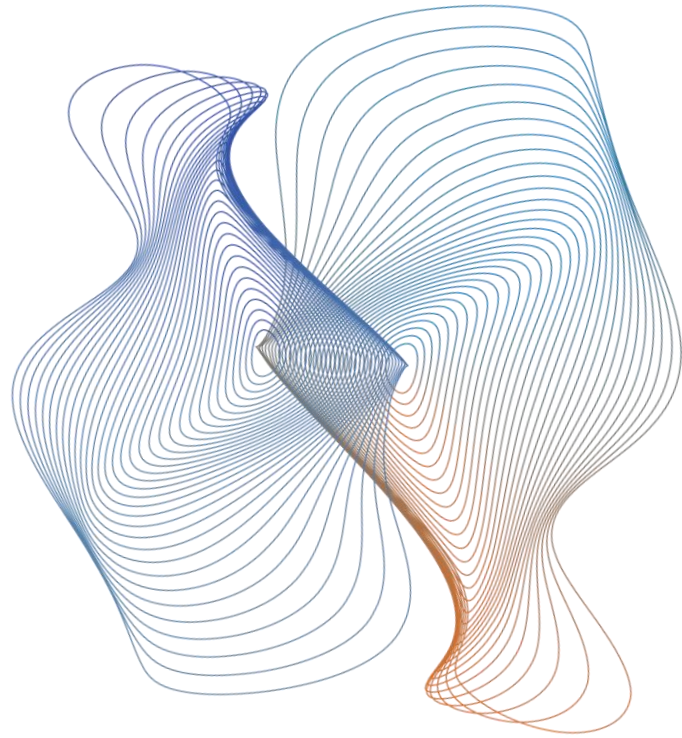


onetierTM

Your **Zero Trust** Technology Partner

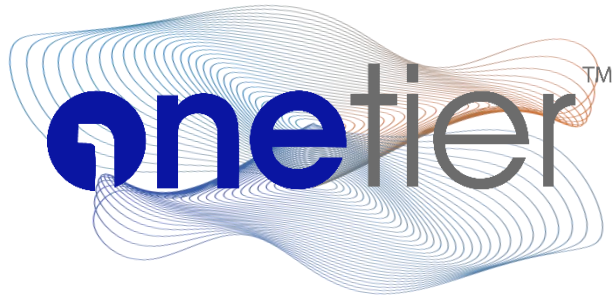


Agenda

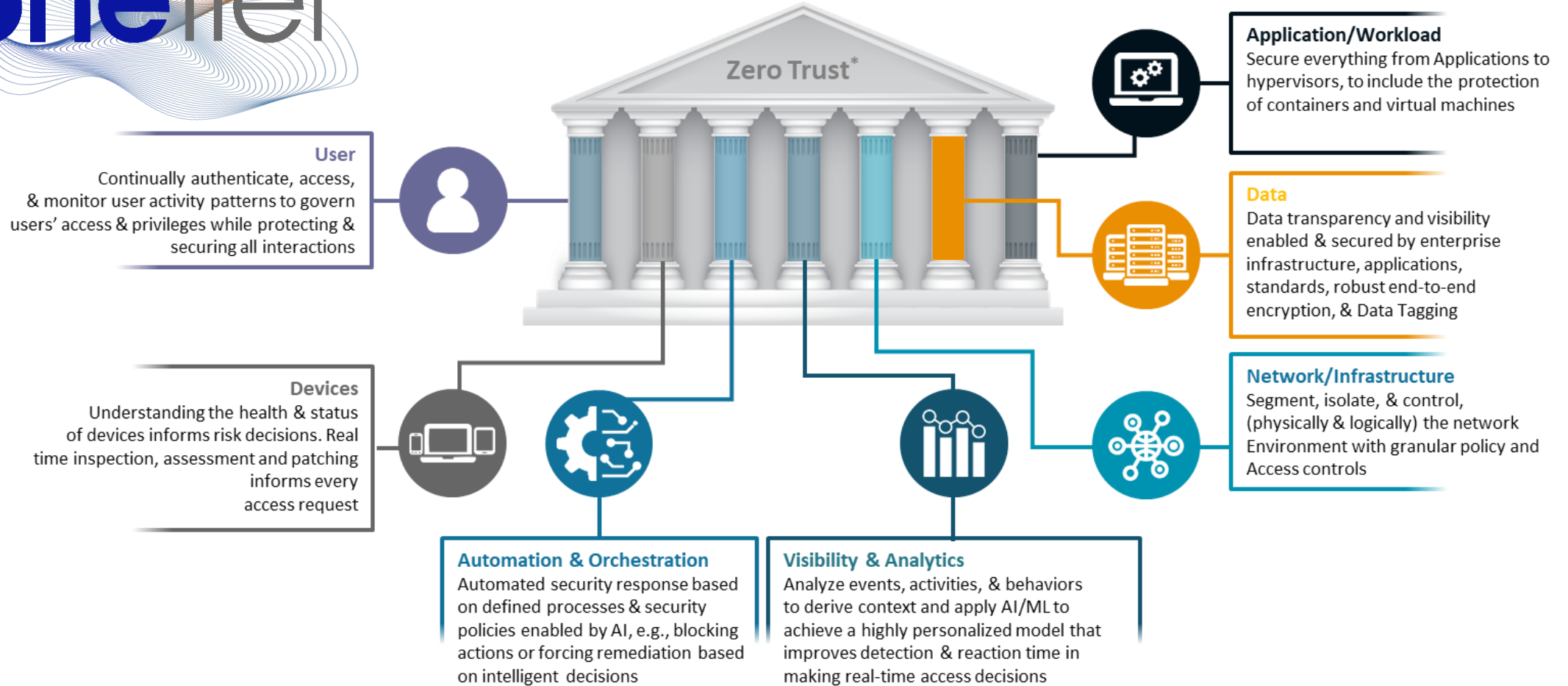
- **What is Zero Trust?**
- **Who is OneTier?**
- **Why OneTier (What Gap We Fill)?**
- **The OneTier Portfolio**

“The scope, speed, and volume of digital attacks continue to outpace enterprise security teams, jeopardizing brand reputation, user trust, and organizational security. Relying on legacy detection and mitigation processes has become insufficient to take on bad actors and wastes an organization’s resources. With Bolster’s AI-powered security workflow and sophisticated domain takedown capabilities, organizations can manage and remediate digital risks at scale while saving time and money.”

- Forrester (Dec 2022) – *The Total Economic Impact (TEI) of Bolster.*



Zero Trust Pillars and Tenets



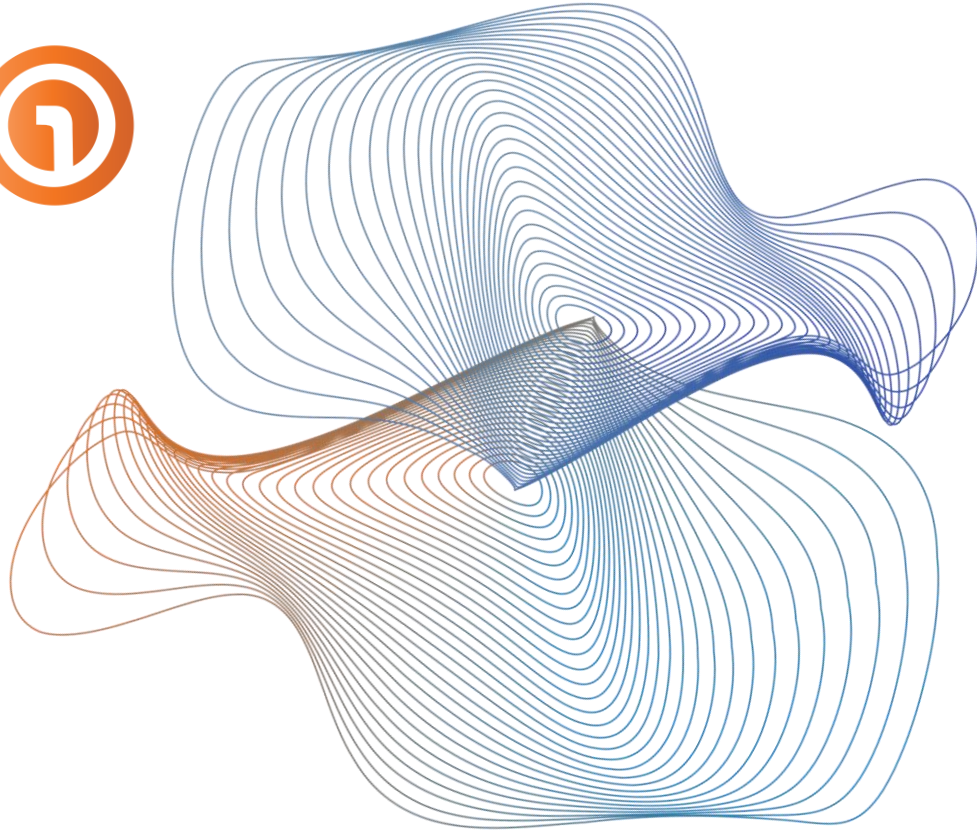


We are a technology solutions provider that plays at the OEM distribution layer. We combine state-of-the-art technology together to create a first of its kind solution for government agencies, contractors, solution providers, and commercial resellers.

We provide software engineering and solution design services related to advanced networking, secure communications, cyber security, encryption, ICAM, data analytics, and risk analysis/prevention.

We have built a solution that integrates cyber and data security together to finally achieve Zero Trust and risk awareness.

Cage Code: 9HW83
UID: PWYBCM98BUT8



Why onetier™
Innovation Through Technology

Problem we solve for

- Understanding your Risk
- Exposure to Increased Cost
- Inhibited Revenue Growth

Fulfilling a Need

- Actual Zero Trust Roadmap
- Digital Infrastructure Transformation
- Unified Security Platform



netier™ ANYCLOUD DATASECURE

Portfolio

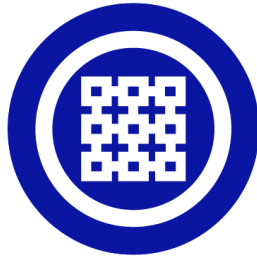
- Security & Operations

Risk Engagement™



- Software & Systems Development
- ML & AI

KubeZT Secure Apps



- Data Management & Storage

Global Data Security™



- SOAR

Security Overwatch™



AnyCloud™ Orchestrator

- Automation
- ML & AI
- Infrastructure Management



Stealth Networking™

- Networking & Wireless Transport



Secure Access™

- Assured Identity
- Browser Isolation
- Access Management



Risk Engagement™

An automated penetration testing tool and service that assesses a client's network for exposure and risk. The tool generates a T score and maps the required remediation steps to NIST 800-53, 171, 207, and all 4700 endpoints of the MITRE ATT&CK framework. This is correlated to real client financials. CMMC 2.0 evaluation and reporting is included.

- SaaS Application
- Threat Score
- Dashboard Monitoring
- Jellyfish Diagram
- Financial Correlation
- NIST 800-53, 171, 207
- ISO 27001
- MITRE ATT&CK Framework
- CMMC 2.0 Compliance
- Mitigation Roadmap
- GAO & Audit Reporting

Capability Description	Capability Status	Expected Loss Value	Expected Recovery Cost
AC - Access Control	74%	\$2,382,717	\$1,191,359
AT - Awareness and Training	72%	\$1,283,894	\$641,947
AU - Audit and Accountability	70%	\$1,314,184	\$657,092
CA - Security Assessment and Authorization	72%	\$2,795,449	\$1,397,724
CM - Configuration Management	76%	\$817,928	\$408,964
CP - Contingency Planning	60%	\$479,913	\$239,956
IR - Incident Response	74%	\$817,928	\$408,964
MA - Maintenance	64%	\$1,314,184	\$657,092
MP - Media Protection	64%	\$1,314,184	\$657,092
PE - Physical and Environmental Protection(s)	80%	\$517,464	\$258,732
PL - Planning	70%	\$1,314,184	\$657,092
PS - Personnel Security	66%	\$1,314,184	\$657,092
RA - Risk Assessment(s)	68%	\$1,314,184	\$657,092
SA - System and Services Acquisition(s)	66%	\$1,314,184	\$657,092
SC - System and Communications Protection(s)	66%	\$1,314,184	\$657,092
SI - System and Information Integrity	66%	\$1,314,184	\$657,092
PM - Program Management	74%	\$1,314,184	\$657,092

NIST 800-53-centric basis to address non-remediated risk: 18 control families → Controls → Control Description, Guidance

Control Description	Priority	Low	Moderate	High
CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES	P1	CP-1	CP-1	CP-1
CP-2 CONTINGENCY TRAINING	P1	CP-2	CP-2	CP-2
CP-3 CONTINGENCY PLAN TESTING	P2	CP-3	CP-3	CP-3
CP-4 CONTINGENCY PLAN UPDATE	P2	CP-4	CP-4	CP-4
CP-5 ALTERNATE STORAGE SITE	P1	CP-6	CP-6	CP-6
CP-6 ALTERNATE PROCESSING SITE	P1	CP-7	CP-7	CP-7
CP-7 TELECOMMUNICATIONS SERVICES	P1	CP-8	CP-8	CP-8
CP-8 INFORMATION SYSTEM BACKUP	P1	CP-9	CP-9	CP-9
CP-9 INFORMATION SYSTEM RECOVERY	P1	CP-10	CP-10	CP-10
CP-10 ALTERATION OF CONFIGURATION	P1	CP-11	CP-11	CP-11
CP-11 ALTERATION OF CONFIGURATION	P1	CP-12	CP-12	CP-12
CP-12 SAFE	P1	CP-13	CP-13	CP-13
CP-13 ALTERATION OF CONFIGURATION	P1	CP-14	CP-14	CP-14

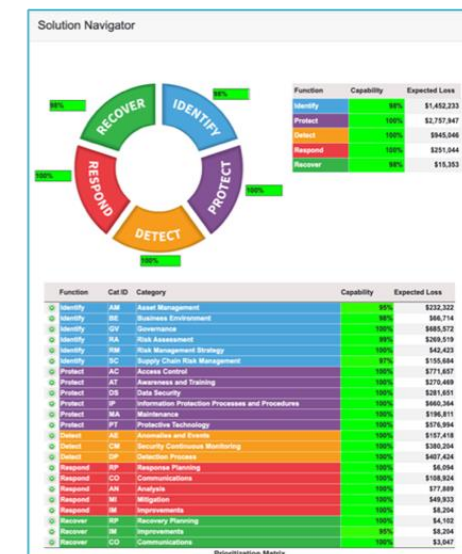
Control Description
The organization:
a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
1. Contingency planning policy [Assignment: organization-defined frequency]; and
2. Contingency planning procedures [Assignment: organization-defined frequency].

Supplemental Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Control Enhancements
None

References
Federal Continuity Directive 1 : <http://www.fema.gov/pdf/about/offices/fcd1.pdf>
NIST Special Publication 800-12 : <https://csrc.nist.gov/publications/search?keywords=ig-800-12>

NIST CSF-based solutions navigator:

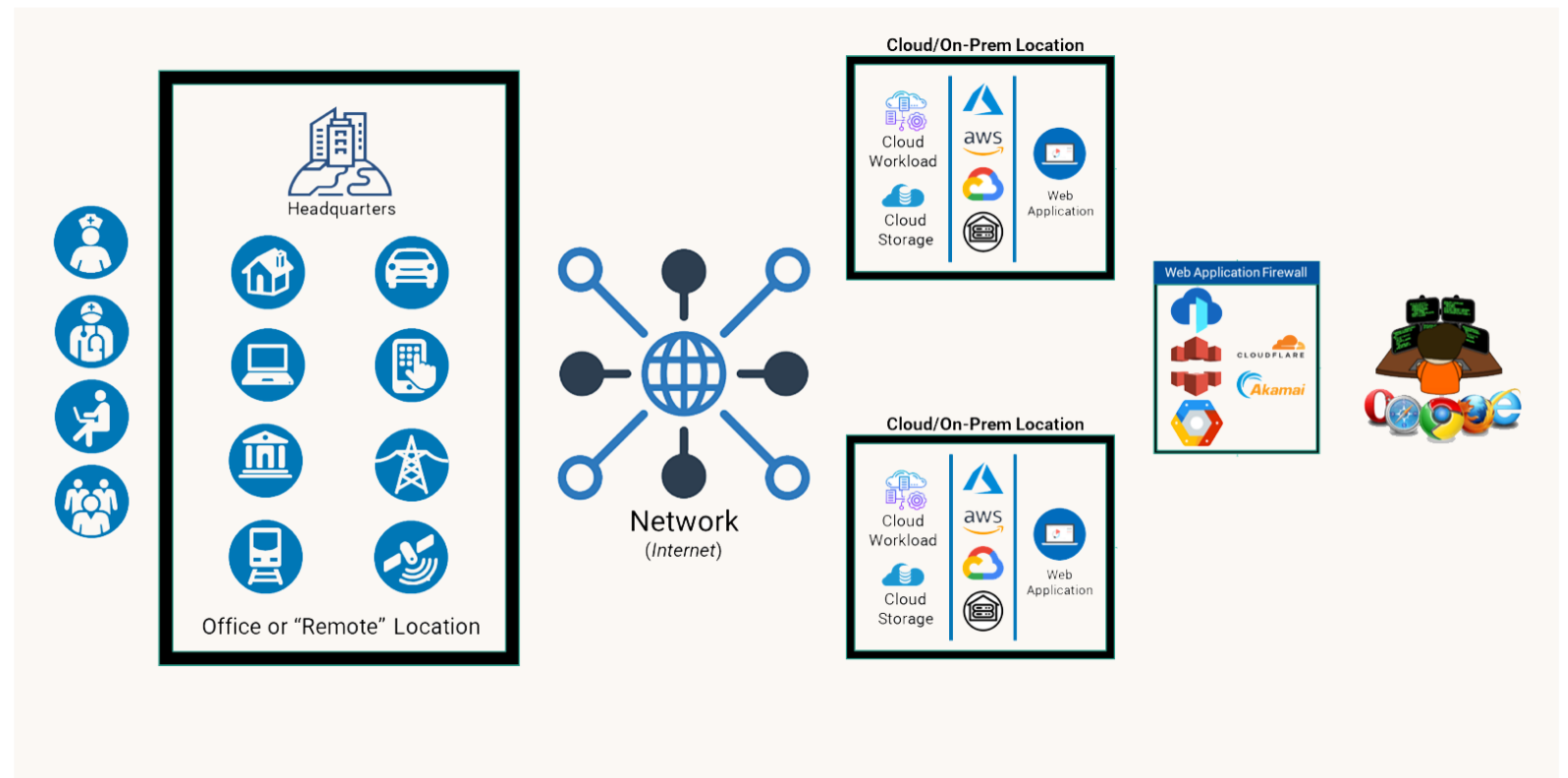




Stealth Networking™

An advanced software defined networking suite that runs across any existing physical network topology. It creates a secure and encrypted multi-channel mesh network of devices that can self-heal and is undetectable as it operates. It has granular policy driven controls across the network.

- Software Defined Networking
- VPN Replacement
- Mesh Topology
- Self-Routing
- Self-Healing
- Multi-Channel
- Edge to Edge
- Encrypted
- Secure
- Accelerated
- Obfuscated
- Mutual TLS
- No Ports Exposed
- Any Device

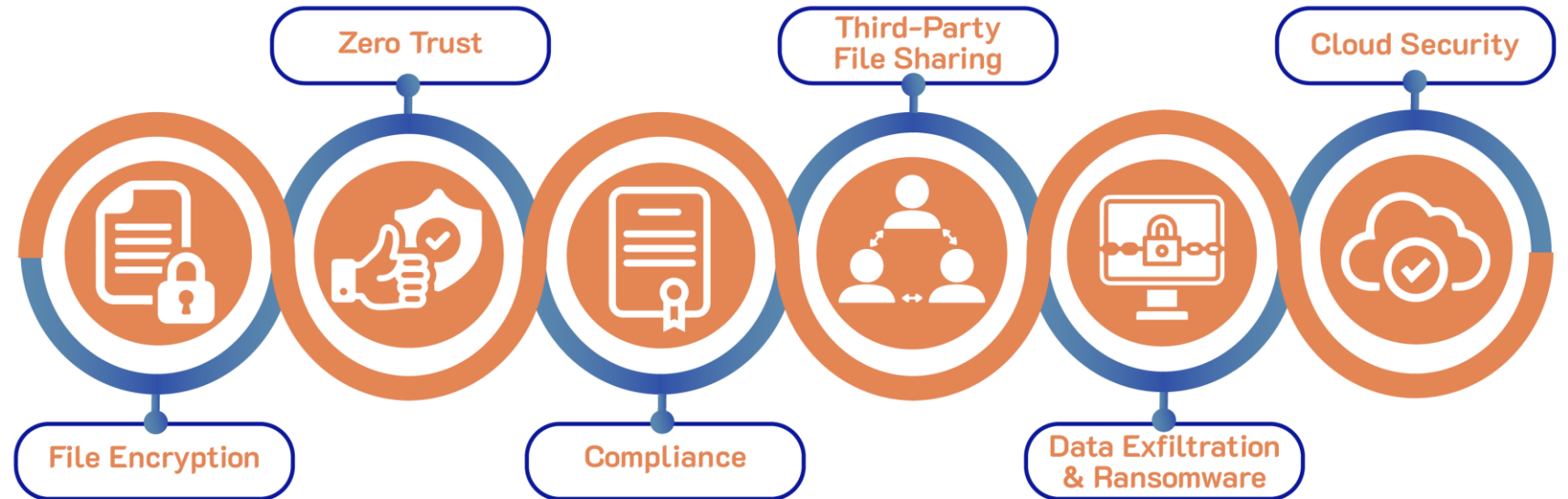


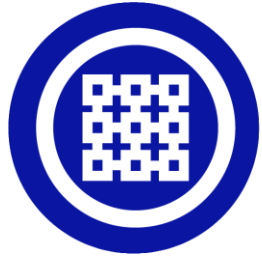


Global Data Security™

A true secure and encrypted global file system that can incorporate any storage array and any combination of structured and unstructured datastores into a single file system for all your users. It is immutable and ransomware proof and eliminates the need for backups of files.

- Global File System
- Secure
- Encrypted
- Policy Controlled
- Any File Mount
- Any Storage Array
- Any Object Store
- Any Cloud for Storage
- Mesh Topology for Files
- Edge Caching & Access
- Accelerated Access
- Immutable Files
- Web Accessible





KubeZT Secure Apps

We are experts in advanced technologies that can help you go from raw and unmanaged data, to ingestion, transformation, and informed decisions, in a matter of hours or days instead of months. KubeZT allows for secure containerized, virtual compute, networking, ICAM, and analytics in a single mesh connected package.

- **Unlimited File Size through Browser**
- **Supports Thousands of Concurrent Users**
- **Guaranteed File Integrity**
- **Upload Interruption Re-Start Support**
- **Advanced Analytics**
- **Cutting-Edge ML/AI**
- **Collaborative Data Science**
- **AutoML (AI to do AI)**
- **Secure Networking**
- **Secure Kubernetes**
- **Integrated LDAP**
- **Integrated DKIM**
- **Integrated Oauth**
- **Integrated DNS**

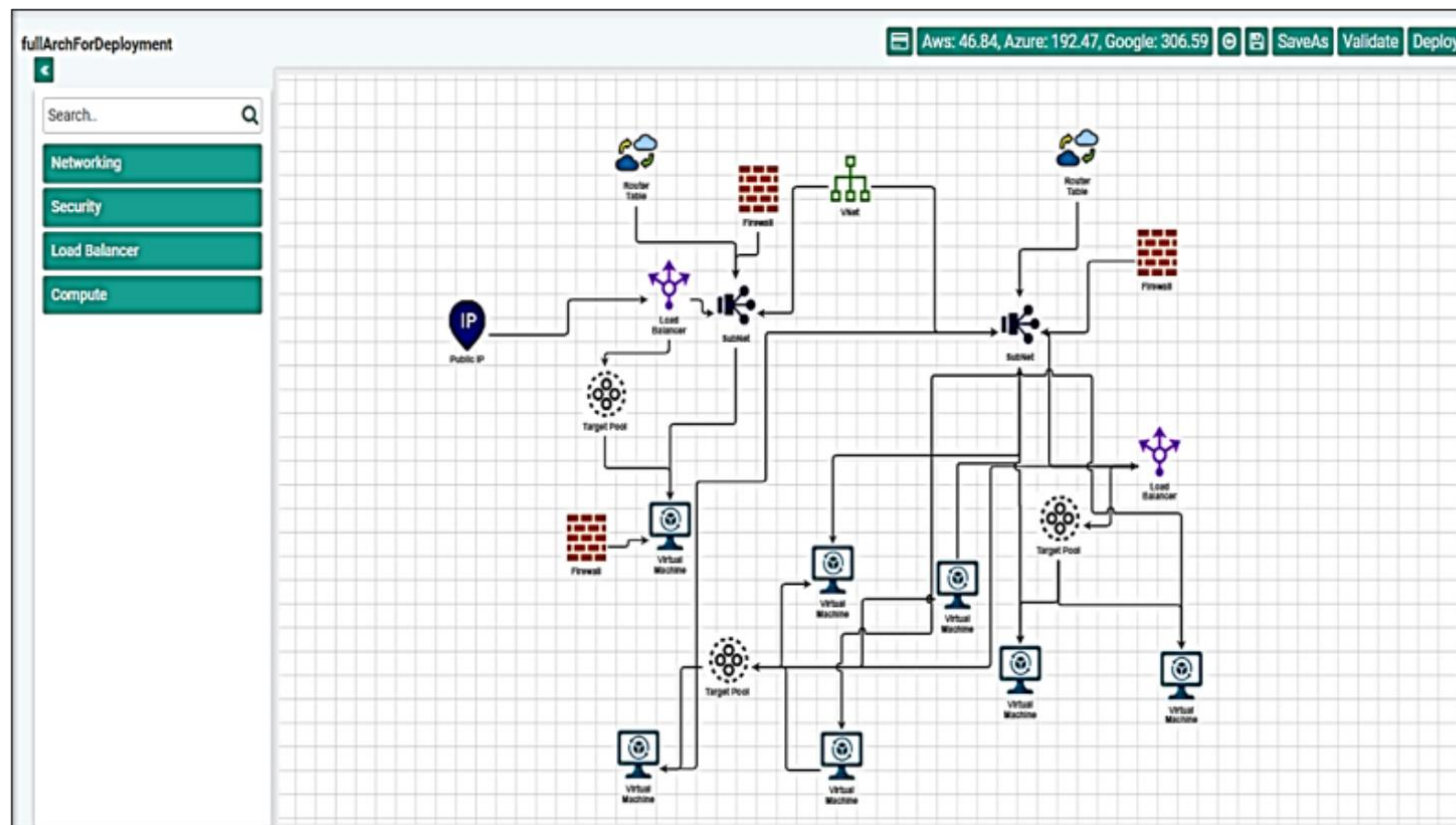
The screenshot displays the KubeZT web interface. On the left is a dark sidebar with navigation options: Dashboard, Learning & Skills (Learning Center, QuantHub), Data Management (Files, Streams), Data Engineering (Pentaho, Apache NiFi), and Data Science (Notebooks). The main area is split into two panels. The top panel shows a Jupyter Notebook titled 'Untitled.ipynb' with Python code for data analysis using pandas, matplotlib, and sklearn. The bottom panel shows a file upload interface with a green header 'UNCLASSIFIED DATA ONLY', a 'Choose Files' button, and a large dashed box for dragging files. Below this, a 'Files' section shows two upload progress bars: 'raw_743_MIB' at 9.42% and 'raw_742_MIB' at 85.18%.



AnyCloud™ Orchestration

A powerful platform that allows any software environment to be deployed automatically into any cloud environment securely with all resources and costing included. This can be done across clouds and physical data centers to create effective hybrid and multi-cloud environments.

- Drag & Drop Creation
- Multi-Cloud Capability
- Hybrid-Cloud Capability
- Full Costing pre-Deployment
- Secure Interface
- All Virtual Components Configurable
- Accelerated Transformation
- Automated Migration
- Environment Monitoring
- Fully Automated Deployments
- Cloud Mapping
- DC to DC Transfer
- Storage Migration
- Mainframe Transformation

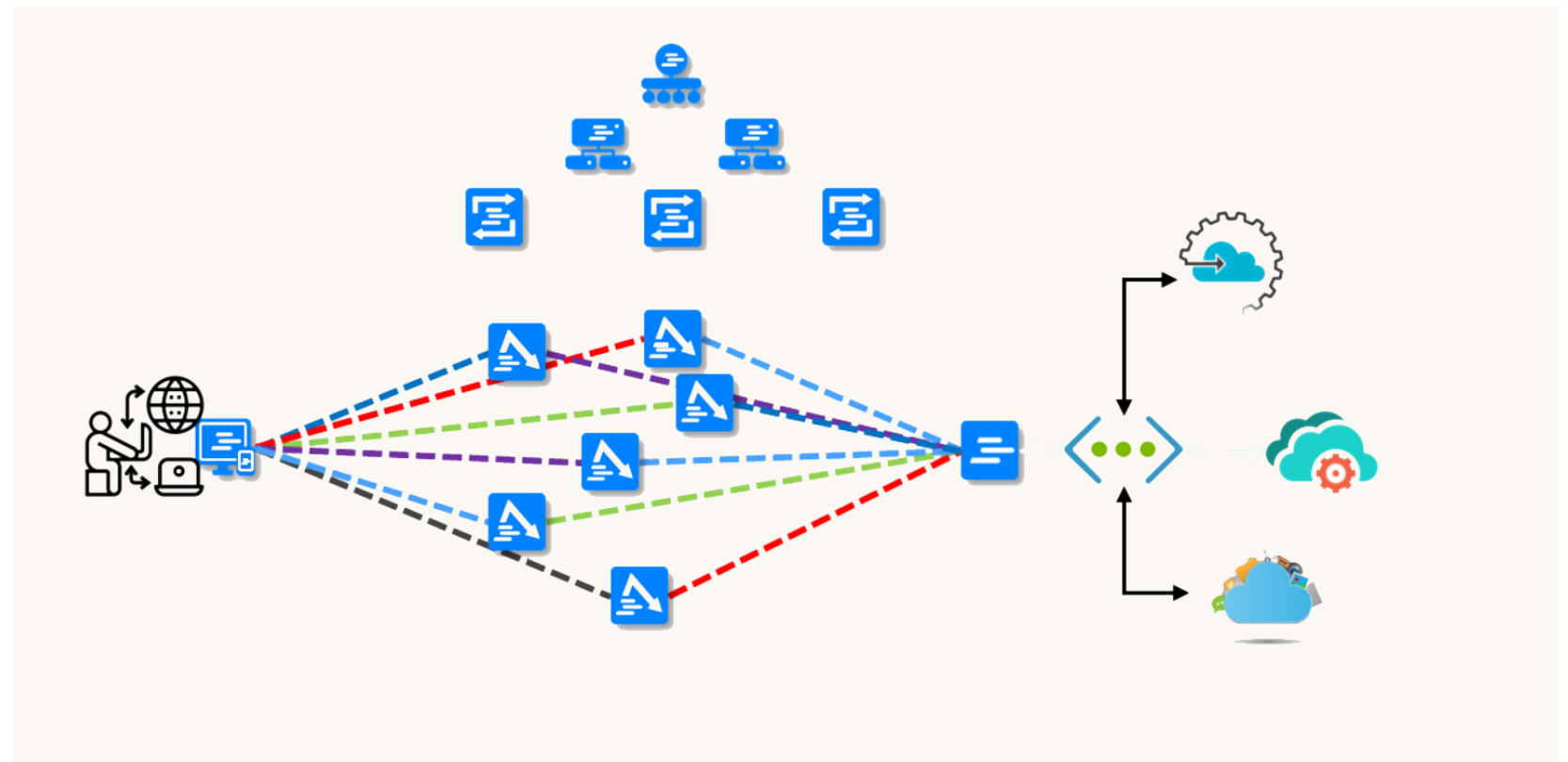




Secure Access™

A flexible and cross domain secure identity access management system that allows users to validate their credentials using multi-factor authentication into federated systems. This is the beginning of the Zero Trust process and NIST 800-207.

- **Multi-Factor Authentication**
- **Federated Access**
- **Policy Controlled**
- **Zero Trust Enablement**
- **Encrypted**
- **Cross Domain**
- **Multi-Cloud and Hybrid**
- **User Validation**
- **Privileged Access Control**

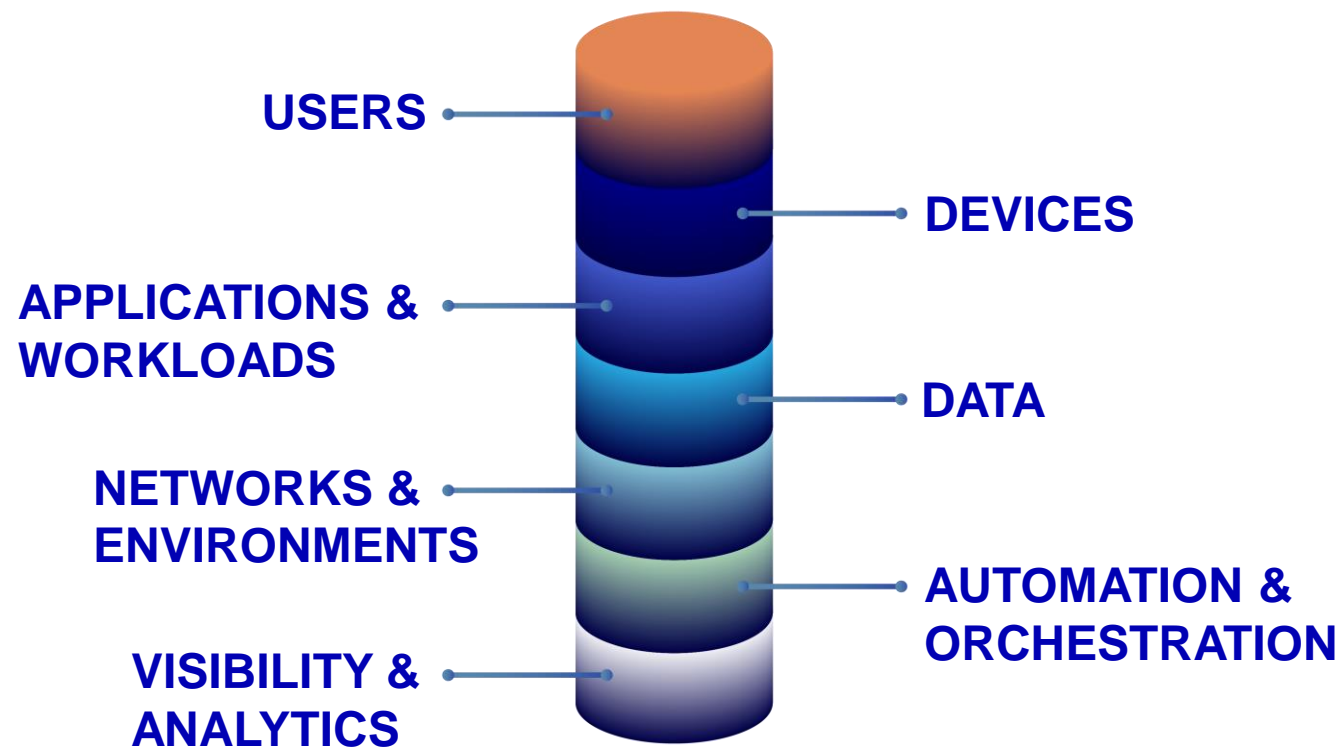




Security Overwatch™

A cyber security solution that integrates with existing endpoint protection and firewalls, as well as our networking product, to monitor inbound and outbound traffic for malicious activity. It also monitors for connections to IPs that pose as friendly, but are a threat in disguise.

- Threat Intelligence
- Integration with Networking
- Integration with Existing Endpoint Protection
- Enabling Zero Trust
- Aggregating Log Files
- Continuous Monitoring
- Monitoring Inbound & Outbound Connections
- Largest Database of Malicious IPs





OneTier Corp is a US based and owned corporation and SAM registered small business. We are a value-added integrator and distributor of advanced technology solutions to government agencies and contractors, solution providers, and commercial resellers.

We provide software engineering and solution design services related to cloud migration and transformation, advanced networking, secure file systems, cyber security, encryption, data analytics, and risk analysis/prevention.

We specialize in locating and combining commercial products from multiple vendors, then integrating them into secure deployable solutions for government and commercial applications.

Chris Romeo
Chief Executive Officer

 Cromeo@onetier.com

 +1 703-829-0115

 Reston, VA, USA

 www.onetier.com

Taber West
Chief Technology Officer

 taber@onetier.com

 +1 303-501-4485

 Los Alamos, NM, USA

 www.onetier.com