SBIR/STTR CS Due Diligence CPG Solutions Webinar

DOE/Office of Science

06 November 2024

U.S. Department of ENERGY

Office of SBIR/STTR Programs

Webinar Agenda

- SBIR/STTR CS Requirement
- Presentations
  - Microsoft - Software as a Service (SaaS) Provider
  - Google – Software as a Service (SaaS) Provider
  - Rikkin - Managed Security Service Provider (MSSP)/Manage Service Provider (MSP)
  - LMNTrix - (MSSP)
  - Blackbelt Secure - (MSSP)
  - BIZ-FOCUS - Information Technology (IT) Consultant/MSP
- Q&A Session (~ 30 minutes)

SBIR/STTR CS Requirement

- Prevent the unauthorized disclosure of sensitive data/intellectual property to foreign countries of concern: China, Russia, North Korea, and Iran.
- SBIR/STTR CS Self-Assessment is required for SBIR/STTR Applicants/Awardees to complete
- A subset of CISA's Cybersecurity Performance Goal Checklist
  - CS Due Diligence
    - URL: https://science.osti.gov/sbir/Foreign-Risk-Management/Cybersecurity-Due-Diligence-Program
    - Link: SBIR Introduction to Cybersecuri… | U.S. DOE Office of Science(SC)
  - CPG Implementation Guidance (under Learning and Resource)
    - URL: https://science.osti.gov/SBIR/Foreign-Risk-Management/Cybersecurity-Due-Diligence-Program/Learning-and-Resources/Implementation-Guidance
    - Link: SBIR Implementation Guidance for… | U.S. DOE Office of Science(SC)
  - To clarify, the presentation today is for informational purpose only and DOE SBIR/STTR Program does not require or recommend that small businesses employ any of the services to fully implement the CPGs.

SBIR/STTR CS Requirement

- 2.L Secure Sensitive
- 2.E Separate User and Privileged
- 2.D Revoke Credentials
- 1.B Organizational CS Leadership
- 2.I Basic CS Training
- 1.A Asset Inventory
- 2.A Change Default Passwords
- 2.R System Backups
- 2.B Minimum Password Strength
- 2.H Phishing MFA
- 2.W No Exploitable Services
- 2.G Detection of Login Attempts
- 2.K Strong and Agile Encryption
- 2.M Email Security
- 2.S Incident Response Plan
- 4.A IR Reporting

Presentation: Software as a Service/Cloud Services

- Software as a Service (SaaS) Provider
  - Services found on the cloud: Office 365, One Drive, Workspace, Google Drive, etc.
  - These services have security features that can be enabled to assist small businesses with keeping the sensitive information/intellectual property secure
    - Presenter: Mr. Chuck Ladd
    - Presenter: Mr. David Harris and Mr. Zach Walker

Microsoft Security

Microsoft 365 / SBIR-STTR Cybersecurity Performance Goals (CPGs)

Chuck Ladd
Security Specialist
cladd@microsoft.com

U.S. Department of ENERGY

Office of SBIR/STTR Programs

Summary of M365

See M365 Maps for differences between E3/G3 & E5/G5

PRODUCTIVITY

M365 Apps for Enterprise
Office suite of apps on up to 5 PCs & Macs

Mobile Office Apps
Office Apps for Tablet & Smartphones

Office on the Web
Office Apps in the browser

Windows 10/11 Enterprise – per user

Viva Insights (My Analytics)
Individual and team effectiveness

Forms
Create forms for surveys, feedback, etc.

Planner
Create plans, assign tasks

Bookings
Appointment Scheduling

To Do
Task Management

MS Search
Search across M365

COLLABORATION

Exchange
Business-class email & Calendar

OneDrive
Cloud Storage and file sharing

SharePoint
Team sites & internal portals

Teams
Persistent chat-based collaboration; Meetings, Live Events, Webinars

Audio Conferencing
Limited

Stream
Video Repository

Yammer:
Private social networking

SECURITY

Anti Virus
Signature based AV/AS

Data Loss Prevention
Prevent sensitive data leaks

eDiscovery (Basic)
Discovery content across email, docs, IM, social.

Entra ID P1
SSO, MFA, Conditional Access, Reporting

Endpoint Management
Intune, MDM, MAM, SCCM, Endpoint Protection

Information Protection
Encrypt and track all files

Adv Threat Analytics
Protection from advanced targeted attacks by applying user and entity behavior analytics

Secure Score
Assesses your current O365 security health

Compliance Management
Track compliance against regulatory requirements

E5 SECURITY

Defender for O365 (MDO):
Zero-day virus and malware protection

Adv Threat Intelligence
Global machine learning based threat detection and prevention; Enhanced data access controls (CLB)

Defender for Cloud Apps (MDCA)
Discover cloud-based apps, gain insight into shadow IT and assess risk.

Entra ID P2
Risk based conditional access, privileged Identity Management, identity protection

Defender for Identity (MDI)
End User Behavioral Analysis – Look for abnormalities in your environment

Defender for Endpoint (MDE)
End-point Detection & Response against zero-day malicious attacks

E5 COMPLIANCE

Information Protection & Governance
Cloud DLP (MCAS + new value)
Communications DLP (Teams chat)
Information Protection
Information Governance
Records Management
Rules-based auto classification
Machine Learning-based auto classification
Customer Key
Advanced Message Encryption

Insider Risk Management
Insider Risk Management
Communication Compliance
Information Barriers
Customer Lockbox
Privileged Access Management

Premium eDiscovery
Case Management, Custodian workflows

Premium Audit
Long term retention, advanced events

ANALYTICS

Power BI Pro
Live business analytics and visualization

Workforce Analytics
Team and Company wide effectiveness based on machine learning

VOICE

Audio Conferencing
Worldwide dial-in for your online meetings

Teams Phone:
Business phone system in the cloud

Utilize Microsoft Entra ID to meet CPGs

Conditional Access

Discover whether your organization is susceptible to known vulnerabilities and exploits. Prioritize risks and address vulnerabilities with guided recommendations

Multifactor authentication (MFA)

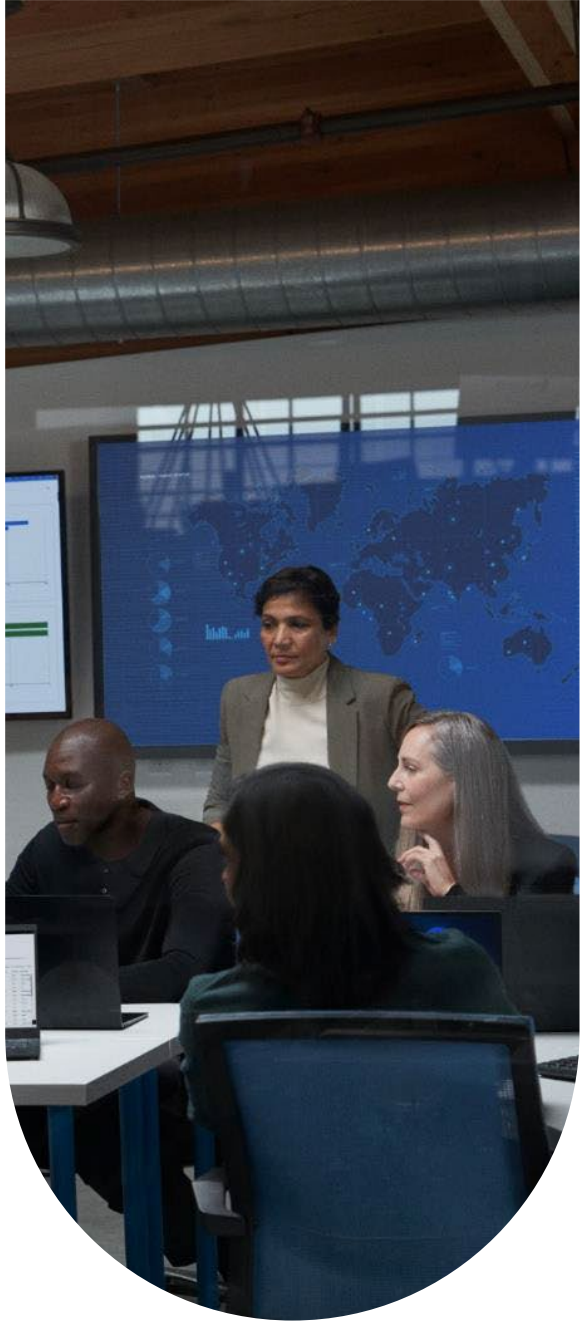
Multifactor authentication addresses 99.9% of identity attacks. Multifactor authentication protects your applications by using a second source of validation, (something they are and something they have) like a phone or token, to verify identity before granting access

Passwordless

Seamless Microsoft Entra ID user experiences start with passwordless authentication, ensuring users never have to touch or remember a password, thereby further breaking your exposure to your weakest security link

Single sign-on (SSO)

Connect your workforce to all your apps, from any location, using any device. Simplify app access from anywhere with single sign-on



Protect your data with industry-leading security

Reduce data breaches by 45% by consolidating identity management

Secure access to resources

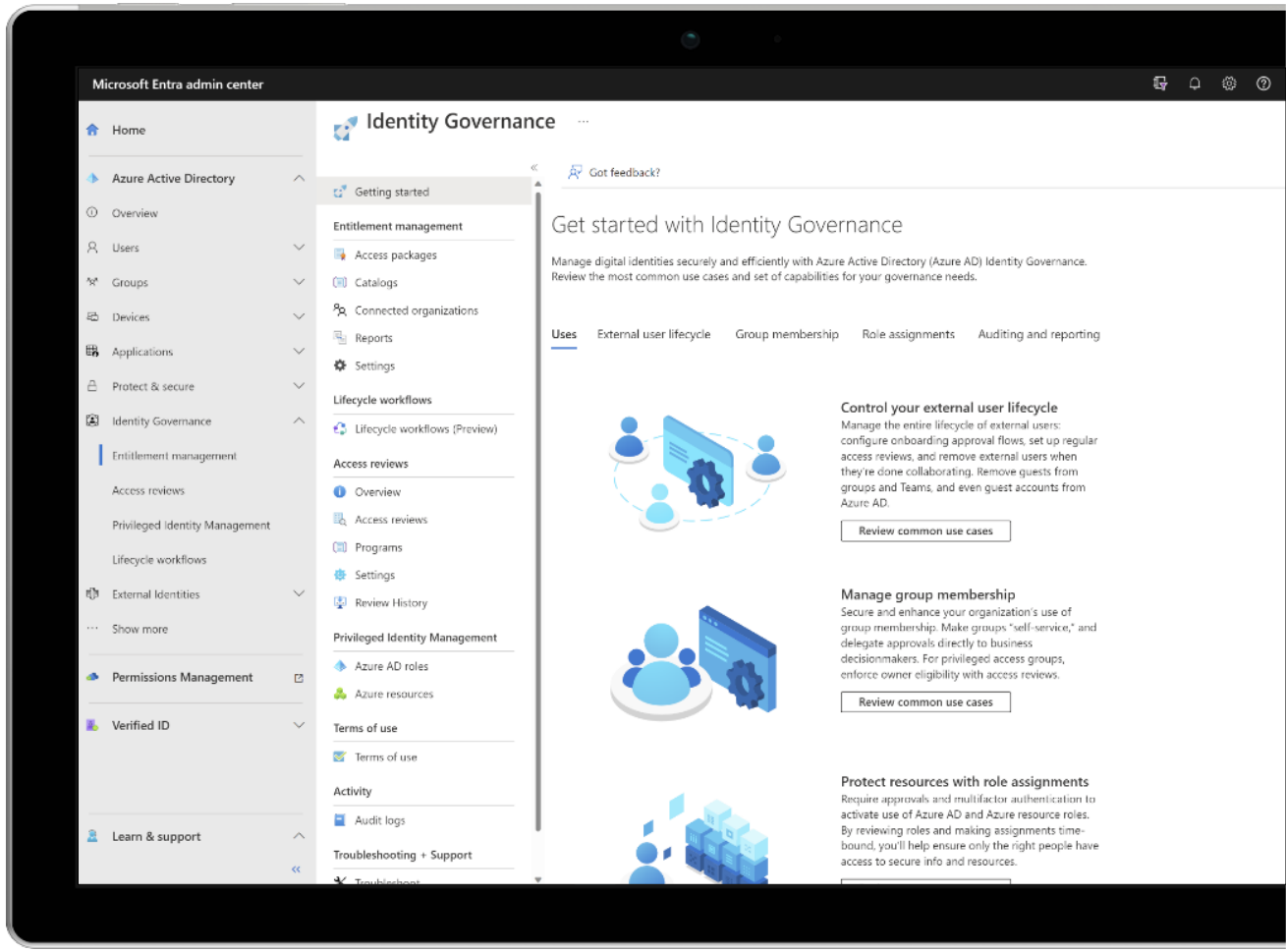
Protect access to resources using strong authentication and intelligent adaptive access

Protect against identity compromise

Intelligently detect and respond to compromised accounts using cloud-based AI and automation

Govern and manage access rights

Protect, monitor, and audit access to critical assets and ensure only authorized users have access



U.S. Department of ENERGY™ *Office of SBIR/STTR Programs*

Use Microsoft Defender XDR to meet CPGs

Build a unified defense with XDR

Cross-domain SOC experience

Hybrid identities

Endpoints and IoT

Email and collaboration

SaaS apps

Data

Cloud workloads

Prevent	Protect	Detect and respond	Extend
Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management	Automatically contain and remediate compromised assets	Use incidents to respond to cross-workload threats from a single portal Speed up response with an experience designed for SOC efficiency	Unified APIs and connectors

Supercharge your SOC with XDR

Enable rapid response with XDR-prioritized incidents

Remediate threats quickly with a complete view of the kill chain and prioritized investigation and response at the incident level

Disrupt advanced attacks at machine speed

Stop lateral movement of advanced attacks with advanced AI capabilities that automatically isolate compromised devices and user accounts

Transform SOC productivity with generative AI

Respond to cyberthreats faster with step-by-step guidance, empower any analyst to build queries in natural language, and reverse-engineer adversarial scripts in seconds

Unify security and identity access management

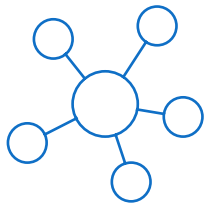
Protect your hybrid identities and identity infrastructure from credential theft and other threats with seamless integration of Microsoft Entra ID and XDR

U.S. Department of ENERGY™ *Office of SBIR/STTR Programs*

Encryption options in Microsoft 365

Data in-transit

Network



TLS

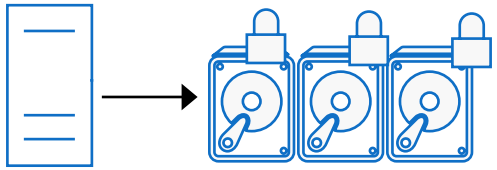
Content

Emails,
Documents

Office 365 Message Encryption
Office 365 Advanced Message Encryption

Data at-rest

Hardware

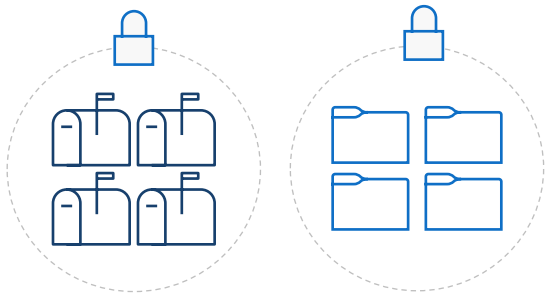


Windows Server

Disk

BitLocker

Application



Exchange Online Mailboxes*

SharePoint and OneDrive Files

Customer Key
Microsoft Managed Key

U.S. Department of ENERGY

Office of SBIR/STTR Programs

How does MIP and OME help with CPGs?

Microsoft Information Protection and Office 365 Message Encryption provide **persistent encryption** on documents and emails

Access to the encrypted document/ email is granted based on the user's identity

- This allows the Admin to enable gated access to sensitive data
- This allows the Admin to limit access to sensitive data

Access to the encrypted document/ email can also be monitored and revoked

- This allows the Admin to audit who has access to the document
- This allows the Admin to audit who has *previously accessed* the document
- This allows the Admin to control future access to the document

Asset Management with Microsoft Intune

Modern endpoint management powered by the Microsoft Cloud

Simplify and consolidate endpoint management

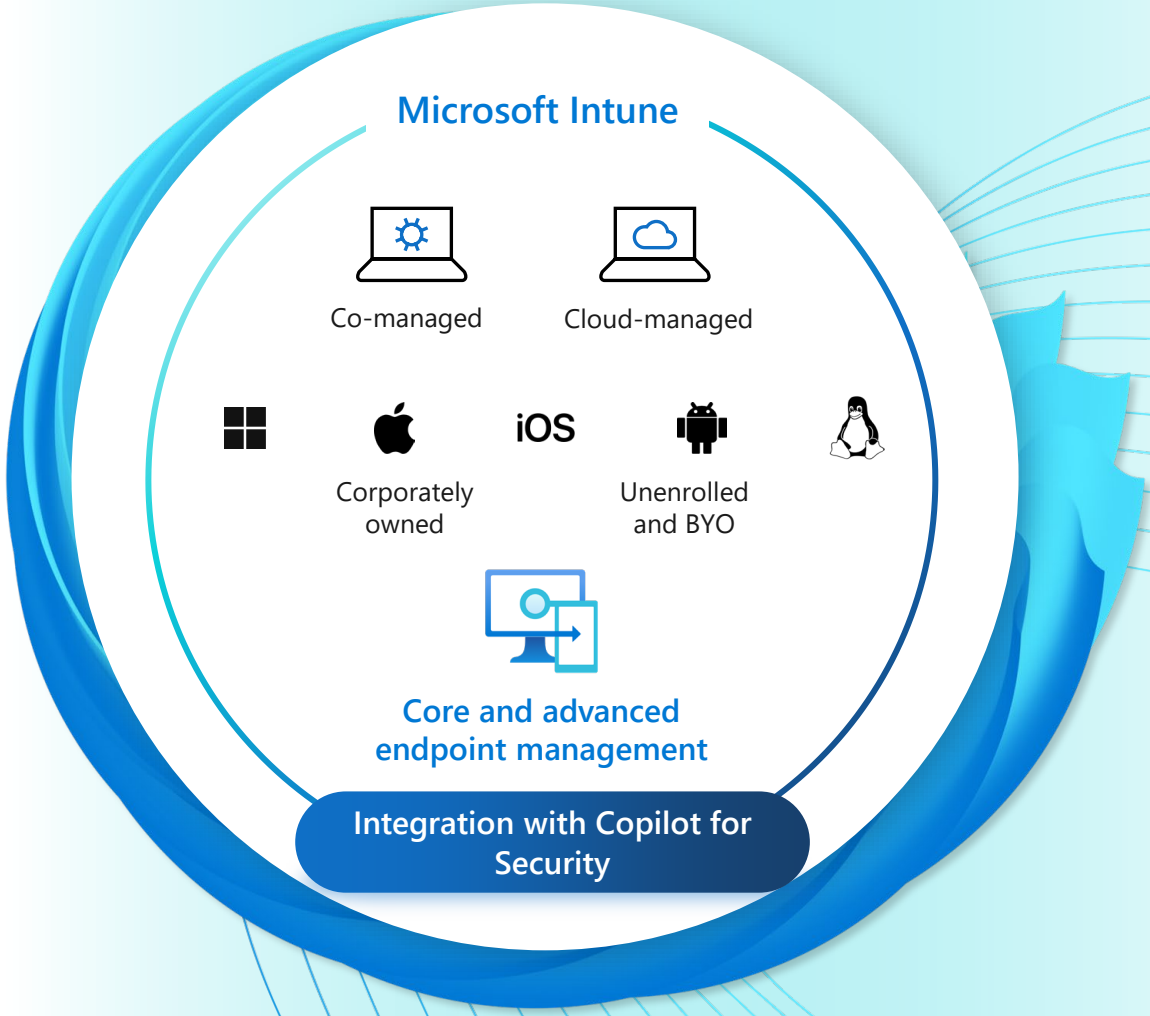
Cut cost and complexity by shifting to the cloud, unifying endpoint management and security tools in one place.

Fortify Zero Trust security

Mitigate threats and improve compliance across all devices by protecting users, devices, apps, and data.

Increase satisfaction

Proactively manage better user experiences while driving operational efficiency with AI and automation.



U.S. Department of ENERGY™ Office of SBIR/STTR Programs

Microsoft

Thank you

U.S. Department of ENERGY

Office of SBIR/STTR Programs

Key Takeaways

- CPGs Addressed
- Solutions Presented

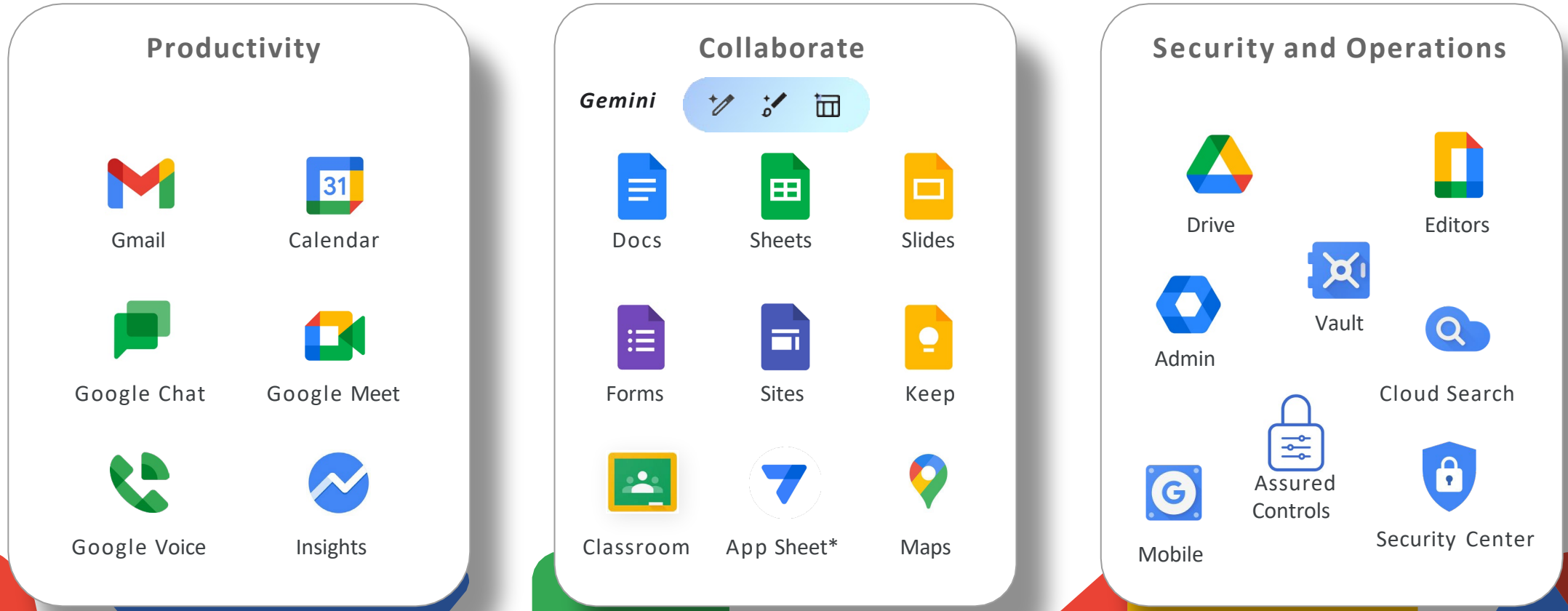
ATX DEFENSE | Google Cloud

CMMC for DoE Small Businesses

November 6, 2024

For detailed information about Google Workspace and CMMC, please visit https://cmmcguide.atxdefense.com or email us at cmmc@atxdefense.com

What is Google Workspace?



What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is the standard for cybersecurity across the 300,000+ DoD contractors that compose the Defense Industrial Base.

CMMC is how contractors will demonstrate their ability to protect sensitive government information by implementing security controls. The mandate to protect this information has been in effect since 2017 but unenforced.

For many contractors, CMMC implementation will be validated by a third party. **Proof of CMMC compliance will become mandatory for winning or renewing Federal contracts.**

This is why we have CMMC

ATX DEFENSE

Will CMMC Apply to my DoE Contracts?

CMMC is effective for DoD on December 16, 2024…
But it's coming for ALL Federal contracts, including those in DoE.

From the proposed rule in the Federal Register:
"This rule will apply the Controlled Unclassified Information (CUI) program requirements in Federal contracts in a uniform manner to protect CUI."

What is the most likely timeline?
November 2024 - Proposed Rule released for comments
Summer-Fall 2025 - Final Rule released (goes into effect 60 days later) Fall-Winter 2025 - Final Rule goes into effect
2026 - Federal contracts start including cybersecurity requirements to protect CUI

Secure Enclaves are the Best Option for CMMC

The CMMC Final Rule, released 15 October 2024, clarifies that devices connecting to virtualization solutions are out-of-scope for CMMC.

This makes virtualized solutions accessible from **any** device, including unmanaged BYOD.

"There are no documentation requirements for out-of-scope assets." (p. 448)

b. Virtual Desktop Infrastructure

Comment: Several comments requested clarification on the use of Virtual Desktop Infrastructures and how to scope its components.

Response: The rule has been updated in table 3 to § 170.19(c)(1) and table 5 to § 170.19(d)(1) to state that an endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of FCI and CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered out of scope.

CMMC Final Rule, p. 165

“It Saved Lives” - Google Workspace is Proven in Crisis

Google Docs’ real-time collaboration features facilitated the evacuation of over 124,000 from Hamid Karzai Int’l Airport in Kabul, Afghanistan when DoD Office 365 couldn’t meet the need.

How airmen used a single Google Doc to save thousands of lives during the Afghan airlift

“The chaos and hecticness of everybody trying to get in and get their evacuees out now became a smoother process.”

BY DAVID ROZA | PUBLISHED JAN 16, 2023 9:30 AM EST

TASK & PURPOSE

”It saved lives” - Col Gregory Cyrus, 621st Contingency Response Group Commander

ATX DEFENSE

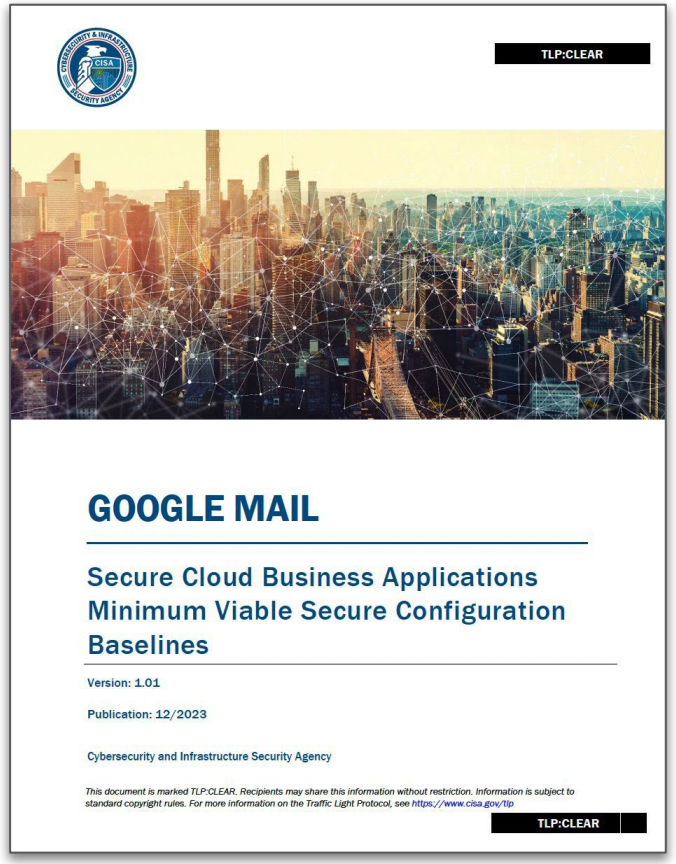
Secure Workspace with CISA Baselines

Cybersecurity and Infrastructure Security Agency (CISA) has Federal security baselines for Google Workspace.

ATX Defense developed additional baselines beyond CISA's recommendations to fully meet CMMC requirements.

Microsoft resellers charge up to $40k to implement CMMC controls in GCC High, but ATX Defense implements Workspace controls **at no cost** for managed services customers because it's the right thing to do.

You can do it yourself for FREE with our CMMC Guide for Google Workspace: https://cmmcguide.atxdefense.com



CISA Secure Baseline for Google Workspace

ATX DEFENSE

CMMC Space: A Better Way for Small Businesses

CMMC Space expands ATX Defense's commitment to security and transparency by providing the first turnkey Virtual Desktop Infrastructure (VDI) solution built around Google Workspace for CMMC.

CMMC Space is a complete CMMC Level 1 solution with **all required documentation and Google Workspace configuration** for $49/user/mo (plus the cost of Workspace) with a month-to-month commitment.

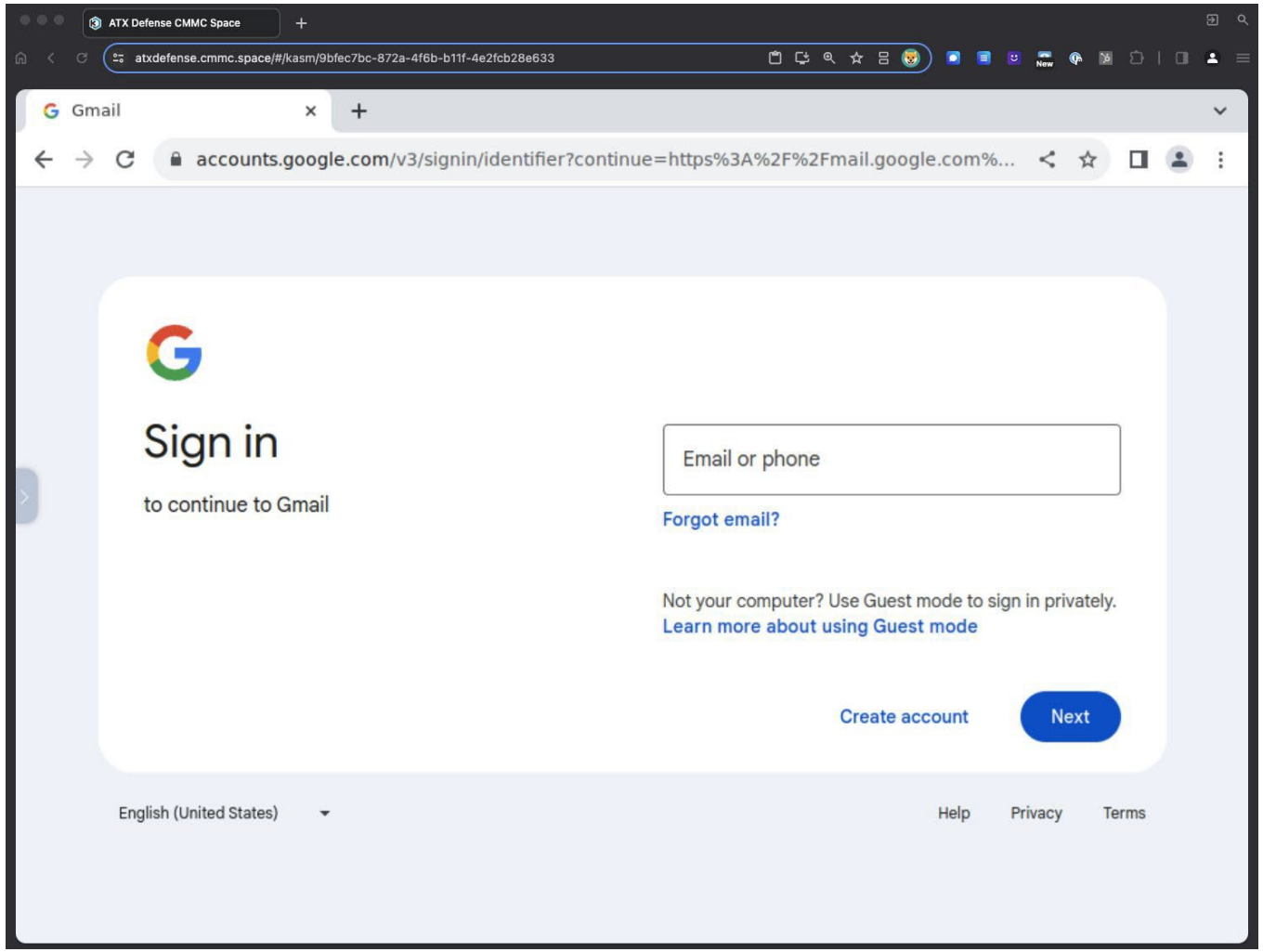
Level 1 customers can easily upgrade to Level 2 for CUI and ITAR compliance when needed.

Google Workspace with CMMC Space	
CMMC Space Level 1 (FCI)	$49/usr/mo
CMMC Space Level 2 (CUI)	$99/usr/mo
Google Workspace Enterprise Plus	$36/usr/mo or $360/usr/yr
Google Workspace Assured Controls Plus	$360/usr/yr *Optional: ITAR*
Technical Support	Included
All CMMC Documentation	Included
Google Workspace CMMC Configuration	Included
First-year Level 2 Cost for 5 Employees	**$7,740**

Microsoft GCC High with VDI Solution	
Level 2 (CUI) Virtual Desktop Solution	$3600/usr/yr
Microsoft GCC High	$1150/usr/yr
Technical Support	$96,000/yr
All CMMC Documentation	$45,000
Microsoft GCC High CMMC Configuration	$40,000
First-year Level 2 Cost for 5 Employees	**$204,750**

ATX DEFENSE

CMMC Space: Google Workspace with a Secure Browser



CMMC Space is a simple virtualization solution accessible from within any modern browser.

CMMC Space provides a hardened Google Workspace and secure Chrome browser managed by ATX Defense.

Our managed service supports all 320 of the CMMC Level 2 assessment objectives.

ATX DEFENSE

CMMC Space Shared Responsibility Matrix Summary

	Controls		Objectives	
	Workspace Only	CMMC Space	Workspace Only	CMMC Space
Customer Responsibility	105	0	312	3
ATX Defense Responsibility	N/A	93	N/A	286
Shared Responsibility	N/A	6	N/A	6
Inherited from Google	5	11	8	25

CMMC Level 2 has a total of 110 Controls composed of 320 Assessment Objectives

Controls are detailed in NIST SP 800-171.

Assessment objectives are detailed in NIST SP 800-171a.

ATX DEFENSE

ATX DEFENSE

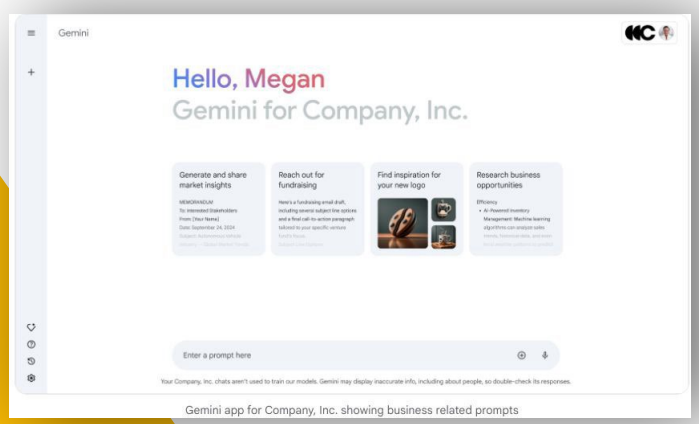
Thank You

Selected NAICS 541611 541519 541613 | CAGE 8U9V5 | UEI H6YBMH9MN3D3 | SBC ID 002105877 | cmmc@atxdefense.com

Add on Services *Included* with Workspace

NotebookLM.google.com (Blog) Add on Service ~ Be an interactive expert in your trusted sources:

- Once you upload source documents (e.g. Google Doc and Slides, PDFs, web URLs, copied text) into a notebook, you can ask NotebookLM questions about the information in your sources.
- It will respond with an answer from the sources you've uploaded along with inline citations from those documents to show you what NotebookLM based its answers on.
- NotebookLM can also be used to generate a variety of content based on your sources, like summaries, briefing docs, timelines, FAQs, study guides or even audio overviews (Podcast, a new feature that lets you listen to a conversation about your source).



Gemini app for Company, Inc. showing business related prompts

Gemini.google.com (Blog) with 1.5 Flash ~ With enterprise-grade data protections and compliance

- Multimodal Understanding with Image and Text Processing: Allowing you to analyze photographs, documents, infographics, and screenshots. It can answer questions related to the content and identify objects within images. It can extract information from various visual content like charts, tables, and web pages, making it useful for research and data analysis.
- High-Volume Tasks: Flash is optimized for tasks where speed and cost-effectiveness are crucial, such as summarization, categorization, and answering simple questions.
- Content Generation with structured outputs to generate responses in structured formats like HTML and JSON, which is helpful for creating web content or organizing data. It can infer new information and make connections between different pieces of information to create content for proposals, market research, and day to day …need something here
- Captioning and Descriptions ability to generate detailed captions and descriptions for images and videos

Key Takeaways

- CPGs Addressed
- Solutions Presented

Presentation: Managed Security Service Provider/ Managed Service Provider

- Managed Security Service Provider (MSSP) is a third-party provider that manages and monitors a small business' systems and devices (i.e. firewalls, virus protection, and intrusion detection) and ensures access is only for authorized personnel. The MSSP focuses on providing network security and IT safety.
- Managed Service Provider (MSP) is a third-party provider that general IT support and services for small businesses that **do not have their own IT departments**. Some MSPs manage the overall IT infrastructure allowing the small business to have more operational control over their IT systems.

    - Rikken: Rick Moore
    - LMNTrix: John Minasyan
    - Blackbelt Secure: Peter Varosky

Key Takeaways

- CPGs Addressed
- Solutions Presented

RIKKIN

ACHIEVING CPG COMPLIANCE

PROVEN STRATEGIES AND INTEGRATED SOLUTIONS FOR GRANT APPLICANTS

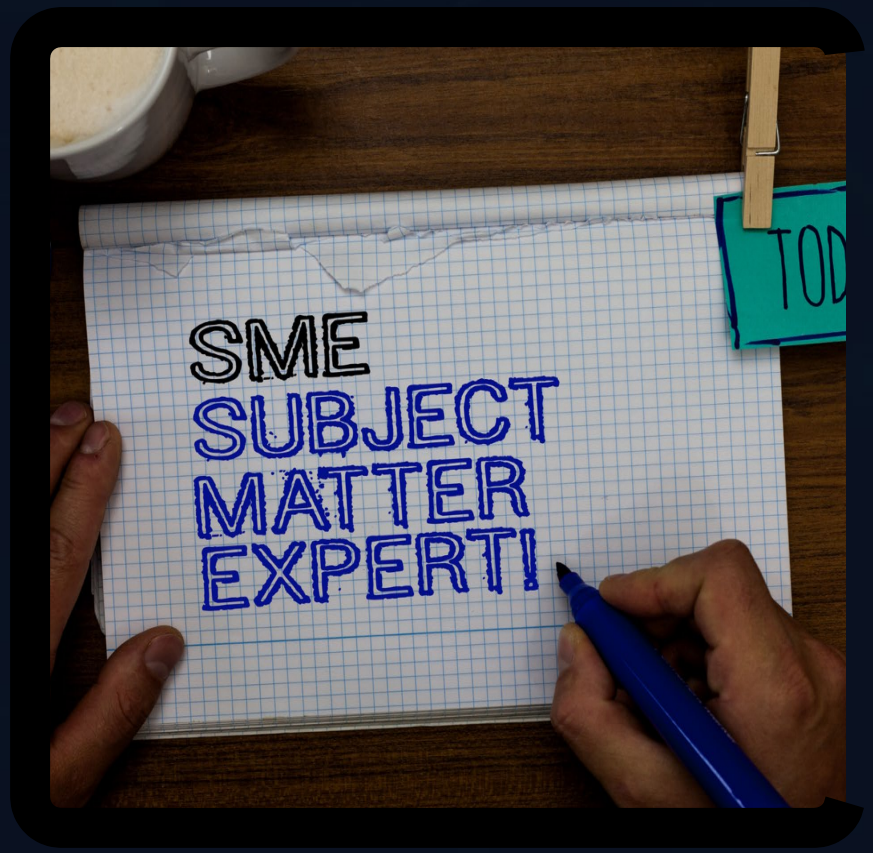
HTTPS://RIKKIN.COM

RIKKIN

PRESENTED BY OUR: CHIEF TECHNOLOGIST & CISO

Seasoned IT and cybersecurity professional with over 35 years of experience in the data processing and IT industry, holding 40+ industry-recognized certifications, including multiple CCIEs (R/S, VoIP, Sec), CISSP, PMP, MCSE, MCNE, HPUX, RHCA, AWS CSA, Azure SAE, and VCP-DCV. Extensive background in federal compliance and auditing, with over 20 years specializing in regulatory standards like FDIC, HIPAA, PCI DSS, and NIST SP 800-171.

Known for a comprehensive approach to compliance and security, leveraging a depth of technical expertise to guide organizations in meeting rigorous standards, implementing best practices, and ensuring robust, compliant infrastructures.



RIKKIN

2.L - SECURING SENSITIVE DATA

HTTPS://RIKKIN.COM

WHY IS SECURING SENSITIVE DATA IMPORTANT ?

A data breach poses risks that go beyond technical issues—it can have long-lasting impacts on every aspect of your organization. Such an incident could result in the loss of valuable intellectual property, potentially endangering your relationship with the DOE. The reputational damage from such incidents is often devastating, eroding trust and confidence in your organization and impacting future opportunities.

BEST PRACTICES

At Rikkin, it is standard practice to secure data by separating user and privileged accounts, controlling access based on employee hierarchy through IAM settings. Additionally, when an employee departs, their credentials are promptly revoked and audited to ensure they no longer have access to any company data.

RIKKIN

1.B ORGANIZATIONAL CS LEADERSHIP

HOW DO YOU CHOOSE THE RIGHT CS LEADERSHIP PERSON?

For DOE SBIR/STTR Self-Assessment Requirement 1B, which focuses on organizational cybersecurity leadership and the identification of personnel to fulfill these roles, requiring a well-defined cybersecurity leadership structure and outline the qualifications of the personnel responsible for overseeing cybersecurity within your organization.

Here's a few key areas where Rikkin can help;

- Identifying Potential CS Leaders and their Roles
- Outline Cybersecurity Responsibilities and Initiatives
- Develop Continuous Improvement and Training Programs
- Provide Virtual or Fractional CISO Services

RIKKIN

2.1 BASIC CS TRAINING

The SANS 2024 Security Awareness Report highlights Social Engineering as a key challenge in security awareness training (SAT). As 89% of practitioners reported that social engineering, including phishing (email), smishing (text), and vishing (voice), represents the greatest human risk in cybersecurity today.

Rikkin will works with organization worldwide, providing the Cybersecurity training that meets and exceeds DOE requirements. Through integrating educational services that are easy for your employees to use, we make it easier for your organization to enhance its cybersecurity posture without straining resources.

1.A ASSET INVENTORY

Asset inventory is a crucial yet complex component of cybersecurity that indirectly influences overall security through its relationship with risk management and permissions assessment.

Together, these three elements—asset inventory, risk management, and permissions assessment—serve as a failsafe to prevent employees from accessing, installing, or logging into unauthorized hardware, software, or services on the company network. By maintaining a clear and controlled asset inventory, organizations can significantly enhance their cybersecurity posture.

RIKKIN

2.A CHANGING DEFAULT PASSWORDS

EVERY DEFAULT PASSWORD WILL NEED TO BE CHANGED, BUT WHY?

Changing default passwords is one of the strongest defenses a company can implement against brute force attacks. These attacks account for over 5% of confirmed security breaches. By updating default passwords, organizations significantly reduce the risk of unauthorized access, preventing malicious actors from exploiting default credentials associated with privileged accounts. This simple yet effective measure ensures that attackers cannot easily pair an employee's username with a known default password, bolstering overall security and safeguarding sensitive information.

BEST PRACTICES

Implementing tools like, Microsoft Intune and Entra ID offers several flexible options for enforcing mandatory password changes, allowing us to tailor the approach to best suit your organization's specific needs. These tools enable us to establish policies that enhance security while ensuring that the password management process aligns seamlessly with your company's operational requirements.

RIKKIN

2.R SYSTEM BACKUPS

Ransomware is one of the most daunting threats in cybersecurity today, capable of inflicting severe financial losses, irreparable damage to your organization's reputation, and exploitation of your employees. The ramifications of a ransomware attack can extend beyond immediate costs; they can lead to the loss of valuable intellectual property and, ultimately, the collapse of your entire business.

Implementing robust cloud-based system backups not only protects your data but also empowers your organization to swiftly recover from data breaches or outages. By ensuring that your critical information is regularly backed up in a secure, off-site location, you can minimize downtime and avoid the devastating consequences of a ransomware attack. This approach safeguards your assets and also reinforces your commitment to maintaining business continuity in the face of evolving cyber threats.

RIKKIN

EXPERTISE YOU CAN TRUST

Rikkin is a technology solutions engineering firm with a deep specialization in cybersecurity, dedicated to empowering you to focus on what you do best — DOE R&D. Our expertise in designing and implementing cutting-edge security solutions for organizations like yours is unmatched. We navigate the complexities of cybersecurity to deliver tailored strategies that protect your critical assets, reduce risk, and ensure resilience against evolving threats. By entrusting Rikkin with your cybersecurity needs, you gain a trusted partner committed to safeguarding your sensitive information, allowing you to drive your core operations forward with confidence.

HTTPS://RIKKIN.COM

RIKKIN

PLEASE HOLD ALL QUESTIONS UNTIL
AFTER PRESENTATIONS ARE COMPLETED...

THANK YOU

FOR MORE INFORMATION PLEASE CONTACT US

EMAIL: INFO@RIKKIN.COM
PHONE: 513-443-6646

HTTPS://RIKKIN.COM

Key Takeaways

- CPGs Addressed
- Solutions Presented

ACTIVE DEFENSE

ZERO HYPE | ZERO FALSE POSITIVES | ZERO EXCUSES

LMNTRIX

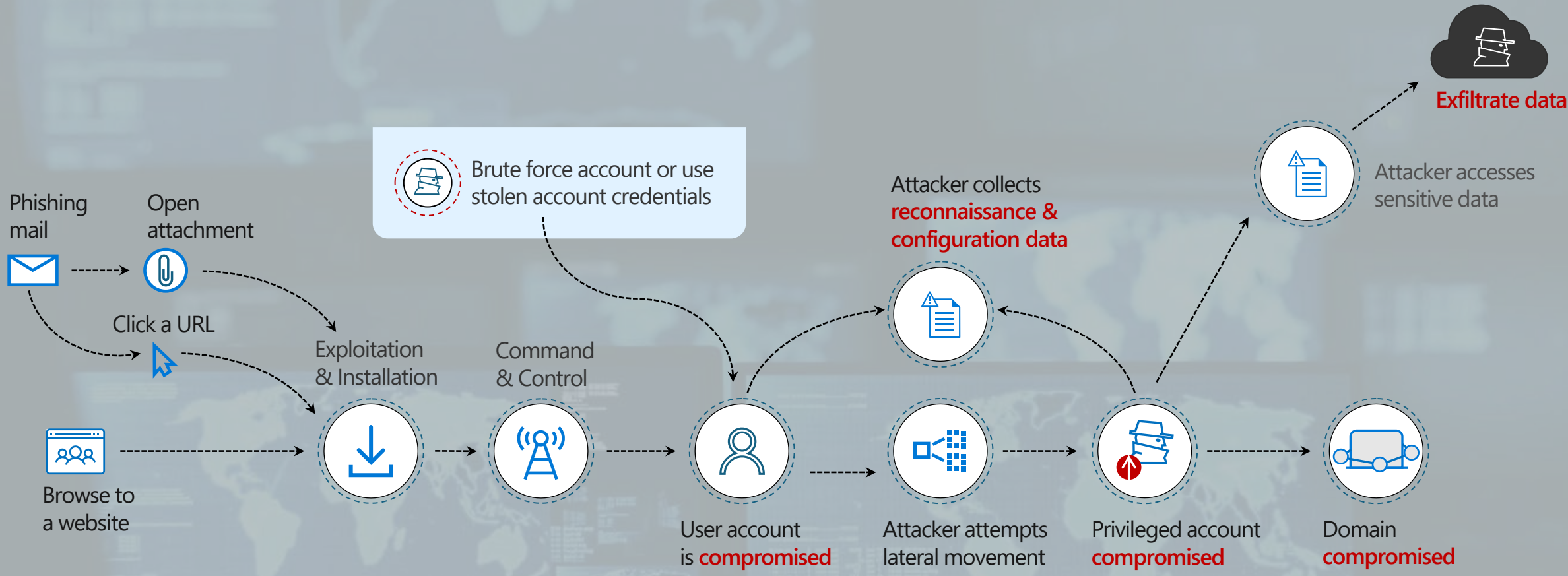
BE THE HUNTER | NOT THE PREY

John Minasyan
John@lmntrix.com

Fun Facts from 2024 DBIR Season

- Mandiant M-Trends 2023:
  - Median Dwell Time down from 16 days in 2022 to 10 days!
    - 6% of investigations identified activity that remained undetected for 1 to 5 years
  - Ransomware Increased to 23% of all incidents vs 18% in 2022
    - 70% of ransomed organizations discovered the breach via the ransom note
- Verizon 2024 Data Breach Investigations Report
  - Substantial increase in exploitation of vulnerabilities and zero-days to gain access (180% increase from 2022)
  - Software supply chain and cloud application vulnerabilities continued to climb as to prevalence in how threat actors got in (15% of breaches, an increase of 68% from 2022)

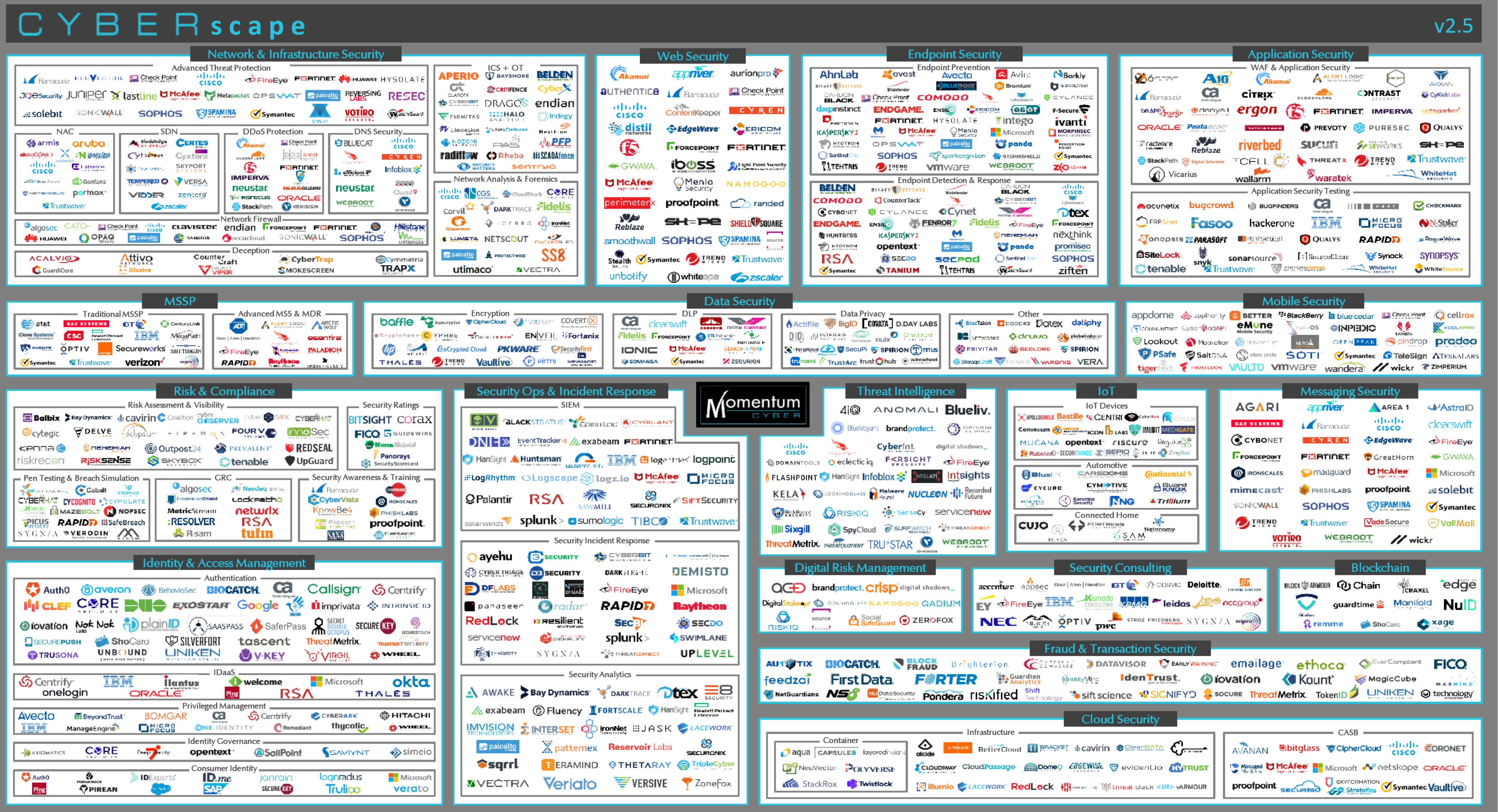
Cybersecurity Attack Progression



Problem – Cybersecurity is Massively Complicated

LMNTRIX

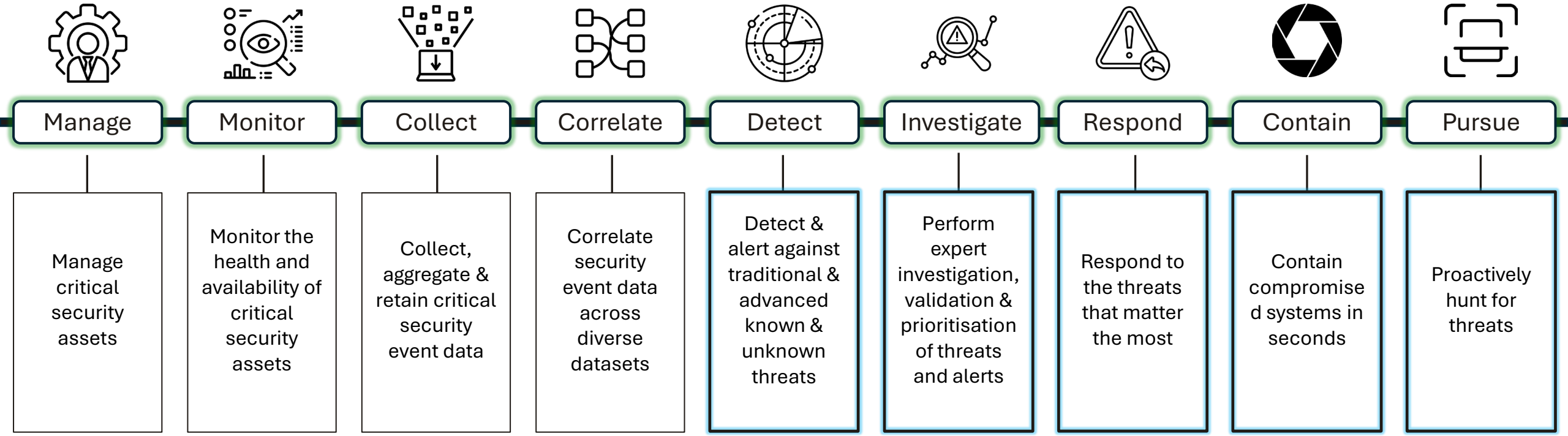
BE THE HUNTER | NOT THE PREY



BE THE HUNTER | NOT THE PREY

** Courtesy of Momentum Cyber

Managing The Entire Lifecycle Of An Alert



How LMNTRIX Can Help

- We provide the tools and service for 24/7/365 monitoring and response to cybersecurity threats

- Our Identity and Vulnerability Management services provide coverage for CPGs:

    - 2.L – Secure Sensitive Data
    - 2.E – Separate User and Privileged Accounts
    - 2.D – Revoking Credentials for Departing Employees
    - 2.W – No Exploitable Services on the Internet
    - 2.M – Email Security
    - 2.G – Detection of Unsuccessful Login Attempts
    - 4.A – Incident Reporting

- In addition, our service provides consulting and direction as to best practices on CPGs:
    - 1.A – Asset Inventory
    - 2.A – Change Default Passwords
    - 2.R – System Backups
    - 2.B – Minimum Password Strength
    - 2.K – Strong and Agile Encryption
    - 2.I – Cybersecurity Training
    - 2.H – Phishing Resistent MFA
    - 2.S – Incident Response Plans

Key Takeaways

- You are a key peg in the cybersecurity defenses of the government of the United States
- Attackers are adept and always probing – they will find the weakest link to exploit
- Identify your critical assets and data – practice rule of least privilege access
- Invest in immutable backup tools and backup your infrastructure and data
- Activate MFA on all connections
- Build visibility inside your perimeter defenses
- Seek a 24/7 monitoring service that will analyze telemetry, investigate alerts, and issue prioritized tickets

Key Takeaways

- CPGs Addressed
- Solutions Presented

BLACK BELT SECURE

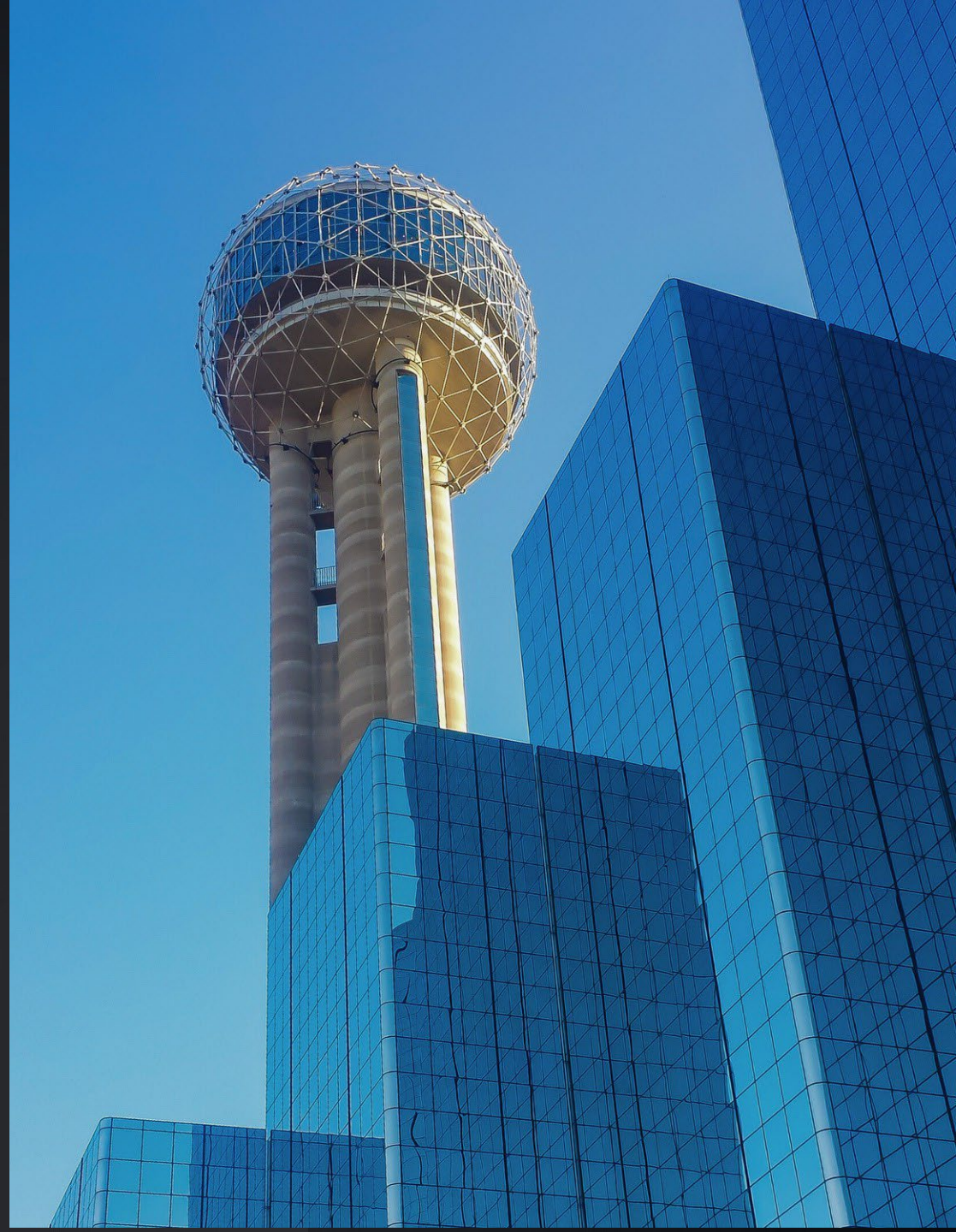
2024

MSSP PROVIDER SERVING TEXAS

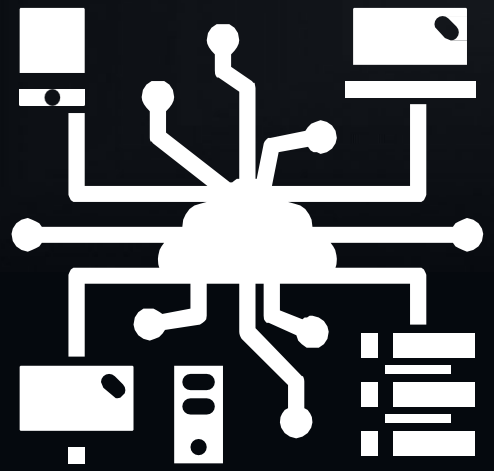
ABOUT US

Nationally award-winning cybersecurity solutions provider.

We are an award-winning managed security services provider (MSSP) based in the Dallas Fort Worth metroplex. We specialize in cybersecurity and infrastructure and have over 20 years of experience working for businesses small to large.



AREAS OF EXPERTISE



NETWORK & INFRASTRUCTURE

CYBERSECURITY

COMPLIANCE

2.A SP 800-53 Control(s): IA-5(1)	Change Default Passwords	Review password policy across organization, for user accounts, devices, infrastructure and IoT. Ensure enforcement.
2.L SP 800-53 Control(s): AC-23, IA-4	Secure Sensitive Data	Review data security measures on premises, cloud and remote. Provide instruction on securing devices from unauthorized access, and assist in implementing procedures to harden security measures.
2.E SP 800-53 Control(s): AC-2(7), AC-6(9), AC-6(10)	Separating User and Privileged Accounts	Review security accounts across the organization and document any weaknesses. Provide remediation steps to tighten access.
2.D SP 800-53 Control(s): AC-2(3), AC-2(1)	Revoking Credentials for Departing Employees	Ensure policies are in-place and being followed for departing employees.
2.R SP 800-53 Control(s): CP-9, CP-9(1), CP-9(3)	System Backups	Review DR Plan and ensure access to critical data is available onsite and remote.
2.B SP 800-53 Control(s): IA-5(1)	Minimum Password Strength	Review policies, enforce through AD/Entra and cloud systems.
2.W SP 800-53 Control(s): CM-7, CM7(4), CM-7(5)	No Exploitable Services on the Internet	Remote pentest. Review with security team and harden as necessary.

CPGs We Can assist with

2.K SP 800-53 Control(s): SC-8, SC-12	Strong and Agile Encryption	Review security encryption settings. Assist in deploying, hardening any that are weak.
2.I SP 800-53 Control(s): AT-1, AT-2	Basic Cybersecurity Training	Ensure policies are in-place and line with basic cybersecurity awareness training. Provide assistance as necessary to effectively deploy a program.
2.H SP 800-53 Control(s): IA-2(1), IA-2(2)	Phishing Resistant MFA	Review tools/systems in-place for MFA.
2.M SP 800-53 Control(s): AT-2, SC-13, SC-8	Email Security	Review email security settings. Test across environment and make recommended changes as necessary.
2.G SP 800-53 Control(s): AC-7	Detection of Unsuccessful (Automated) Login Attempts	Conduct audit on environment. Ensure systems are in-place to prevent threat actors and document.
2.S SP 800-53 Control(s): IR-1, IR- 2, IR-8, IR-9	Incident Response Plans	Review IR Plan. Test and update as necessary.

Let's Work Together

Peter Vavrosky

audit@blackbeltsecure.com

214-789-2607

Black Belt Secure

Key Takeaways

- CPGs Addressed
- Solutions Presented

Presentation: IT/CS Consultant

- Information Technology (IT)/CS Consultant is a subject matter expert regarding IT/CS and specializes in customizing short-term or project-based applications or configurations for businesses.
- Differences between IT/CS Consultant and MSP
  - MSPs provide long-term, ongoing IT support and Management.
  - MSPs engage continuously, to manage day to day IT needs.
  - BIZ-FOCUS: Ken Oporto


Biz-Focus

About Us

BIZ-FOCUS is an IT Consultancy focused on Accelerating Growth for Small Business & Startups

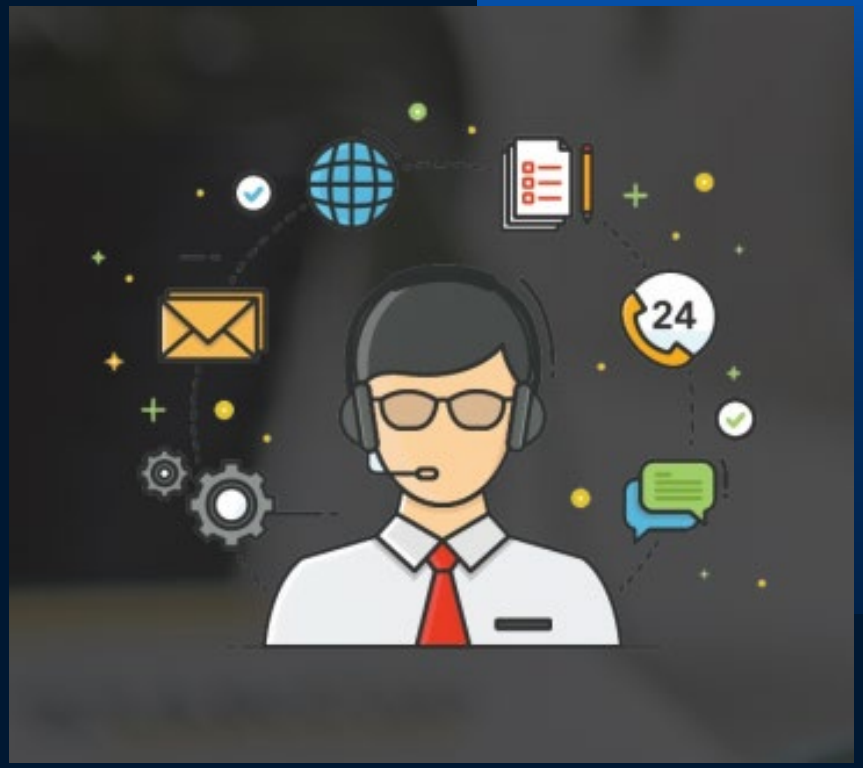
- Managed Networking, Infrastructure, Security
- Cloud Infrastructure, Dedicated & Virtual Servers
- Microsoft, Google, AWS Partnerships and Solutions
- Development Projects
- Staff Augmentation

BIZ FOCUS

Ken Oporto

Who?

- 25+ Years Experience in a wide variety of IT careers before establishing an MSP
- Deep Govt. Contracting experience as a technical lead across 14+ Federal/State agencies.
- 2 Lights Out fully automated datacenters built
- $1 Billion + in Contract Value won as a Chief Cloud Solutions Architect



(IT) Trades he is a Jack of 97%

(IT) Trades he is a Master of 0%

Pro Tip: No one is. Technology constantly evolves, and we do our best to adapt and keep up.

BIZ FOCUS

I have direct experience as the technical lead in a Startup past SBIR Award Recipient: I've been in your shoes.

- **Pressures are high, the future depends on qualifying and winning.**
- **Cyber Security requirements at this phase were recommended in the past, and now becoming more formalized. This will only increase every phase/year.**
- **Self Assertion is the start. The best teams prepare for whats ahead well in advance.**

Options :

Do it yourself if team resources and timelines allow. Utilize any available guidance to accelerate.

Offload the work to CS automation tools, Cybersecurity Experts and/or an MSP for a Done For You approach.

BIZ FOCUS

This CPG Assessment is the first step of many.

- Compliance with these 16 CPGs Gets you in the door
- 22 more gets you to the complete CISA CPG Checklist.
- 110+ Requirements to CMMC 2/3 and beyond.

16 CPGs
SBIR/STTR Baseline Requirements

38
Out of Total Requirements in CISA CPG Checklist

110+
CMMC Level 2 / 3

BIZ FOCUS

Securing the technology isn’t enough.

- Process-Driven requirements involve a technical component, but they emphasize processes, policies, and user behavior as much as—or more than—specific technical implementations. We address both with education and documentation.

- For the CISA CPG Checklist, resources represent up to 54 documents and 200-280 pages of process/policy/SOP documentation on average.

54+

Policies, Procedures, SOPs

200+

Pages

BIZ FOCUS

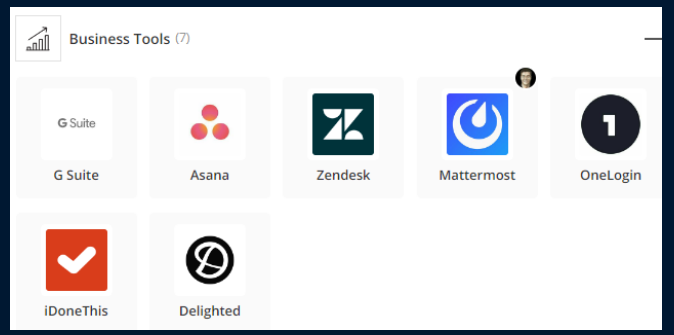
So how does an IT Consultant / MSP Help?

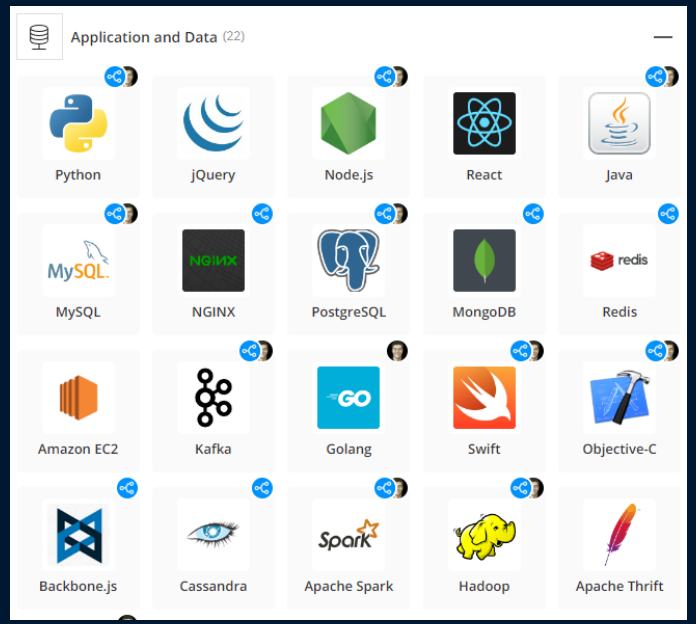
1. Consultation & Solution Review – A baseline survey

- We don't have fancy software and don't take the automated approach – we learn YOUR environment and tailor the guidance and materials to fast track your compliance.

- Hundreds of platforms secured – we have specific guidance (walkthroughs, scripts, docs) for 90%+.

- Review any existing documentation/policy and identify process gaps.



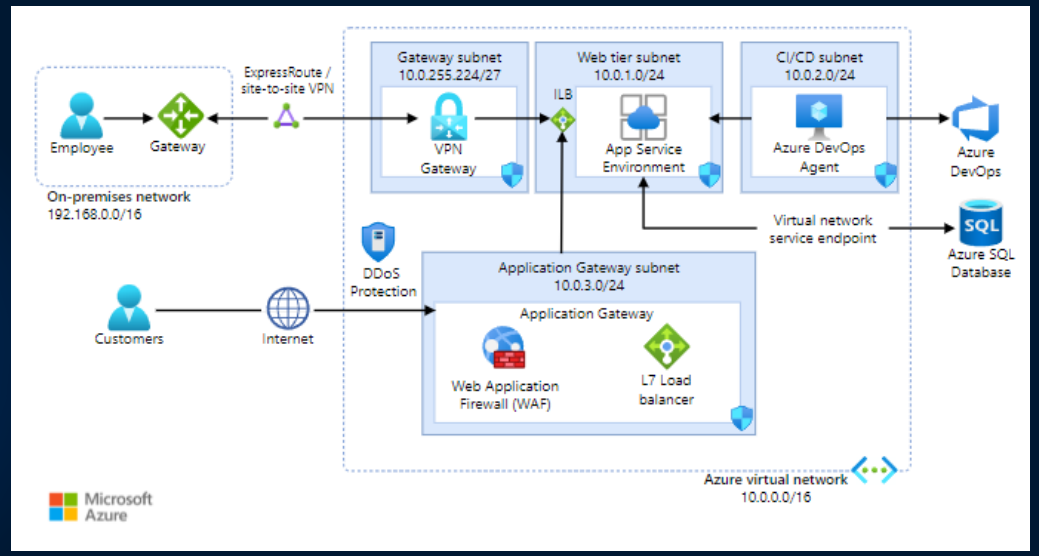


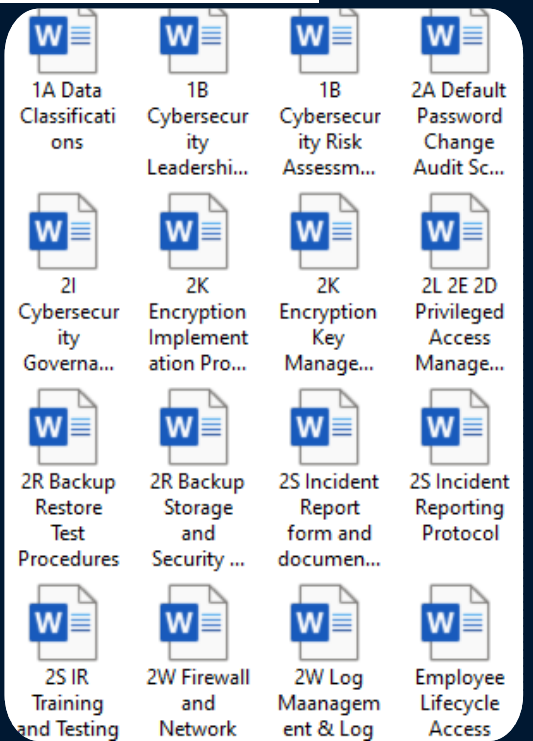
BIZ FOCUS

So how does an IT Consultant / MSP Help?

2. Implementation Guidance & Documentation Quickstarts

- Extended guidance and walkthroughs on configuration settings and policy changes
- Pre-built document outlines to rapidly populate associated company Policies, Standard Operating Procedures, and Incident Response handling documents.
- Vendor blueprints / architecture frameworks tailored to your stack and approach.





BIZ FOCUS

So how does an IT Consultant / MSP Help?

2. Implementation Guidance & Documentation Quickstarts

- **Example:** Covering CPGs for:
- Default password changes
- Role Based Access Control, Access Control Lists
- Data Encryption
- **In platform:** AWS
- Using Services: EC2, IAM, Redshift, RDS, S3

- Implement yourself with command line.
- Or Run our scripts (populated with your environment details already), to check, update, and monitor for changes.

```
aws iam change-password \
  --old-password <old-password> \
  --new-password <new-password>
```

```
aws redshift modify-cluster \
  --cluster-identifier <cluster-identifier> \
  --master-user-password <new-password>
```

```
aws rds modify-db-cluster \
  --db-cluster-identifier <cluster-identifier> \
  --master-user-password <new-password> \
  --apply-immediately
```

```
aws ec2 modify-security-group-rules \
  --group-id <security-group-id> \
  --security-group-rules <rules>
```

```
aws ec2 authorize-security-group-ingress \
  --group-id <security-group-id> \
  --protocol tcp \
  --port 22 \
  --cidr <trusted-ip-range>/32
```

```
aws iam update-account-password-policy \
  --minimum-password-length 12 \
  --require-symbols \
  --require-numbers \
  --require-uppercase-characters \
  --require-lowercase-characters \
  --allow-users-to-change-password \
  --max-password-age 90 \
  --password-reuse-prevention 5
```

BIZ FOCUS

So how does an IT Consultant / MSP Help?

2. Implementation Guidance & Documentation Quickstarts

- **Example:** Covering CPGs for:
- Network Boundary Security
- Role Based Access Control, Access Control Lists
- Data Encryption
- **In platform:** Azure
- Using Services: Network Security Groups, Storage Account, AZ Monitor, Blob / Storage Containers, Subnets

- Implement yourself with command line.
- Or Run our scripts (populated with your environment details already), to check, update, and monitor for changes.

```
az security pricing create --name VirtualMachines --tier Standard
```

```
az storage container immutability-policy create \
  --name <container-name> \
  --account-name <storage-account-name> \
  --resource-group <resource-group-name> \
  --period 30 \
```

```
az storage container create \
  --name <container-name> \
  --account-name <storage-account-name> \
  --public-access off
```

```
az storage logging update \
  --services bqt \
  --log rwd \
  --retention 7 \
  --account-name <storage-account-name>
```

```
az network nsg rule create \
  --resource-group <resource-group-name> \
  --nsg-name <nsg-name> \
  --name AllowSSH \
  --protocol Tcp \
  --priority 1000 \
  --destination-port-ranges 22 \
  --access Allow \
  --direction Inbound \
  --source-address-prefixes <trusted-ip-range>
```

```
az storage account update \
  --name <storage-account-name> \
  --resource-group <resource-group-name> \
  --encryption-services blob file table queue
```

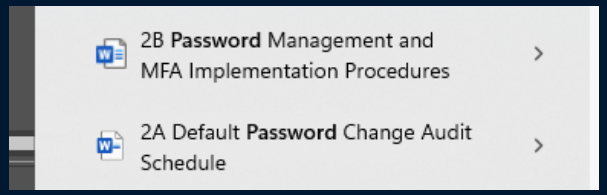
BIZ FOCUS

So how does an IT Consultant / MSP Help?

2. Implementation Guidance & Documentation Quickstarts

- **Example:** Covering CPGs for:
- Sensitive Data Access
- Role Based Access Control
- Data Encryption
- **In platform:** Windows / IIS / VPS
- Using Services: Active Directory, Windows Server, SMB

- Implement yourself with command line and MS Tools
- Or work with MSP to apply, update, and monitor.



- **Enforce Password Complexity:** Open Local Group Policy Editor:
  - `gpedit.msc` > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
  - Enable **"Password must meet complexity requirements"**
  - Set minimum password length, maximum age, and enforce password history.
- **Set Account Lockout Policy:** In the same section, configure **Account Lockout Policy** to prevent brute-force attacks.

- **Enforce Password Complexity**: Open Local Group Policy Editor:
  - `gpedit.msc` > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
  - Enable "**Password must meet complexity requirements**"
  - Set minimum password length, maximum age, and enforce password history.
- **Set Account Lockout Policy**: In the same section, configure **Account Lockout Policy** to prevent brute-force attacks.

What is the Security Compliance Toolkit (SCT)?

The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products.

The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active Directory or individually through local policy.

The Security Compliance Toolkit consists of:

- Windows 11 security baseline
  - Windows 11, version 24H2
  - Windows 11, version 23H2
  - Windows 11, version 22H2
  - Windows 11, version 21H2
- Windows 10 security baselines
  - Windows 10, version 22H2
  - Windows 10, version 21H2
  - Windows 10, version 20H2
  - Windows 10, version 1809
  - Windows 10, version 1607
  - Windows 10, version 1507
- Windows Server security baseline
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016

- **Set NTFS Permissions:**
  - Right-click the folder where Office is installed > **Properties** > **Security**
  - Restrict access by granting permissions only to administrators and authorized users. Remove unnecessary groups like **Everyone** or **Authenticated Users** if not required.
- **Restrict Macro Execution**: In PowerPoint Options:
  - **Trust Center** > **Trust Center Settings** > **Macro Settings**
  - Set macros to "Disable all macros with notification" or "Disable all macros except digitally signed macros."

BIZ FOCUS

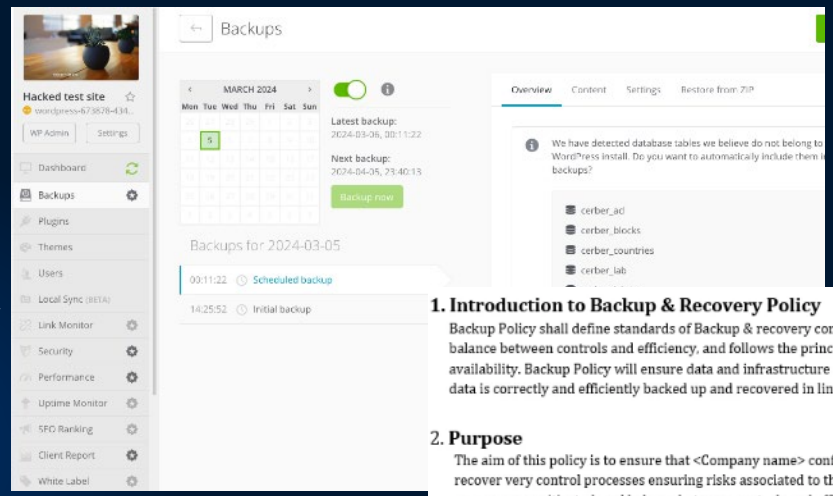
So how does an IT Consultant / MSP Help?

2. Implementation Guidance & Documentation Quickstarts

- **Example:** Covering CPGs for:
- Backup/Disaster Recovery
- Policies, Controls, and User Behavior

- **In platform:** Webserver, SaaS Website, M365

- Implement yourself or work with MSP to apply, update, and monitor.



1. Introduction to Backup & Recovery Policy

Backup Policy shall define standards of Backup & recovery control processes such that it achieves a balance between controls and efficiency, and follows the principle of Confidentiality, Integrity and availability. Backup Policy will ensure data and infrastructure are protected from risks. such that the data is correctly and efficiently backed up and recovered in line with this policy and best practices.

2. Purpose

The aim of this policy is to ensure that <Company name> conforms to the standard backup & recover very control processes ensuring risks associated to the management of data backs and recovery are mitigated, and balance between controls and efficiency is maintained.

3. Scope

The scope of policy applies to everyone in the <Company name>, including its staff, service providers and consultants. This policy is regarded as crucial to the effective protection of data and other IT Assets.

4. Policy

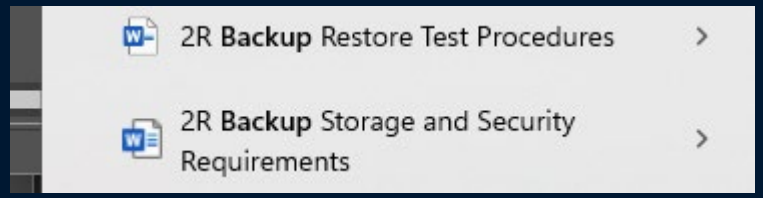
consultation with

different from its

ocedures must be
ures must include.

tal backup, etc.)

maintained (both



BIZ FOCUS

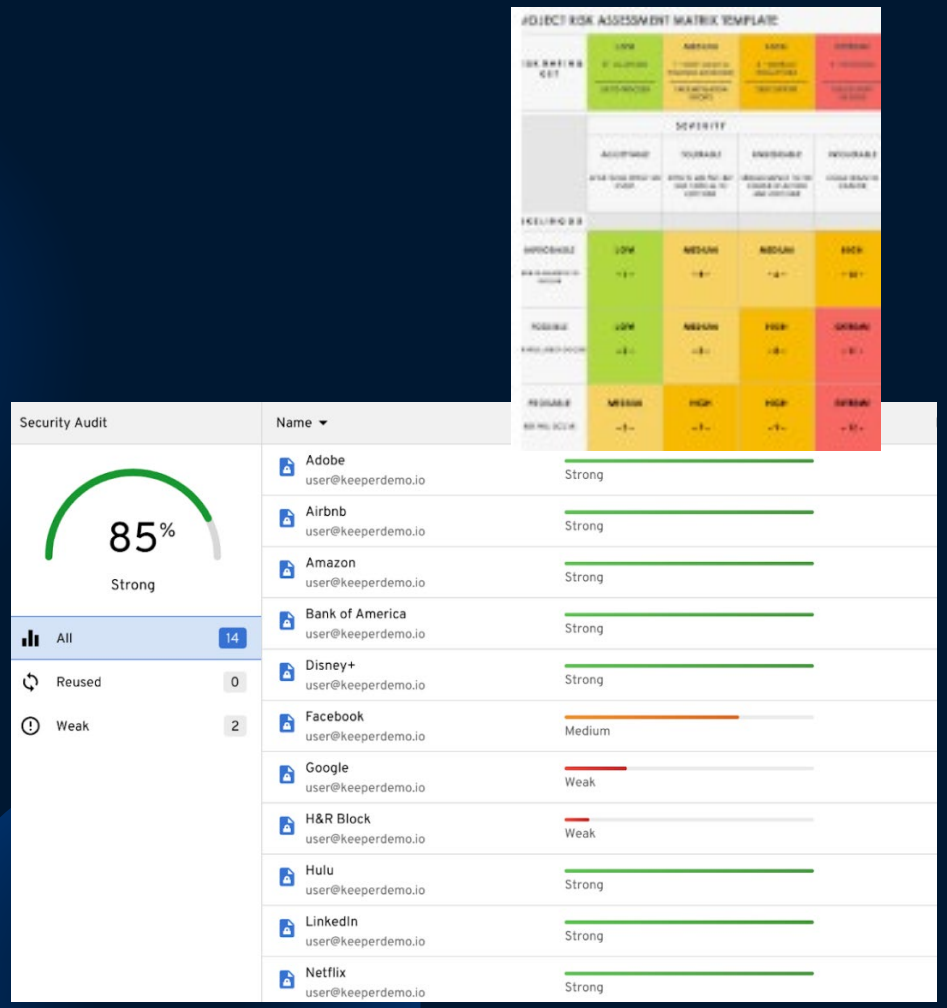
So how does an IT Consultant / MSP Help?

3. Compliance Review and SBIR/STTR specific risk rating

- After you've completed the changes, we can review and assess as a third party, to validate compliance and provide an expected Risk Score before you apply.

- Audit preparedness by validating the documentation and policies/SOPs, not just the technical coverage.

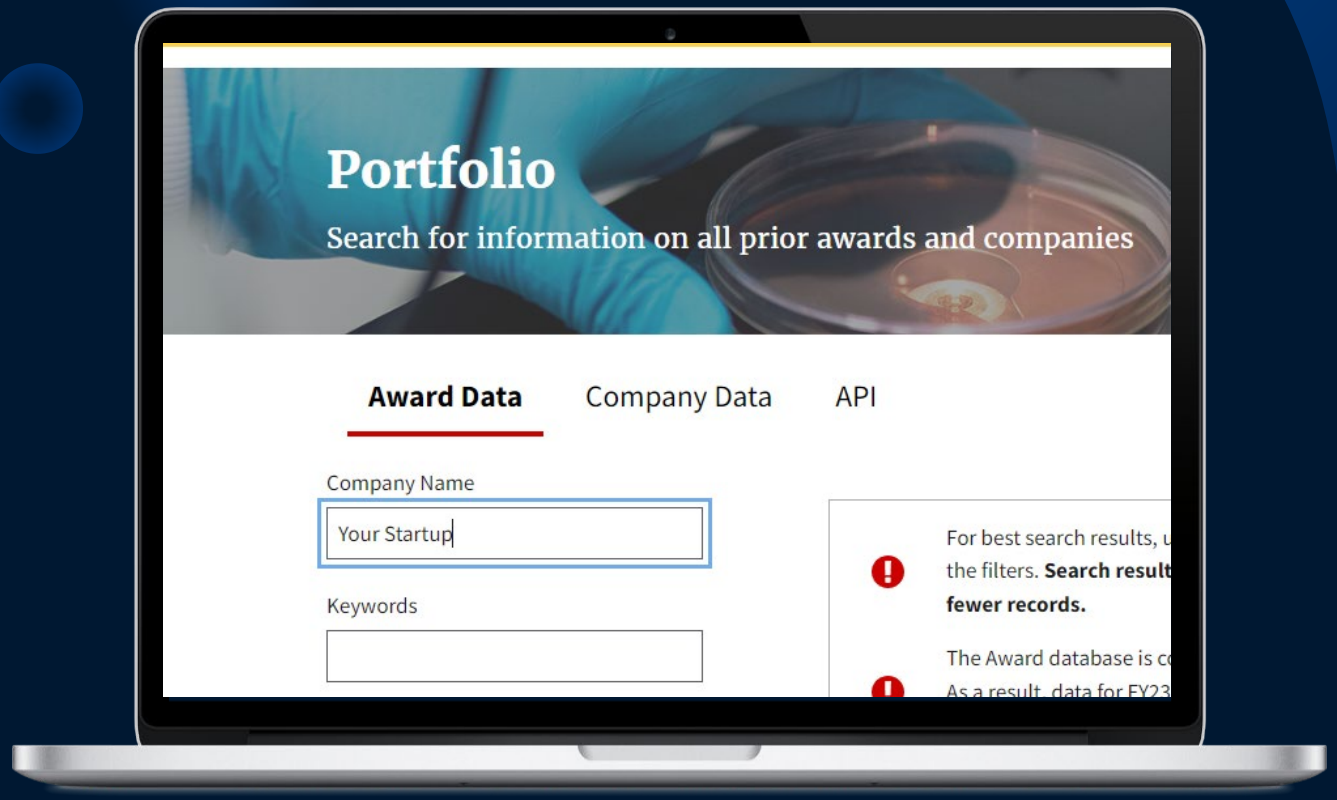
- Recommend appropriate compliance monitoring or automation tools to maintain compliance.



BIZ FOCUS

We look forward to Seeing your team again

From our team to yours –
Wishing each of you continued success to Phase II and beyond



260 +

SMB Clients Accelerated

$1B+

Lead Technical Solutioning Wins

BIZ FOCUS

Questions, Comments?
Reach out any time.

Biz-focus.com

(703) 628-9663 Direct
(703) 493-0536 Office

ken@biz-focus.com

Presentation Related Questions and Direct Contact

sbirsttr@biz-focus.com

Request the Free Walkthrough Docs & Resource Pack

Key Takeaways

- CPGs Addressed
- Solutions Presented

Q&A SESSION