ERACENT ARMORED ZERO TRUST RESOURCE PLANNING

WHAT
Complete implementation & management of your Zero Trust Program

WHY
Continuous, and
systematic reduction of risk

HOW
Risk based / Silo busting approach

WHO
Executive • Cyber • IT Admin
Risk • Audit • Business • AppDev

ZT FUNCTIONS

IDENTIFICATION
DEVICES
APPLICATIONS
NETWORKS
INFRA
DATA
INTELLIGENCE
AUTOMATION
GOVERNENCE

PROCESS

Immediate Results
Parallel Execution
Continuous Visibility
Phased Approach
Iterative Risk Reduction

BENEFIT

Immediate Impact
Every Step
Every Phase

WWW.ERACENT.COM

ERACENT ARMORED

ZERO TRUST RESOURCE PLANNING (ZTRP)

Move Beyond Discussion....
Successfully Implement Zero Trust Architecture and Manage Your Zero Trust Program

OVERVIEW

Zero Trust is critical to reducing cyber related risk. Zero Trust is achievable now. The concept of Zero Trust is simple.

Never Trust, Always Verify

THE REALITY

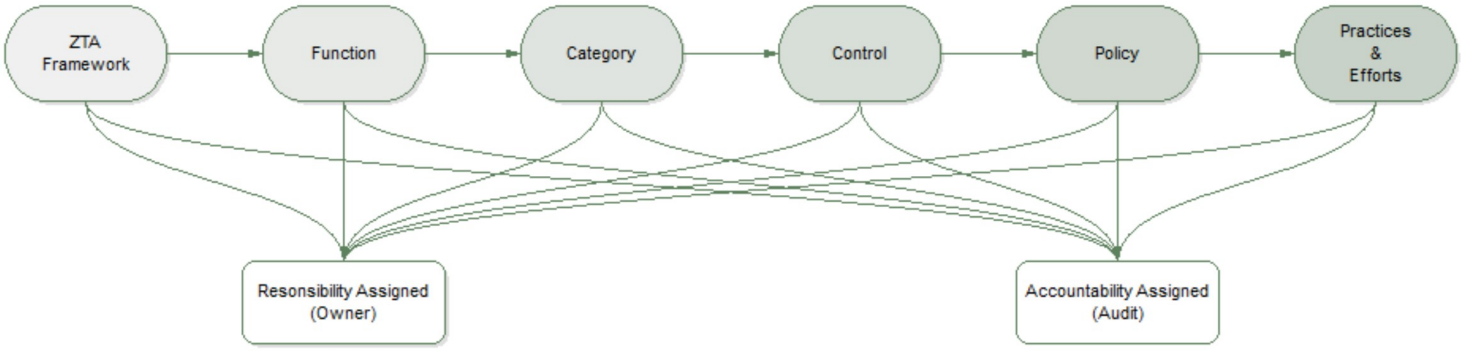
The Zero Trust Architecture is a reality. Organizations fail to implement Zero Trust due to partial adoption and implementation. Missing links are:

1. **Framework**—Adoption of a a Cyber Risk Based Approach leveraging a flexible and detailed framework.
2. **Ownership**—Assignment of ownership across endpoints, software ,networks, systems, controls, policies, etc.
3. **Prioritization**—a failure to classify and prioritize the most critical systems, data, networks, individuals that access your
4. **Discovery** — Adoption of enterprise wide discovery that tightly integrates into the ITAM solution
5. **ITAM** — a unified system that merges all aspects of ITAM into a single transparent system
6. **Data Enrichment**—Bringing critical data, providing greater context with respect to discovered assets
7. **Application Analysis**—Zero Trust does not stop at the network. Understanding and removing risk related to Proprietary, Open Source, and In House developed software
8. **Visibility**—over what is newly discovered on the network. This includes hardware, virtual assets, and software. Visibility into data and intelligence gathered. Visibility at a macro and micro level

- Identification
- Device
- Applications
- Data
- Network
- Infrastructure
- Intelligence
- Automation
- Governance

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

Framework Management—Actionable Governance



ACTIONABLE GOVERNANCE

The Zero Trust Architecture requires the implementation of Cyber Security related controls, policies, practices, ownership, transparency, and audit. Attempting to achieve Zero Trust without a Risk Based framework approach creates disorganization, chaos, and significant overages in spend.

Through role based implementation of the Framework, the organization can divide and conquer. This allows all owners to take on areas specific to them, and assign forther ownership on subordinate items. This capability rapidly increases update and execution to the framework.

While managing the framework, organizations can adopt as many features or as few features as is appropriate. Each framework item can have distinct owners or one owner can be charged with everything. Each item can be measured by a metric. Each item can be scheduled for audit.

By allowing role based access to all areas of the platform, adoption and implementations is dramatically accelerated. With roots in the NIST Cyber Security Framework, Framework management can start small and iteratively expand. Organizations that require adherence to many frameworks or regulations are not impeded from expanding past the Zero Trust Framework into areas such as CMMC, CSF, GDPR, and others.

And, because one system holds all of the documented processes, owners, policies, transparency is built in. Instantaneous reports can present status, completion of tasks, third parry integrations, relationship of policy / practices to other areas such as orphaned ownership, endpoint and vulnerability information, end of life data, risky open source libraries, data processes and approvals, endpoint approvals, etc. Governance goes beyond documenting things to do but active measurement of completions, status, risk.

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

Ownership — Built into every aspect of the Platform

OWNERSHIP — A KEY TO REDUCING CHAOS

The Zero Trust Architecture requires that actual ownership is assigned to everything that is done. This allows the adoption to start out slow, perhaps with only a single person flagged as an owner. As adoption of the Zero Trust Framework occurs, a natural progression of ownership occurs. Each owner contributes to the identification and reduction of cyber related risk. Each owner assists in identification of required information. Each owner becomes part of a mesh that detangles and simplifies Cyber Security initiatives and moving to a successful implementation of Zero Trust.

More elements are adopted, more functionality implementation of controls, policies, practices, ownership, transparency, and audit. Attempting to achieve Zero Trust without a Risk Based framework approach creates disorganization, chaos, and significant overages in spend.

Through role based implementation of the Framework, the organization can divide and conquer. This allows all owners to take on areas specific to them, and assign forther ownership on subordinate items. This capability rapidly increases update and execution to the framework.

The key is to just start the program. Start as large or as small as possible. Fill in as many gaps as possible. Identify as much Risk as possible. Iteratively identify what is most important. Iteratively remove risk from the board.

One thing is certain, without ownership there is no responsibility and no accountability. To coin a phrase, assign the first few owners to get the ball rolling, then—**just do it!**

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

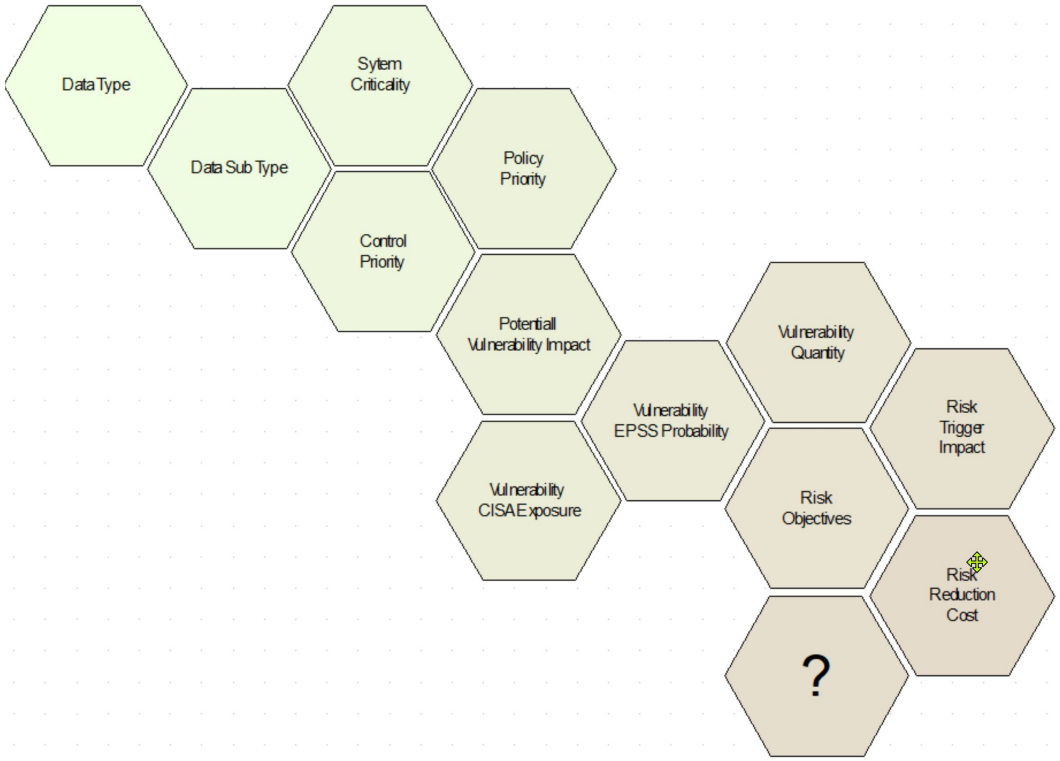
Prioritization — Multiple methods to Prioritize Effort

PRIORITIZATION — A KEY TO CREATING FOCUS

Prioritization can take the form of many methods.

Squeaky Wheel— The loudest voice will control the conversation, and set prioritization. This method is highly subjective and leads to poor implementation of Zero Trust.

Most Visible—Systems, data, or groups that are most the most visible may control the conversation. Incidents that impact larger groups may create the most embarrassment, create the most news, oftent tend to drive effort. The method is highly subjective and does not prioritize based on most critical impact.



Haphazard Approach — Tends to have no prioritization at all. Efforts, spend, focus are item du jour. All team members focus on what they believe is important. Work started today may be put aside and a new thing worked on tomorrow. Risk is never reduced, accomplishments never occur

Risk Based Approach— A risk based approach to Cyber Security, Risk Reduction, and Zero Trust leverages objective prioritization.

The Zero Trust Framework provides the flexibility to use a multitude of objective prioritization methods. Decision making, focus, and effort looks to leverage built in prioritization.

Implementation of the ZTA framework provides key reference points, ownership, value assessments, and other value add. Governance is implemented, automations of critical data is acquired, decision making is supported, and continuous improvement occurs. Cyber related risk is reduced.

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

CITAM Discovery — Not a once and done exercise

CITAM, or Cyber Security IT Asset Management, is a requirement of Zero Trust Architecture. Further, discovery must be continuous and autonomous. Going beyond a set of controls, policies, and practices, the ZTRP comes with discovery built in. ZTRP Discovery provides a wide range of data related to what is on the network, when it was first seen, and how it is configured. Discovery extends to all networked devices. Detailed information is acquired for compute devices (windows, linux, unix, VM's, workstations, mobile devices, servers, network devices, printers, scanners, Android, Apple, etc.) is acquired.

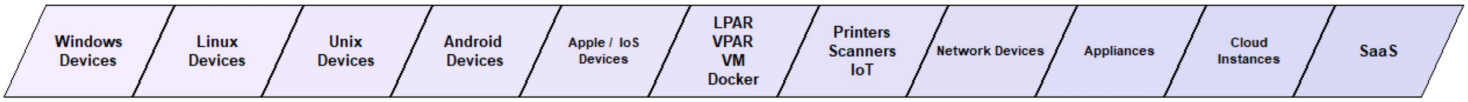
Data is collected through base discovery processes with extended data brought in through agent or agentless methods. Data extends far beyond typical collection methods. Disk space, disk serial numbers, bios info, connected devices, removeable storage, all software installed, drivers, services. A complete understanding with significant cyber implications are gained.

- **Network device detection (Network Probe)** – Detects servers, PCs, hubs, switches, routers, parent and child relationships and more.
- **Cross-platform network discovery** for Windows, all flavors of UNIX, Solaris, True64, HPUX, Linux, Mac, AIX, AS/400, Android and Blackberry devices. Complete and accurate details are provided about machine configuration, installed software, peripherals and more.
- **Agentless or agent-based scanning**, with the same results and degree of accuracy/completeness.
- **Scanning of virtual environments**, with reporting on the relationships between physical hosts and virtual guests. Environments currently include VMWare ESX, Solaris Zones and AIX LPARS and Microsoft Hyper-V, among others. Virtual Application detection is provided for Microsoft App-V/Softgrid, Citrix XenApp, and VDI/Thin Client environments.
- **Software ID Tag Detection** – Supports the detection and reporting of software ID tags that meet the ISO 19770-2 standard.
- **Software Utilization monitoring –** Can monitor specific products down to the keystroke and mouse-click level. While an organization may be compliant based on purchases-to-installations, if nobody is using a license actively, there may be savings opportunities (e.g., re-allocate licenses, scale back maintenance, utilize free viewers or concurrent licenses for less frequent users).
- **Server Utilization monitoring** – By looking at servers core-by-core and process-by-process, the system can identify which virtual or physical servers are overloaded or under-utilized. This data can help when assessing which physical servers may be candidates for virtualization and resulting savings (e.g., power, cooling, floor space charges, etc.).
- **Software Distribution** – Enables the **creation and deployment of .msi, .pkg and .rpm packages**. In the package builder, instructions may be defined for silent (no user interaction) installation and uninstallation of these packages. The deployment package may be configured to target devices based on hardware attributes, whether particular applications are or are not installed on a given machine, or a combination of these.
- **ITMC Discovery can also assist with the distribution process performed by SCCM** by identifying all target machines based on hardware attributes, whether particular applications are or are not installed on a given machine, or a combination of these. This list of machines can then be sent directly to an existing SCCM collection, or a new SCCM collection can be created and populated. All of these actions can be performed within the native ITMC web interface.
- **Application Dependency Mapping** identifies what software is speaking to external and internal processes. What is the service or application, what port is it using, what port is it conneting to, what far end IP is it speaking to.

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

CITAM Management— Cyber IT Asset Management Comes Before Protections

Discovery is the first stage of Cyber Security IT Asset management. Once data is acquired it must be leveraged by multiple teams that span Cyber Security, IT Administration, Human Resource, Risk, Audit, and Financial Management programs. Why is this important? Because all too often IT Assets / Endpoints / Computers / Devices are managed by multiple teams using different mechanisms, isolating information. This creation of data silos causes a separate vision of truth for each. Silos of information waste time, money, and accuracy. Silos also increase risk and camouflage the threat landscape.



An abridged list of CITAM benefits:

- **Lifecycle Management** – From acquisition to disposal, all assets are properly managed.
- **Disposal management—** Key to Lifecycle management is how you dispose of assets. All of the data you are protecting still exist on hard drives prior to disposal. Managing the method of disposal, acquisition of disposal certificates are critical.
- **Software Management—** Full visibility into the distribution of software, patches, updates, operating systems, drivers, services and additional details are visible. Support contracts are managed. Cost is reduced. Exposure is identified.
- **Utilization**—tells a story on how assets are used. The collection of time series data related to disk, network, cpu utilization allows for better and more efficient configurations. Additionally, data supporting anomaly detection is also acquired. Utilization can present trends and lead to better management of key assets.
- **Application Dependency Mapping—**tells the story on how software is used and what it speaks to. A better understanding of application and communications leads to a more secure environment.
- **Virtual Instance Detection**— Virtual instances may include virtual machines, docker images, and other items. While these are normally seen on servers, they may also be propagated to workstations. Understanding where ethese are can lead to answering the question of why they are. Remember, every VM is a compute instance. A failure to manged these just as every other compute instance is managed leads to additional risk. Are they patched? Are they vulnerable? Do they contain obsolete software? Are they provisioned to do dangerous things?
- **Endpoint Approval—**Every major cyber framework has a requirement to understand the role of endpoints on the network. A unified solution allows for rapid assessment and approval of endpoints.
- **End Point Categorization—**Association of endpoints to systems allows for better management and focus. If a critical system / Platform / application consists of several endpoints then each can be a weal link. Any endpoint can be an entry point into the system and its data. Endpoint categorization allows for the documentation of what the endpoints are, who are the owners, what the value is, etc.
- **User Access**— Who is logging onto endpoints. When are they logging onto endpoints. Where did they log in from. Tracking this information provides a better ability to manage these, detect ownership, notify users when issues arise, etc.
- **Services Status**— Do you know what services are installed on endpoints? Are they running? Are they dangerous? Tracking these leads to better management of endpoints.
- **Network Config**— Many devices can contain more than one IP Address. Have more than one network interface. May have firewalls turned on or off. May have ports open. Through discovery and IT asset management leads to reduced risk.

ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

Data Enrichment—Discovering hidden asset information

Once endpoints are discovered and data is collected, enrichment must occur. Enrichment data may include power utilization, weight, BTU generation, size, and other details. Most important is Cyber related enrichment data. Most importantly, enrichment is a closed loop system that completes the picture of what has been discovered. Enrichment, in a continuous and autonomous process, has many high level and more details steps. The most critical are:

1) **Normalization**—ensures that what is discovered uses a standardized naming convention. This includes item names, publishers, manufacturers, etc. If a new item, never discovered before occurs, it is research and added to the catalog. All occurring without system administrators intervention.

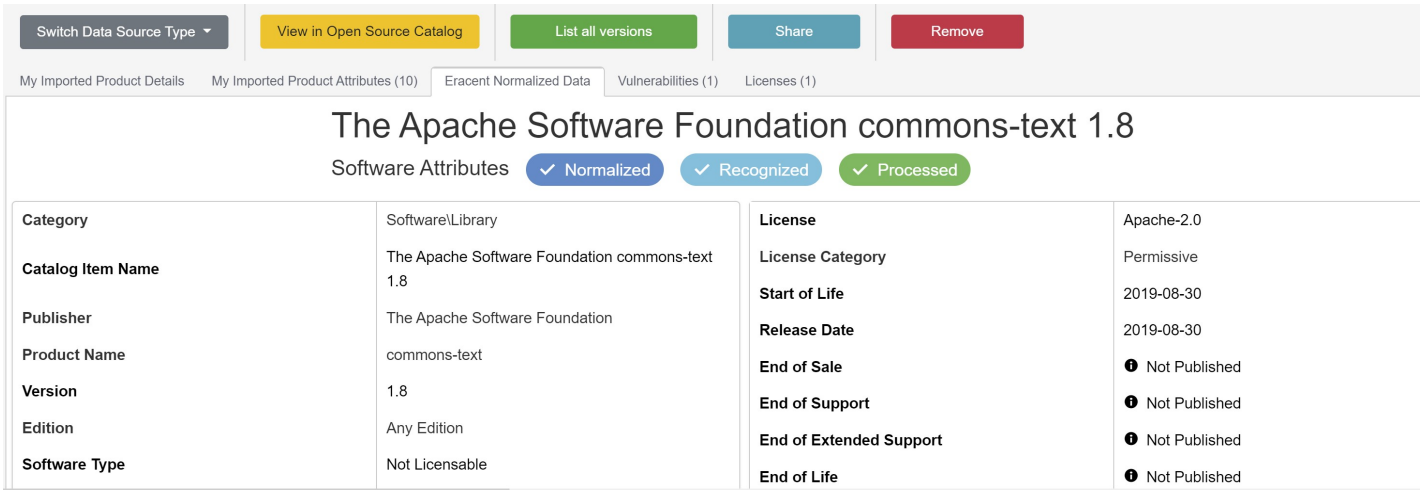
2) **Lifecycle**—collection of lifecycle data showing end of life, end of sales, end of support, and end of extended support dates. All is critical from a cyber perspective.

3) **Open Source lifecycle**—unique from commercial products, an extensive process for identifying, normalizing, and acquiring Open Source lifecycle data, also known as obsolescence, is acquired.

4) **Vulnerability Discovery**—Vulnerabilities are discovered for software, operating systems, drivers, and open source libraries.

5) **CISA / CVE Flagging**—while it is important to remediate all vulnerabilities, it is often not realistic to attempt this. Instead prioritizations are used. One method of prioritizing vulnerability focus is through the type (low, medium, high, critical). An additional method is by flagging the vulnerabilities that are on the CISA / CVE list.

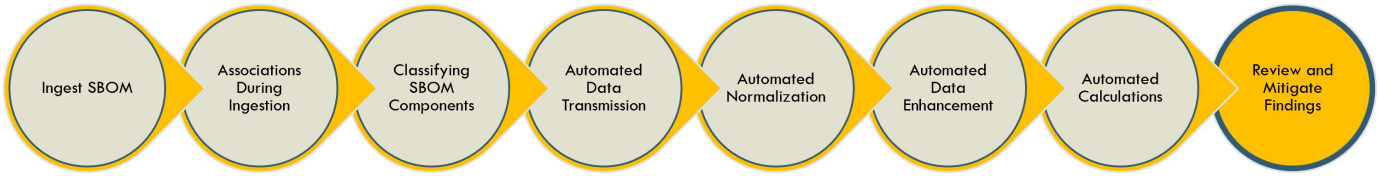
6) **EPSS Tagging**— while it is important to remediate all vulnerabilities, it is often not realistic to attempt this. Instead prioritizations are used. One method of prioritizing vulnerability focus is through the type (low, medium, high, critical). An additional method is by tagging the vulnerabilities with a probability or likelihood that the specific vulnerability will be exploited.



ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

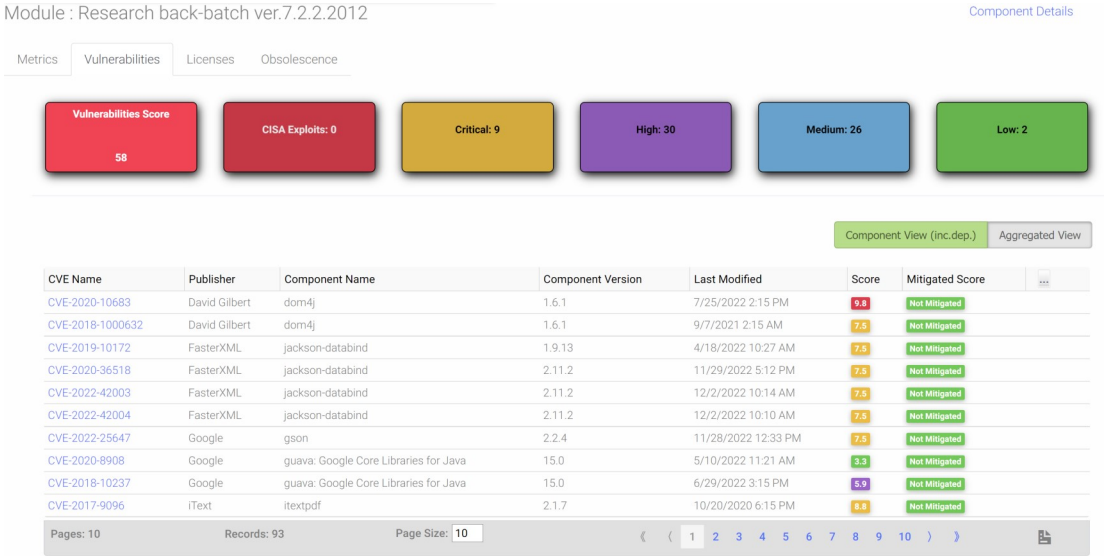
Application Risk Analysis—Quantification of Open Source Impact

Custom, in house developed, or limited distribution software creates a significant risk due to the use of Open Source libraries. Often these libraries can be compiled into a software package with no evidence that they are used. To address this risk, the concept of the SBOM was born. Software Bill of Materials, or SBOM provides detailed information into how this software is constructed and dependencies present. Eracent Armored Zero Trust Resource planning (ZTRP) comes with built in Application Risk Analysis (ARM). ARM goes beyond simplified risk assessment of individual SBOMS and allows for intelligently managing these and the risk they present. By using an intuitive and advanced process, managing these types of assets are dramatically accelerated.



Critical Features of Application Risk Management

- **SBOM Ingestion** – Ingest an manage SBOMS from several to thousands.
- **Normalization** — autonomous normalization of publishers, names, and other details.
- **Vulnerability Discovery** — of all libraries used at the SBOM level, and propagation across all SBOM's.
- **Grouping** — of SBOMS in a hierarchy of associations.
- **Vulnerability Enrichment**—that brings in CISA / CVE flags and EPSS scores.
- **System Association**—Association of SBOMs against systems. So if one system is created through multiple elements, each can be brought in. In the example of an ERP system there could be application layer SBOMS, Database SBOMS, workflow system SBOMS, etc.
- **Ownership**—of SBOMS. Who owns the SBOM, Who is responsible for what is discovered and risk.
- **Mitigation**—Vulnerabilities can be audited, refuted, and mitigated based on use.
- **Obsolescence**—of libraries are identified with graduations of concern. Is the library the most recent one, how old is it, how many newer versions exist, when was the last version released. With this information an organization can transparently understand the risk of using a library in the event that it is no longer supported by the publishing group.



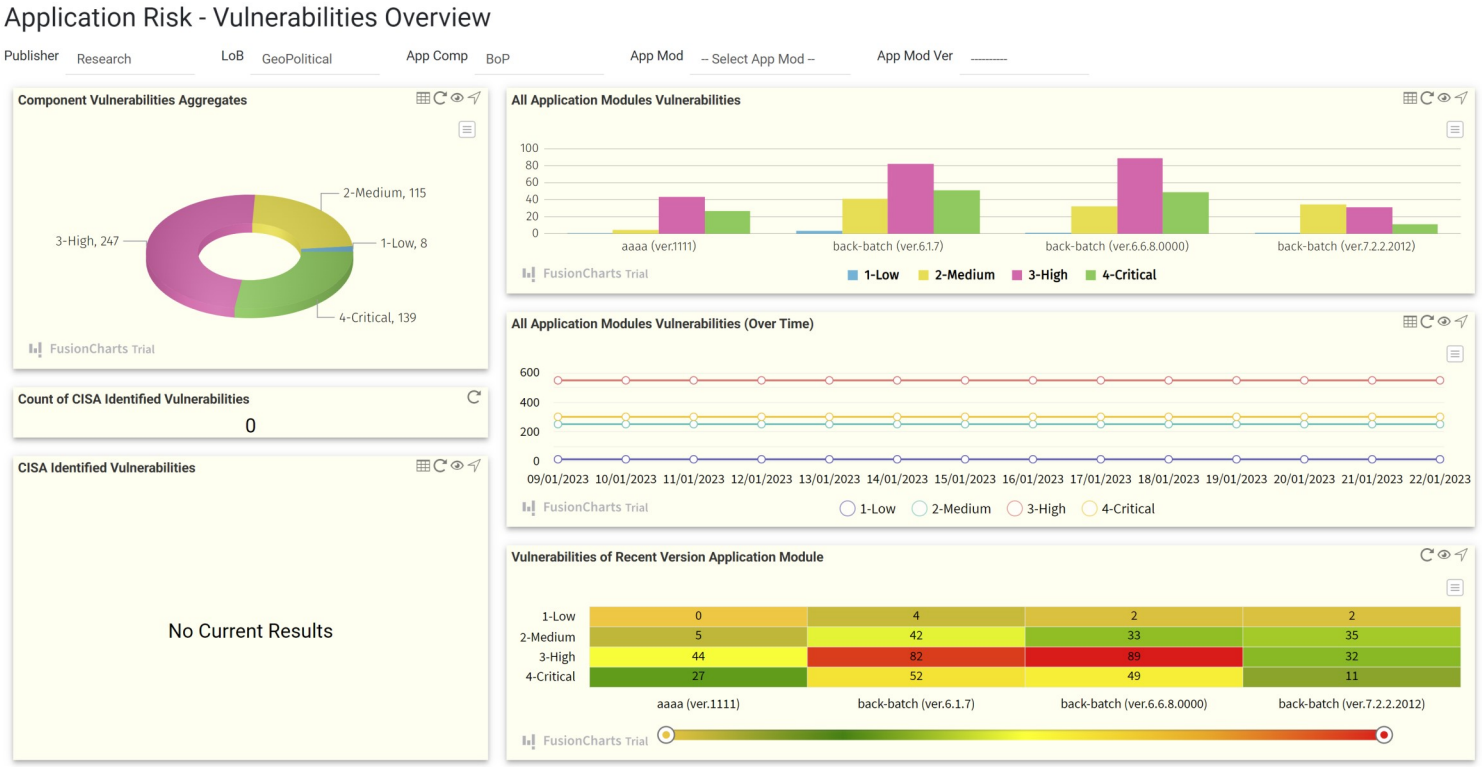
ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

Intelligence—Unlocking the value of the ZTRP

ZTRP comes with a complete Cyber Intelligence engine built in. Managing data qeries, filters, Drill down queries, time series metric collection, transform / load queries, export queries, and dashboards are managed from within ZTRP.

Cyber Intelligence Elements

- **Data Query** – Data Queries bring data into the dashboard layer. Data queries may leverage filters, hierarchical filters, and drill down queries.
- **Filter** – allows data presented on a dashboard to be dynamically changed. Filters may be dependent on other filters.
- **Drill Down Data Query** – allows for clicking on a dashboard visual element and bringing forward additional results.
- **Metrics** – are a specialized query that runs at predetermined intervals to acquire time series data.
- **Alerts**—allows for notification of a metric goes out of tolerance for eather warning thresholds or critical thresholds.
- **Export Data Queries**—allows for a query results to be executed and forwarded to an identified individual, individuals, or distribution lists.
- **Dashboards**—are an orchestrations of multiple charts, queries, filters, and drill downs into a single unified visual view.
- **Transform / Load**– Sometimes data most be moved from staging tables, or simplified to allow for faster aggregated results to be brought forward. Transform / load queries can run and redetermined intervals during the day, week, month, or year.

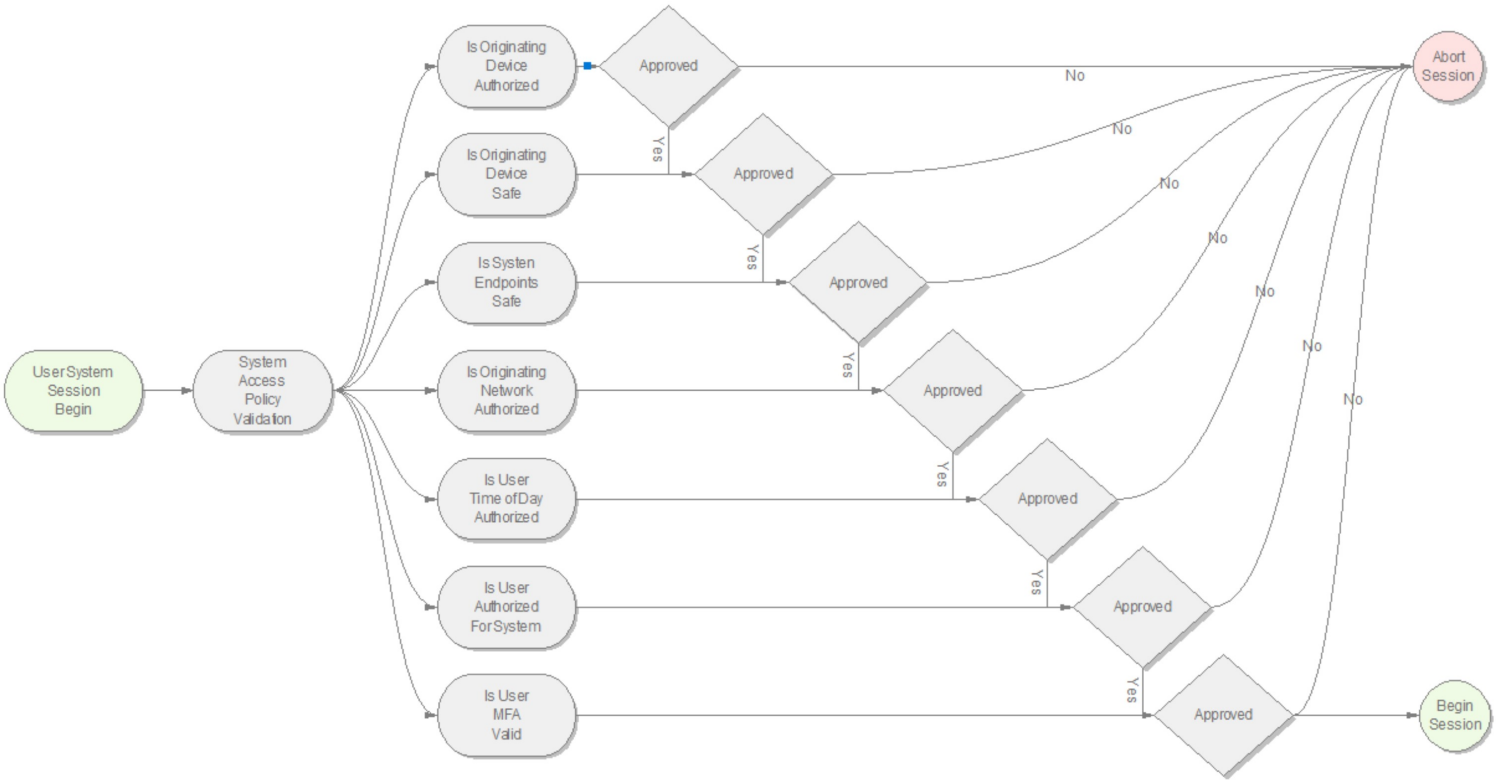


ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

ZTRP Use Case—Dynamic Authorization to Access

Zero Trust requires an orchestration of multiple key areas related to Cyber Security. One critical area is the authentication of who is accessing systems, from where. In this use case we ask the question, what if an valid person with valid credentials, but other critical defects attempts to log into a high risk system. If they have critical vulnerabilities are they allowed access? What if the vulnerabilities are on the CISA / CVE list? What if the endpoints associated with a critical risk system has critical vulnerabilities, is it allowed to operate? By allowing this information to be exposed, we can corelate this data with policies. If elements are non compliant, exposing these to the access system allows a more control and ability to assess items critical to Zero Trust.

Zero Trust considers multiple sources of information

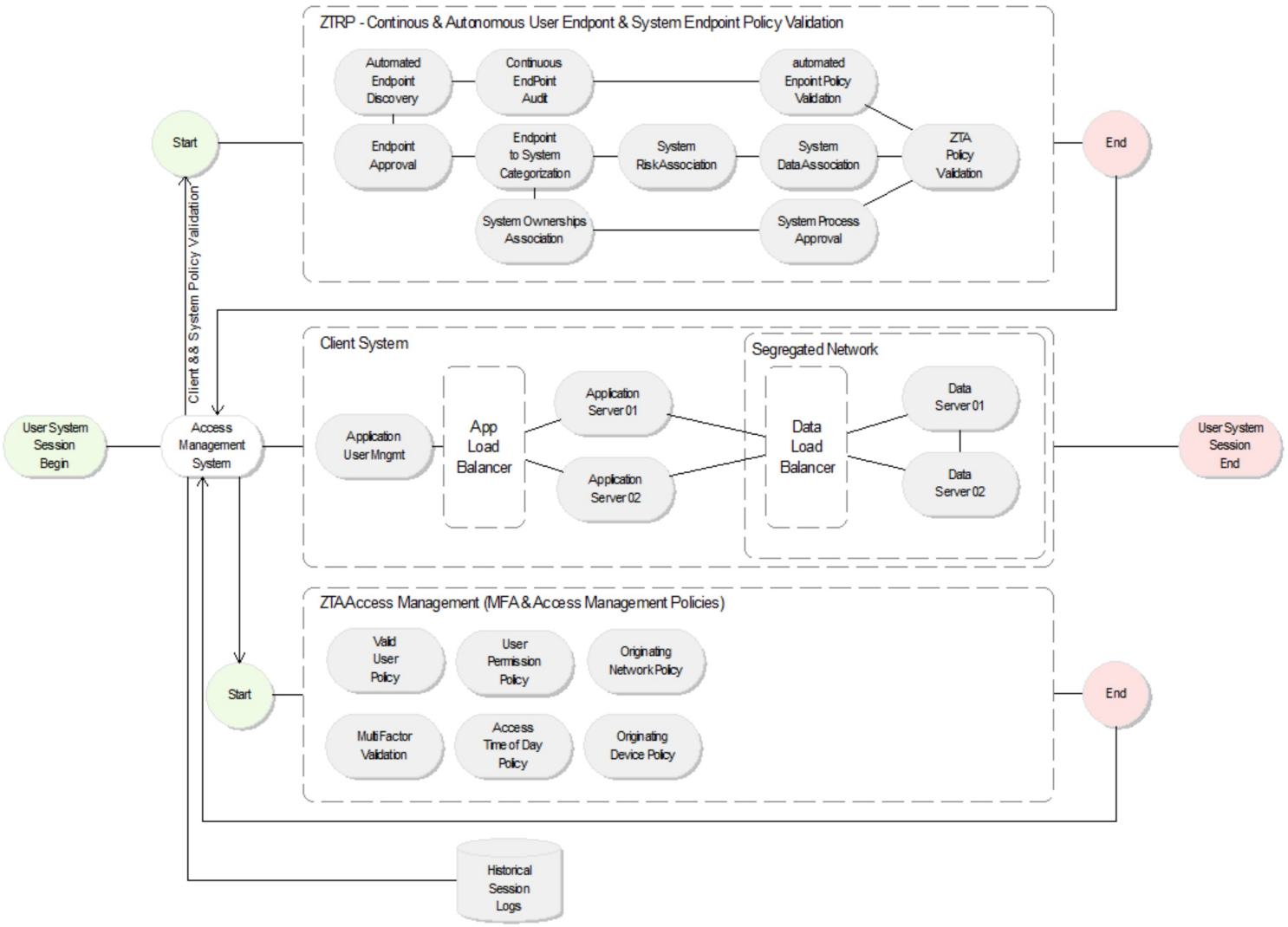


ERACENT ARMORED ZERO TRUST RESOURCE PLANNING (ZTRP)

ZTRP Use Case—ZTRP Place in System Access

Zero Trust Resource planning allows for various Cyber related policies to be controlled through a centralized system. Critical to Zero Trust is understanding what policies may be in place and deciding if those are used to control user sessions accessing systems. In this variation on our access use case we can see that autonomous audit of the endpoints allows discovery if an endpoint moves the user workstation or system endpoints out of compliance. Additionally, since other artifacts are identified in your MFA system, Cyber ITAM system, and various other details, the potential for a more controlled Zero Trust is possible. The key is, if the information exists it can be used.

Zero Trust considers multiple sources of information



ERACENT ARMORED

ZERO TRUST RESOURCE PLANNING (ZTRP)

Move Beyond Discussion....
Successfully Implement Zero Trust Architecture and Manage Your Zero Trust Program

Zero Trust is critical to reducing cyber related risk. Zero Trust is achievable now. The concept of Zero Trust is simple if a continuous and methodical approach is adopted. Eracent Armored Zero Trust Resource Planning provides you with the tools and process to achieve ZT.

Never Trust, Always Verify

Never Trust, Always Verify becomes just another Cyber Scurity platitude without embracing key requirements. Assign ownership, detail objectives, discovery Core Data, corellate context data, work toward objectives, audit results. Zero Trust Resource Planning (ZTR) provides this structure through the Zero Trust Framework, built

- Identification
- Device
- Applications
- Data
- Network
- Infrastructure
- Intelligence
- Automation
- Governance