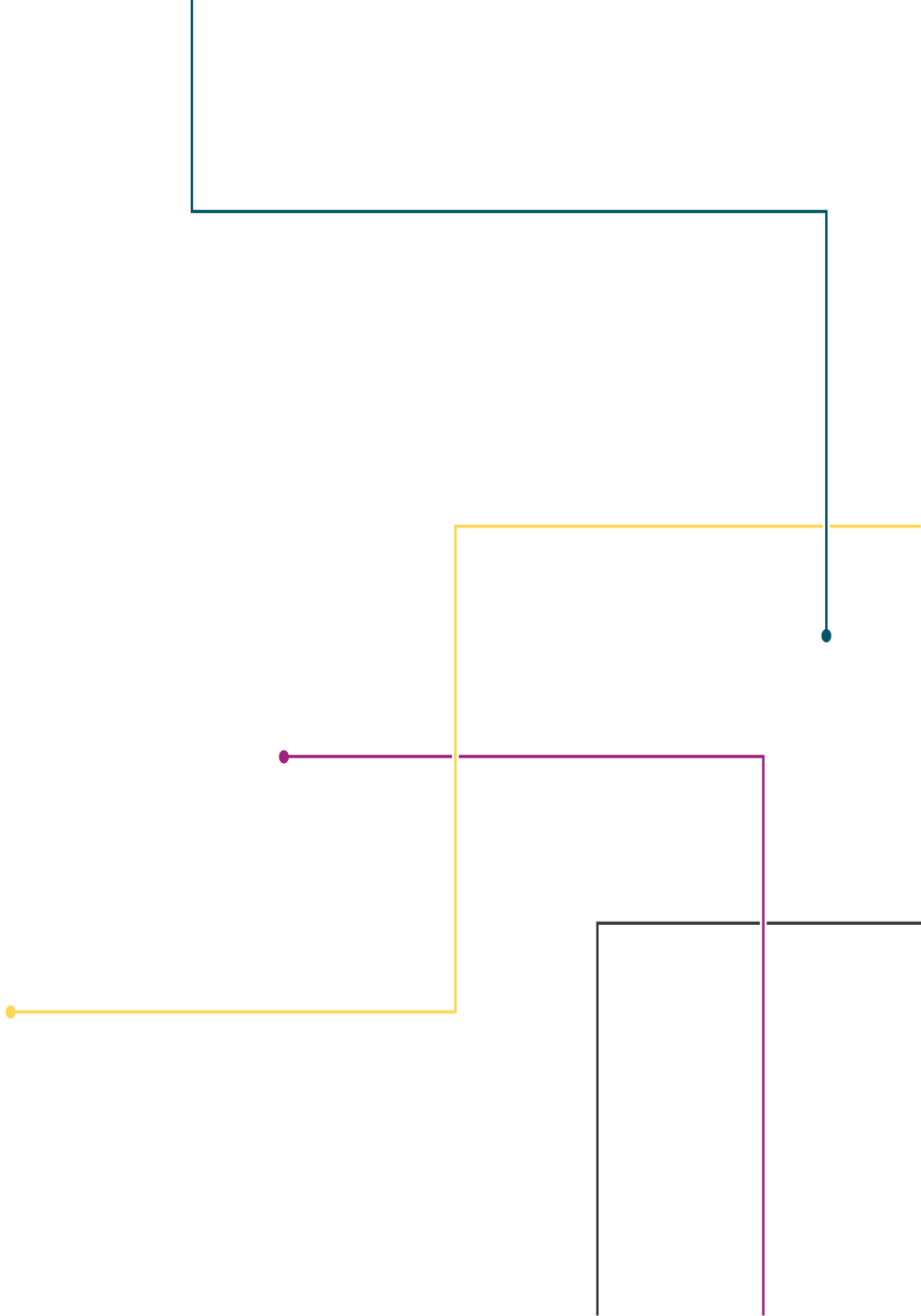
You get all threat management technologies in a single platform

You get proven AI platform



QUESTIONS?

Thank you!



VIRGINIA
IT AGENCY

UPCOMING EVENTS

ISO KNOWLEDGE SHARING WEBSITE

The ISO knowledge sharing website is a Sharepoint site where information security officers (ISO) and auditors can network and discuss current challenges facing their agencies. It also allows other agencies to learn how resolve these issues by brainstorming solutions together.

The link to the website:
https://covgov.sharepoint.com/sites/VITASec/ISOKnowledgeSharing/SitePages/Home.aspx

To request access to this website, contact:
Commonwealthsecurity@vita.virginia.gov

CYBERSECURITY AWARENESS MONTH 2021

CYBERSECURITY AWARENESS MONTH 2021

Cybersecurity Month is fast approaching! 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

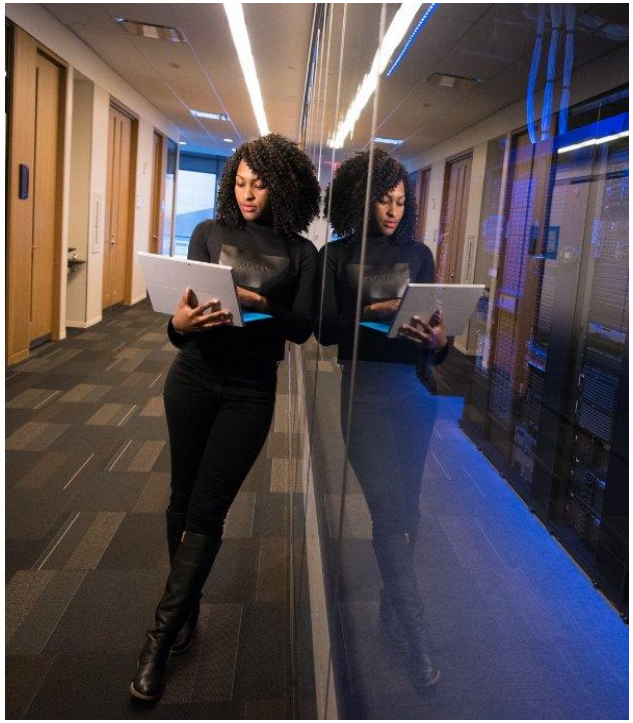
Explore how cybersecurity and staying safe online is increasingly important as our world continues to operate virtually for so much of work and play.

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

CYBERSECURITY AWARENESS MONTH WEBINAR



htttps://register.gotowebinar.com/register/2593840704767229967

VIRGINIA IT AGENCY

AUGUST ISOAG MEETING DETAILS

Date: August 4, 2021
Time: 1- 4 p.m. WebEx

Agenda

Bill Fitzpatrick
Beth Waller
Nick Christensen
Darrell Raymond & Eric Culbertson

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!