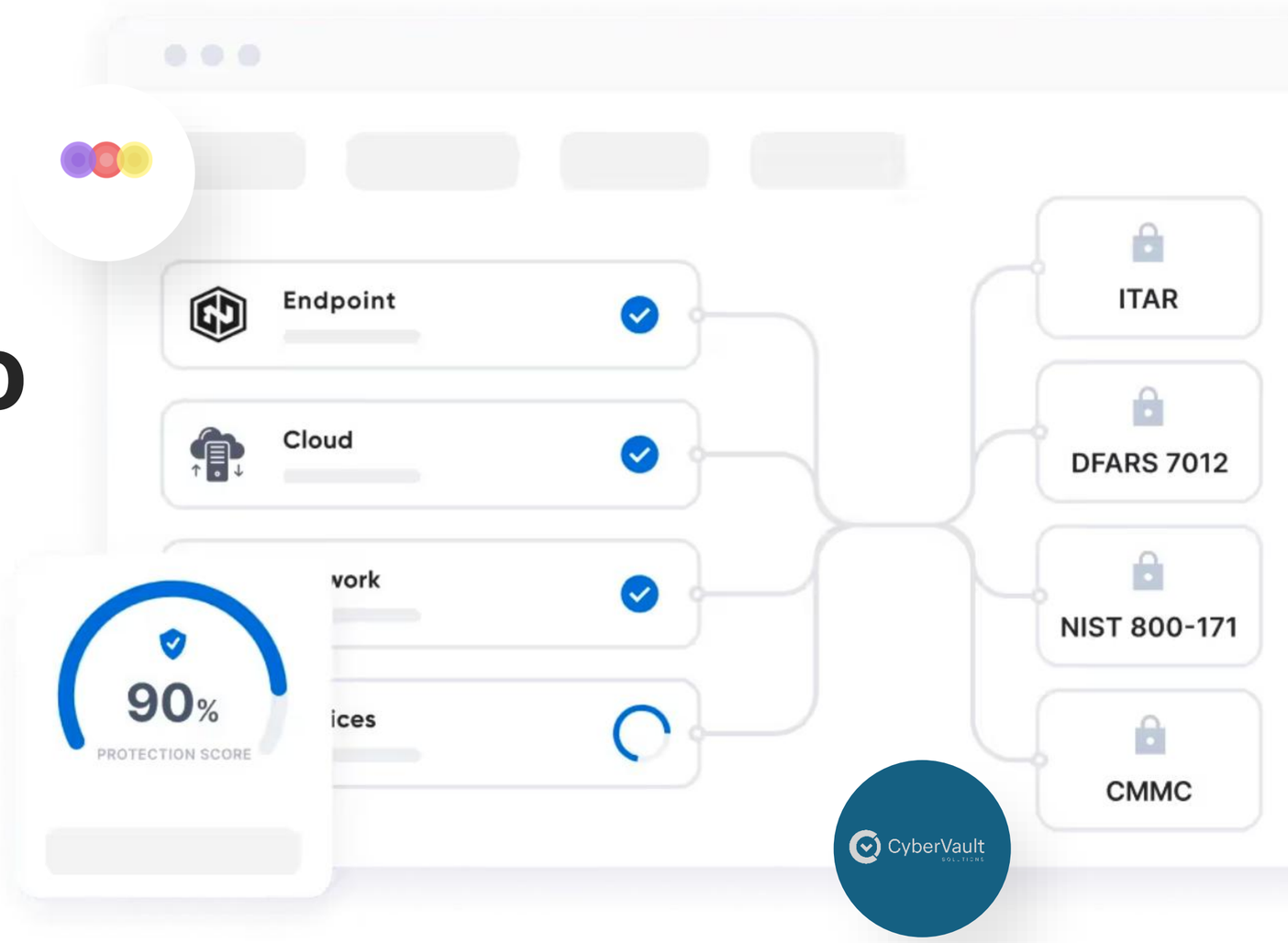
CyberVault
SOLUTIONS

CYBERVAULT SOLUTIONS

Implementing Zero Trust Compliance

We provide unparallelled, seamless, and world class cybersecurity strategies to the world's most critical organizations.



CyberVault
SOLUTIONS

Executive Summary

Zero Trust is a new way of doing security and poses a cultural change for your organization.

“Consider anything and everything a threat until successfully verified”.

CyberVault
SOLUTIONS

Compliance and Landscape

Mandates

- Executive Order 14028, “Improving the Nation’s Cybersecurity”
- OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”.

Frameworks

- NIST - Zero Trust Architecture SP 800-207
- CISA - Zero Trust Maturity Model

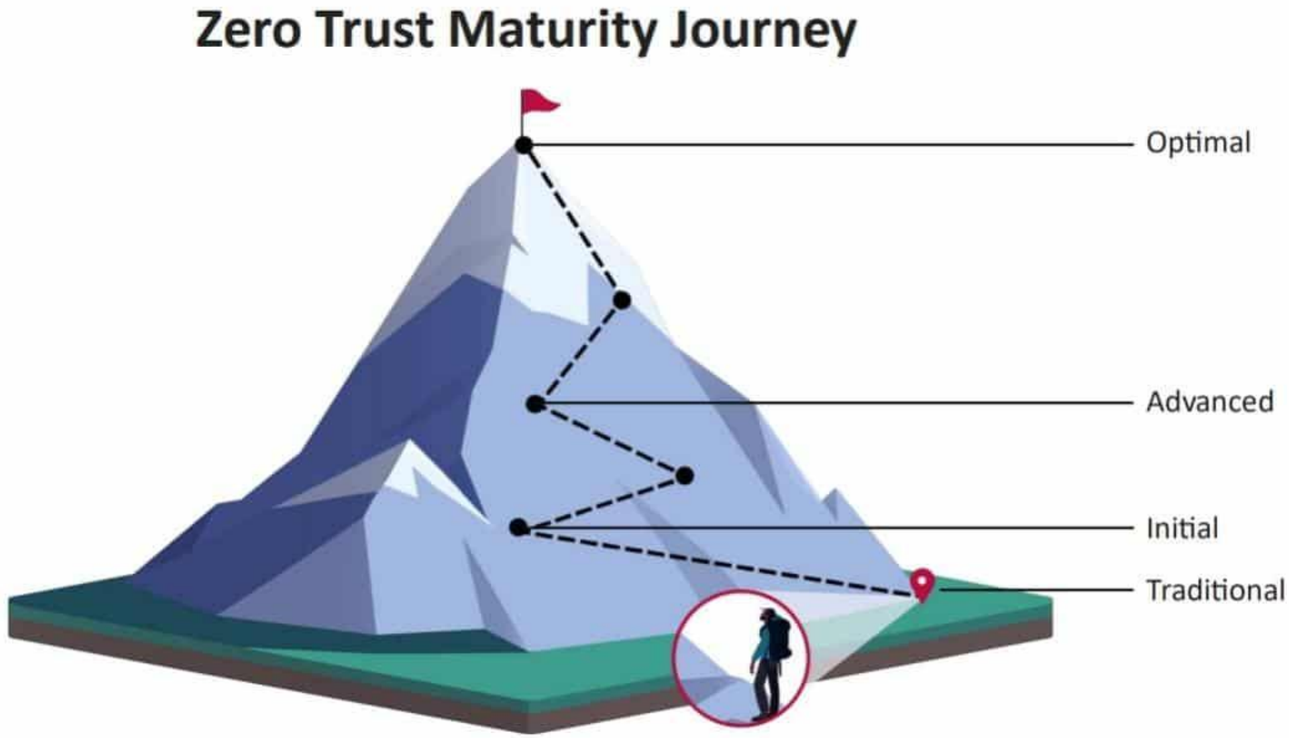
Our Approach

- Conventional security designs protect our data from outsiders;
- With Zero Trust architecture, we now protect access, Identity and data regardless of location.

CyberVault
SOLUTIONS

OUR STRATEGY:

We take a traditional assessment-first approach to evaluate your current infrastructure and build a roadmap to Zero Trust maturity. Starting with foundational elements already in place, we focus on transitioning through the key phases: **Traditional**, **Initial**, **Advanced**, and ultimately reaching the **Optimal** phase.



HOW WE GET YOU TO OPTIMAL:

Assess Current Posture:

Conduct gap analysis using CISA's Zero Trust Maturity Model. Leverage existing tools and configurations as a baseline.

Prioritize Quick Wins:

Roll out foundational elements like MFA and device compliance.

Develop a Roadmap:

Tailor strategies for scaling to Advanced and Optimal phases, ensuring alignment with business goals.

Implement and Optimize:

Continuously refine policies and processes while introducing advanced automation and analytics.

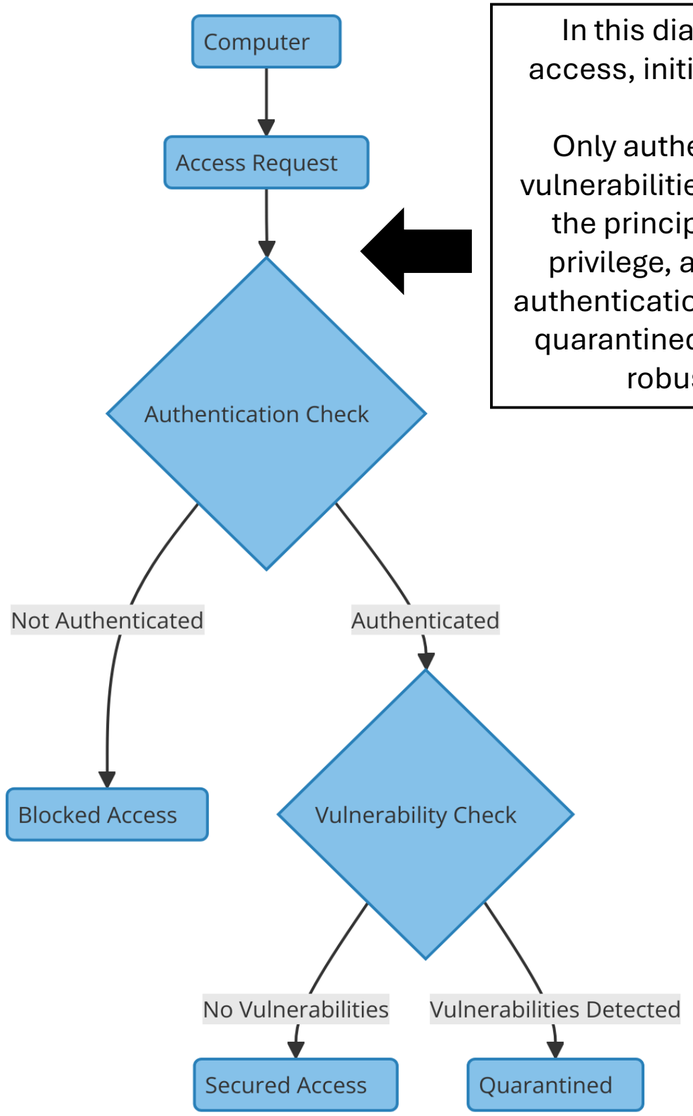
"There is no universal solution that fits every organization; our strategy focuses on providing customized and tailored solutions that work with your existing infrastructure".

CyberVault
SOLUTIONS

Our internal Zero Trust Matrix Strategy

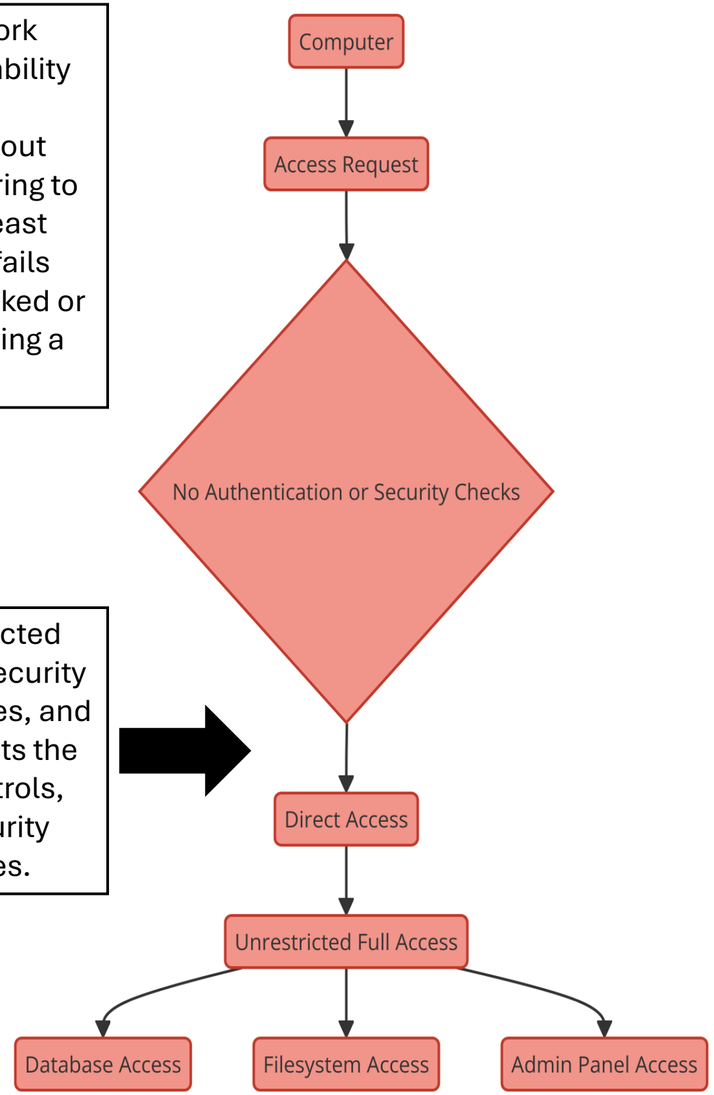
	Zero Trust Pillar	Maturity Stage	Compliance Focus/Action Items
2	Identity	Traditional	Password-based authentication with basic MFA for admin accounts.
3	Identity	Initial	Enforce MFA for all users and adopt single sign-on (SSO) solutions. Centralize user identity and privilege management.
4	Identity	Advanced	Implement continuous authentication and monitoring for privileged accounts.
5	Identity	Optimal	Fully adopt passwordless, risk-based adaptive authentication, and behavioral monitoring.
6	Device	Traditional	Basic inventory of devices with endpoint security (e.g., antivirus, firewall).
7	Device	Initial	Maintain real-time device inventory and ensure endpoint detection and response (EDR) for all devices.
8	Device	Advanced	Implement zero trust policies for BYOD, remote access, and device posture assessments.
9	Device	Optimal	Automate device security posture checks, including compliance enforcement and threat hunting.
10	Network/Environment	Traditional	Perimeter-based security (firewalls, VPNs), manual network segmentation.
11	Network/Environment	Initial	egin network segmentation based on critical assets. Introduce microsegmentation and start moving away from VPN reliance
12	Network/Environment	Advanced	Implement least-privilege network access, including monitoring east-west traffic.
13	Network/Environment	Optimal	Full dynamic network segmentation based on user and device behavior, automated threat detection.
14	Application	Traditional	Basic web application firewalls (WAF), vulnerability scanning for key applications.
15	Application	Initial	Implement secure application development lifecycle (SDLC) with static and dynamic code analysis.
16	Application	Advanced	Enforce container and API security, and use real-time monitoring and threat intelligence for application behavior.
17	Application	Optimal	Fully automated application security checks with real-time remediation and orchestration.
18	Data	Traditional	Data is manually classified, basic access controls.
19	Data	Initial	Data is automatically classified and encrypted in transit and at rest. Begin applying DLP tools.
20	Data	Advanced	Apply continuous monitoring and encryption for structured and unstructured data with automated policy enforcement.
21	Data	Optimal	Full data lifecycle management with continuous risk assessment, automated tagging, and protection.
22			

CyberVault
SOLUTIONS



In this diagram, the computer requests network access, initiating an authentication and vulnerability assessment process.
Only authenticated devices and systems without vulnerabilities are granted secure access, adhering to the principles of verifying explicitly, granting least privilege, and assuming a breach. If a system fails authentication or shows vulnerabilities, it is blocked or quarantined to prevent potential threats, ensuring a robust and proactive security posture.

This diagram shows an unrestricted system where users bypass all security checks, accessing databases, files, and admin panels directly. It highlights the dangers of missing access controls, emphasizing the need for security measures to prevent breaches.



Zero Trust Implementation

CyberVault SOLUTIONS

Traditional → "Still relying on the old ways—open trust, broad access, and minimal segmentation.

Initial → "Just getting started with Zero Trust—testing the waters and building the foundation."

Advanced → "Making solid strides—integrating tools, automating workflows, and reducing risk."

Optimal → "Running like a well-oiled Zero Trust machine—adaptive, automated, and deeply integrated."

Requirements

CyberVault
SOLUTIONS

Traditional ⟶ Relies on perimeter firewalls, VPN access, and static credentials with minimal segmentation or identity validation.

Initial ⟶ Implements multi-factor authentication, centralized identity management, and basic network segmentation to reduce unauthorized access.

Advanced ⟶ Utilizes microsegmentation, context-aware access controls, endpoint detection and response (EDR), and automated threat detection to enforce least privilege and reduce lateral movement.

Optimal ⟶ Employs AI-driven analytics, dynamic policy enforcement, continuous monitoring, and full integration across identity, network, and workload domains to maintain an adaptive Zero Trust environment.

Tools Overview

CyberVault SOLUTIONS

Traditional → This level relies on perimeter firewalls like Cisco ASA, VPN solutions such as AnyConnect, and password-based authentication, with minimal segmentation or identity validation.

Initial → This level introduces multi-factor authentication tools like Duo Security, identity providers such as Azure AD, basic network segmentation using VLANs or ACLs, and foundational monitoring through SIEM solutions like Splunk.

Advanced → This level leverages context-aware access via Okta Adaptive MFA, microsegmentation using tools like Illumio, advanced threat detection with EDR platforms such as CrowdStrike and automated incident response through SOAR solutions like Palo Alto XSOAR.

Optimal → This level implements AI-driven analytics from tools like Exabeam, dynamic risk-based policy enforcement using Zscaler ZPA, automated identity governance through SailPoint, and continuous diagnostics with full integration across identity, network, device, and workload domains.

Zero Trust is not a checkbox, a product, or a one-size-fits-all approach. It's a mindset — and more importantly, a strategy — that requires a tailored blend of people, processes, and technology.

There is no single tool that can deliver complete Zero Trust compliance. While some technologies move organizations closer to automation and enforcement, true Zero Trust security is achieved through a bundle of coordinated efforts across domains.

People are the heart of security — they interpret data, respond to threats, make decisions, and continuously improve posture. But they are human. They fatigue, make mistakes, and can't be expected to carry the burden alone.

Processes define how to operate securely — they create structure, repeatability, and accountability. But even the best-documented processes fail without people to execute and adapt them in real-world scenarios.

Technology provides the scale, speed, and intelligence needed to detect, prevent, and respond — but it is ineffective without skilled professionals to configure it, tune it, and question its output.

Zero Trust is a bundle deal — and always will be.
Success lies in aligning people, processes, and technology toward a shared goal of minimizing implicit trust and continuously validating access.

In a world of evolving threats, a holistic Zero Trust approach isn't just ideal — it's essential.

CyberVault
SOLUTIONS

PROBLEM: Organizations believe that Zero trust is a one shoe fits all approach

HOW WE DIFFER

Tailored Solutions – Simplified Approach

Taking a phased approach, leveraging your existing tools and resources to efficiently guide you from initial compliance to a mature Zero Trust posture.

Leveraging Existing Technologies

Our focus is on optimizing the tools already in place, creating cultural and process shifts rather than introducing unnecessary complexity.

Flexible Strategies

We assess your current state and align our approach with your unique compliance journey, building on existing frameworks like CISA and NIST.

Mixed Methodologies

Integrating the best practices from CISA and NIST, delivering customized solutions, grounded in proven strategies.

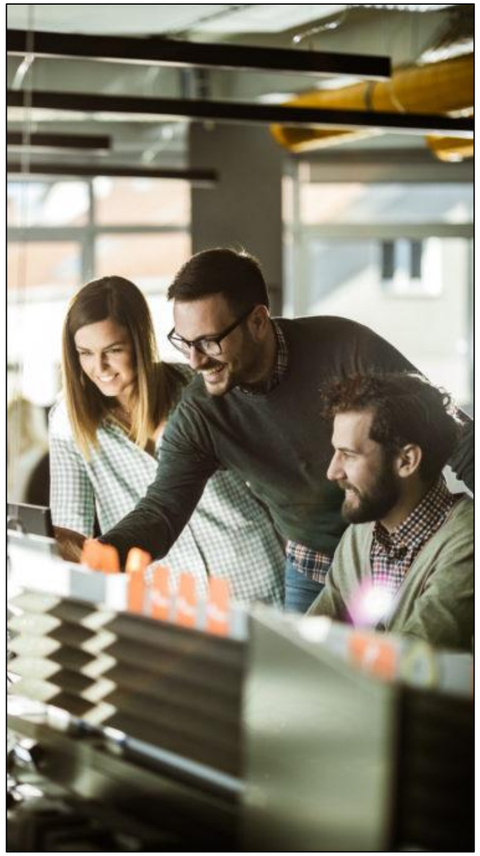
Zero Trust Culture

We emphasize cultural transformation by aligning people, processes, and technologies to create a sustainable Zero Trust environment.

CyberVault
SOLUTIONS

OUR PROCESS

Proposed RoadMap & Phased Approach



STEP 1

Full evaluation & Infrastructure scoping

Review current infrastructure, security tools, technical controls, documents, policies, hardware and software.

STEP 2

Align and adhere to frameworks

To ensure compliance and standardization, we align with proven frameworks such as: NIST, ISO, CMMC etc..

STEP 3

Mitigation Strategies

We will provide tailored mitigation strategies based on our assessment and findings.

STEP 4

Continuous Monitoring

We continuously monitor your environment with 24/7 real-time alerts and maintenance.

STEP 5

Ongoing Partnership

We offer continuous support, updates, and expert guidance, keeping your compliance journey seamless.

CyberVault
SOLUTIONS

Why Choose CyberVault?

- **3.9K+**

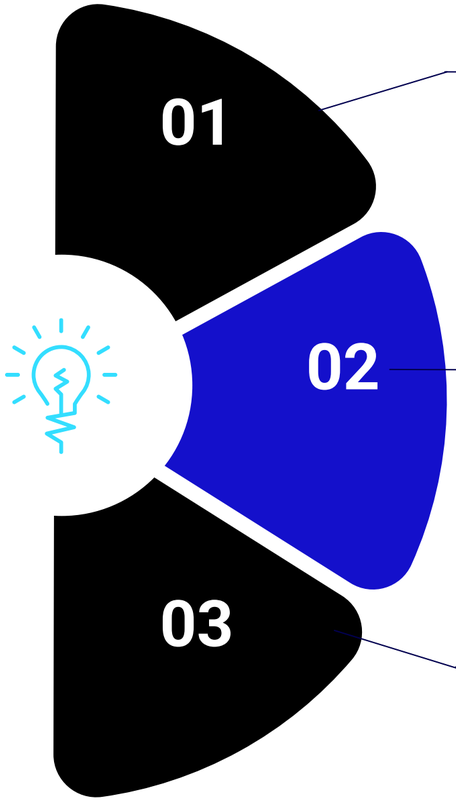
  The number of individuals who have benefited from cybersecurity awareness training, both from an individual perspective and through the initiatives led by the company.

- **97%**

  Overall Customer Satisfaction Based on Service Queue Feedback Surveys.

- **Integrity**

  Leading organizations have sought out CyberVault Solutions for expertise in Zero Trust implementation, compliance, cybersecurity training, and comprehensive cybersecurity support services.



Trusted by Leading Institutions

Our solutions are trusted by government and commercial entities. We ensure data security, regulatory compliance, and seamless IT infrastructure to in support of all environments.

Specialize in Education

While many companies focus on various industries, we specialize in the unique needs of academic institutions, safeguarding student data and optimizing IT resources for enhanced educational experiences.

All-in-One Solution

CyberVault Solutions delivers tailored cybersecurity and IT solutions for organizations of all sizes. We implement, monitor, maintain, and document systems from start to finish, ensuring security, compliance, and efficiency. With personalized service and quarterly reviews, we adapt to your unique needs and challenges.