Eracent Armored™

Zero Trust Resource Planning (ZTRP™)

Move Beyond Discussion….

Successfully Implement Zero Trust Architecture and Manage Your Zero Trust Program

June 2023

Introduction

Zero Trust Architecture is critical for reducing cyber-related risk. Zero Trust can be achieved now. The concept underpinning Zero Trust is simple:

Never Trust, Always Verify.

The Reality

Zero Trust Architecture is a reality. However, despite hundreds of vendors offering "Zero Trust solutions", most organizations have failed to actually implement Zero Trust due to partial adoption and incomplete vision. The all-too-common approach of simply buying and implementing tactical security detection and mitigation tools does not result in adequate protection. Let's learn why and what will work.

A successful Zero Trust implementation requires these elements:

1) **Framework**—Adoption of a Cyber Risk-Based Approach, leveraging a flexible and detailed framework.
2) **Ownership**—Assignment of ownership across endpoints, software, networks, systems, controls, policies, and more.
3) **Prioritization**—The classification and prioritization of the most critical systems, data, networks, and individuals that comprise your computing environment.
4) **Discovery** — Adoption of enterprise-wide hardware and software discovery that provides up-to-date and complete foundational data for multiple initiatives, i.e., Cybersecurity, IT Service Management (ITSM), IT Asset Management (ITAM) and Software Asset and License Management (SAM).
5) **IT Asset Management (ITAM)** — A unified system that offers visibility and brings together all aspects of asset lifecycle management.
6) **Data Enrichment**—Bridging data gaps and providing greater context about the products that are in use, empowering users for more effective reporting and actions.
7) **Application Analysis**—Zero Trust does not stop at the network. It's critical to understand and remove various risks related to Proprietary, Open Source, and in house-developed software.
8) **Visibility**— Knowing what is newly discovered on the network, including hardware, virtual assets, and software. An immediate view into data and intelligence that has been gathered, at macro and micro levels.

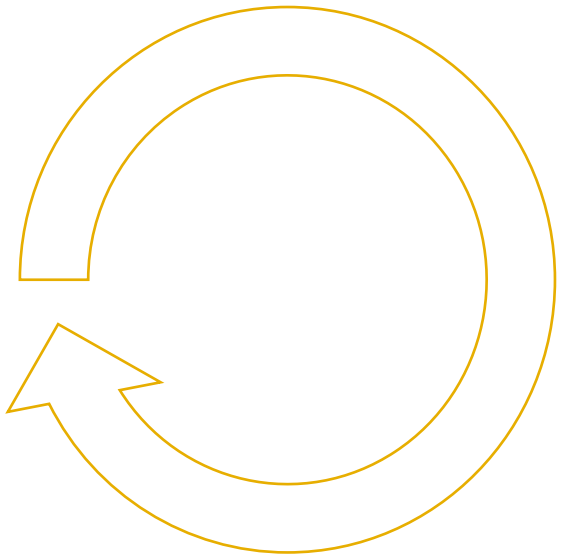
Introducing Eracent Armored™ Zero Trust Resource Planning™ (ZTRP™)

To guide successful Zero Trust architecture implementations – and to support effective ongoing ZT programs – Eracent introduces the Zero Trust Resource Planning (ZTRP) toolset.

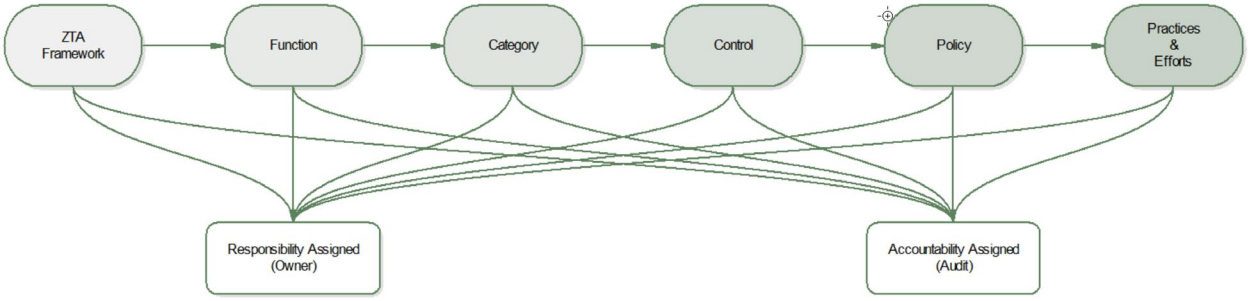
ZTRP is a focused application of Eracent's Intelligent Cybersecurity Platform™ (ICSP™), providing structured and automated process management to ensure that every endpoint and application is covered, and no critical steps are overlooked. ***Even if you are utilizing other tactical security applications for identification and mitigation, ZTRP brings all aspects of your cybersecurity and Zero Trust initiatives together and provides total visibility and centralized management and reporting.***

Based on the broader ICSP platform, ZTRP is both framework-driven and flexible, enabling your organization to work towards meeting industry standards while supporting aspects that are unique to your program. ZTRP also provides very detailed reporting as well as summary dashboards to track metrics and monitor progress towards meeting your program's goals.

ZTRP is a part of the Eracent Armored™ family of cybersecurity solutions from Eracent. Eracent has been providing exceptionally accurate and high-quality foundational data about enterprise-class networks, computing devices and software since 2000. Its highly scalable discovery, utilization, lifecycle management and data enrichment solutions are in use in some of the largest, most complex computing environments around the world.



Framework Management—Actionable Governance



Actionable Governance

The Zero Trust Architecture requires the implementation of Cybersecurity related controls, policies, practices, ownership, transparency, and audit. Attempting to achieve Zero Trust without a risk-based framework approach results in disorganization, chaos, and significant overages in spending.

Through role-based implementation of the framework, an organization can divide and conquer. This allows all owners to take on areas that are specific to them and assign further ownership on subordinate items. This capability rapidly increases updates and execution of tasks related to the framework.

While managing the framework, organizations can adopt as many – 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 and each item can be scheduled for audit.

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

And, if a single management system holds all the documented processes, owners, and policies, transparency is built in. Detailed reports can present status, completion of tasks, third-party integrations, and the relationship of policies and practices to other areas. These areas can include orphaned ownership, endpoint and vulnerability information, end-of-life data, risky open source libraries, data processes and approvals, endpoint approvals, and much more. Governance goes beyond documenting things to do and includes active measurement of task completions, status, and risk.

Ownership — Built into Every Aspect of the Platform

Ownership – A Key to Reducing Chaos

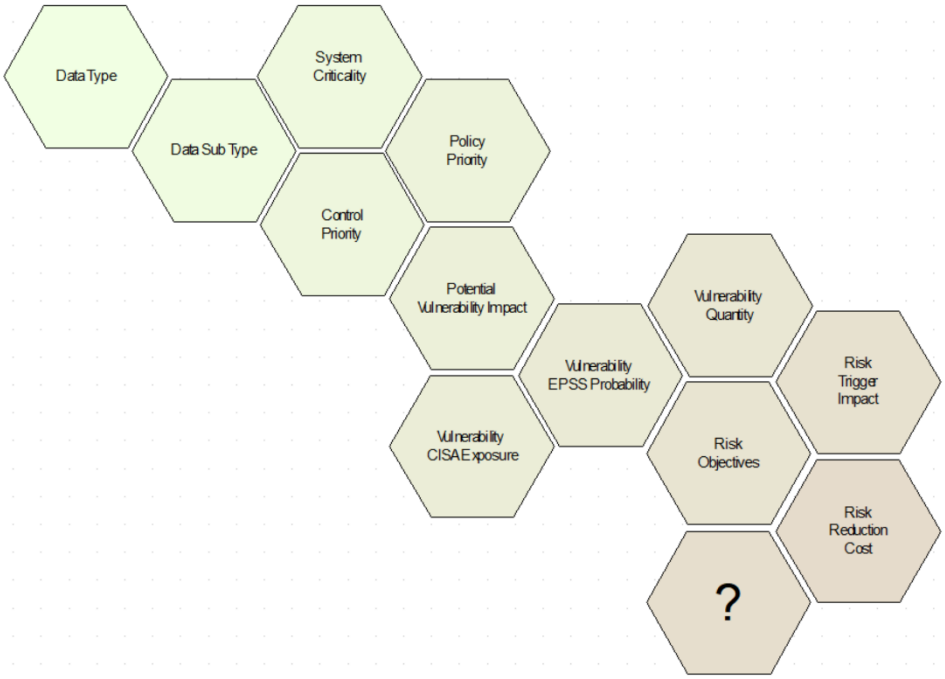
The Zero Trust Architecture requires that clearly defined ownership is assigned to everything that is done. This allows the adoption to start out slow, perhaps with only a single person flagged as an owner. As adoption of the Zero Trust Framework occurs, a natural progression of ownership occurs. Each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

More elements are adopted, and more functionality is utilized during the expanding implementation around controls, policies, practices, ownership, transparency, and audit. As stated earlier, attempting to achieve Zero Trust without a Risk-Based framework approach results in disorganization, chaos, and significant overages in spending.

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 many elements of 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!**

Prioritization — Multiple Methods to Prioritize Effort



Prioritization – A Key to Creating Focus

Priorities can be set using a number of different approaches. These include:

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 conversa□on. Incidents that impact larger groups may create the most embarrassment or make the most news, so these often tend to drive effort. The method is highly subjective and does not prioritize based on the most critical impact.

Haphazard Approach — This approach tends to have no prioritization at all. Efforts, spend and 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, and accomplishments are rarely achieved.

Risk-Based Approach— A risk-based approach to Cybersecurity, 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 all look to leverage built-in prioritization.

Implementation of the Zero Trust Architecture (ZTA) framework provides key reference points, ownership, value assessments, and other value-add items. Governance is implemented, automation of critical data is acquired, decision making is supported, and continuous improvement occurs. Cyber-related risk is subsequently reduced.

CITAM Discovery — Not a “One and Done” Exercise

CITAM, or Cybersecurity IT Asset Management, is a requirement of Zero Trust Architecture. It's not only required, it provides data that forms the entire foundation of an effective Zero Trust program. Further, discovery must be continuous and autonomous.

Going beyond a set of controls, policies, and practices, the Zero Trust Resource Planning (ZTRP) platform includes best-in-class cross-platform discovery. ZTRP Discovery™ is scalable to hundreds of thousands of devices, and it 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 that may be a point of potential risk. Detailed information is gathered for every computing device on every platform - Windows, Unix, Linux, VMs, Mac, servers, network devices, workstations, Apple and Android-based mobile devices, printers, scanners, and more.

Data is collected through discovery processes that use both agent-based and agentless methods. ZTRP Discovery collects far more extended data than typical collection methods. Extended data includes disk space, disk serial numbers, BIOS info, connected devices, removable storage, all installed software, drivers, services, and much, much more. **This data provides cyber programs with a complete understanding of everything on the network as well as anything that may have significant cyber implications.**

ZTRP Discovery provides the following:

- **Network device detection (Network Probe)** – Detects all 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, Apple and Android 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 and completeness.
- **Scanning of virtual environments**, with reporting on the relationships between physical hosts and virtual guests. Environments currently include VMWare ESX, Solaris Zones, 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 the usage of 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). From a security perspective, unused software may be removed, eliminating a potential point of risk on a device.

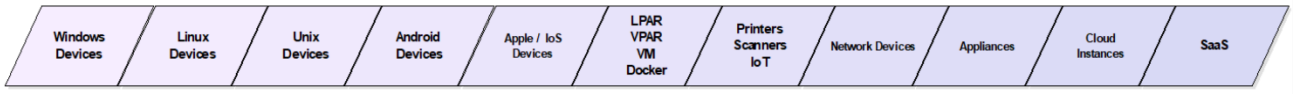
- **Server Utilization monitoring** – By looking at servers core-by-core and process-by-process, the system can identify which virtual or physical servers are overloaded or under-utilized. This data can help when assessing which physical servers may be candidates for virtualization and resulting savings (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 various criteria. 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 connecting to? To what far end IP is it speaking?

CITAM Management— Cyber IT Asset Management Comes Before Protections

Discovery is the first stage of Cybersecurity IT Asset Management. Once data is acquired, it must be leveraged by multiple teams that span Cybersecurity, IT Administration, Human Resources, Risk, Audit, and Financial Management programs. Why is this important? Because all too often, IT Assets - including endpoints, computers, and other devices - are managed by multiple teams using different mechanisms, thus isolating invaluable information. This creation of data silos causes a separate vision of the "truth" for each team. Silos of information waste time and money and can negatively impact accuracy. Silos also increase risk and camouflage the threat landscape.



The following is an abridged list of CITAM benefits:

- **Lifecycle Management** – From acquisition to disposal, all assets are properly and proactively managed.
- **Disposition Management**— Key to Lifecycle management is how you dispose of assets. All of the data you are protecting still exists on hard drives prior to disposal. Managing the method of disposal, establishing a secure chain of custody and recording of disposal certificates are all critical steps.
- **Software Management**— Full visibility into the distribution of software, patches, updates, operating systems, drivers, services, and additional details is essential. Support contracts are managed, costs are reduced, and potential exposures are identified.

- **Utilization**—These metrics tell the story of how assets are used. The collection of time-series data related to disk, network and CPU utilization allows for better and more efficient configurations. Additionally, data supporting the detection of anomalies is also acquired. Utilization can present trends and lead to better management of key assets.
- **Application Dependency Mapping**—Dependency Mapping shows how software is used and its context in the computing environment. A better understanding of applications and their communications and interactions 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 these are can help you answer the question of why they are. Remember, every VM is a computing instance. A failure to manage these just like every other computing instance 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 every endpoint on the network. A unified solution allows for rapid assessment and approval of endpoints.
- **Endpoint Categorization**—The association of endpoints to systems allows for better management and focus. If a critical system, platform, or application consists of several endpoints, then each of these can be a weak 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 the owners are, the value each endpoint provides, and more.
- **User Access**— Who is logging onto endpoints? When are they logging onto endpoints? From where did they log in? Tracking this information provides a better ability to manage these actions, 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 services leads to better management of endpoints.
- **Network Configuration**— Many devices can contain more than one IP Address. They may have more than one network interface. They may have firewalls turned on or off or may have ports open. Managing configurations through discovery and IT asset management leads to reduced risk.

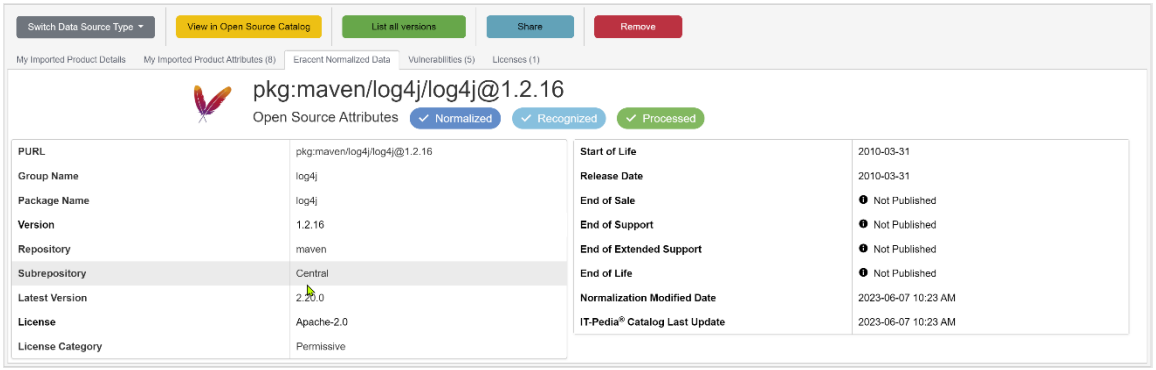
Data Enrichment—Revealing Hidden Asset Information

Once endpoints are discovered and data is collected, enrichment is the next key step. Enrichment data often includes attributes that cannot be discovered, or which is not included in procurement data. Traditionally, it has often required a lot of manual research to find this information which can be scattered about through many disparate sources.

Enrichment data about hardware devices may include power utilization, physical dimensions, weight, BTU generation, and other details. Most important is cyber-related enrichment data. Data enrichment is a closed loop system that completes the picture of what has been discovered and is being managed.

A continuous and autonomous enrichment process includes many high level and detailed steps. The most critical elements include:

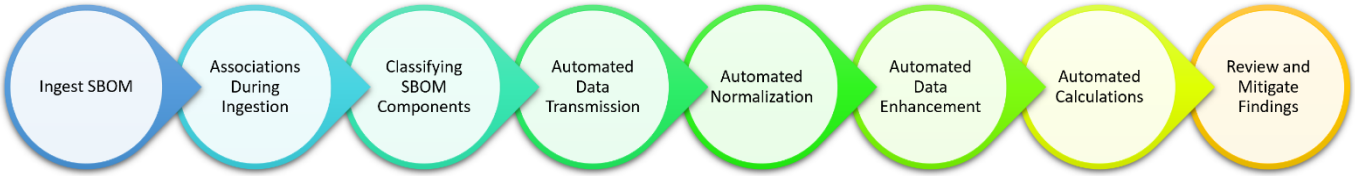
- **Data Normalization**—This ensures that the representation of what is discovered uses a standardized naming convention. This includes item names, publishers, manufacturers, and more. If a new item that has never been discovered before appears, it is researched and added to the catalog. All of this happens without system administrator or user intervention.
- **Lifecycle Dates**— An enrichment data library provides a collection of manufacturer-provided lifecycle data that includes general availability (GA), end of life (EoL), end of sale, end of support (EoS), and end of extended support dates. All of these dates are critical from a cyber perspective.
- **Open Source Lifecycle Management**—An extensive process for identifying, normalizing, and acquiring Open Source lifecycle data provides the basis for obsolescence management.
- **Vulnerability Discovery**—Vulnerabilities are discovered and reported for software, operating systems, drivers, and open source libraries.
- **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 to flag the vulnerabilities that are on the CISA / CVE list.
- **EPSS Tagging**— As stated above, while it is important to remediate all vulnerabilities, it is often not realistic to attempt this. In addition to prioritizing vulnerability focus through the type (low, medium, high, critical), another method is to tag the vulnerabilities with the probability or likelihood that each specific vulnerability will be exploited.



Application Risk Analysis—Quantification of Open Source Impact

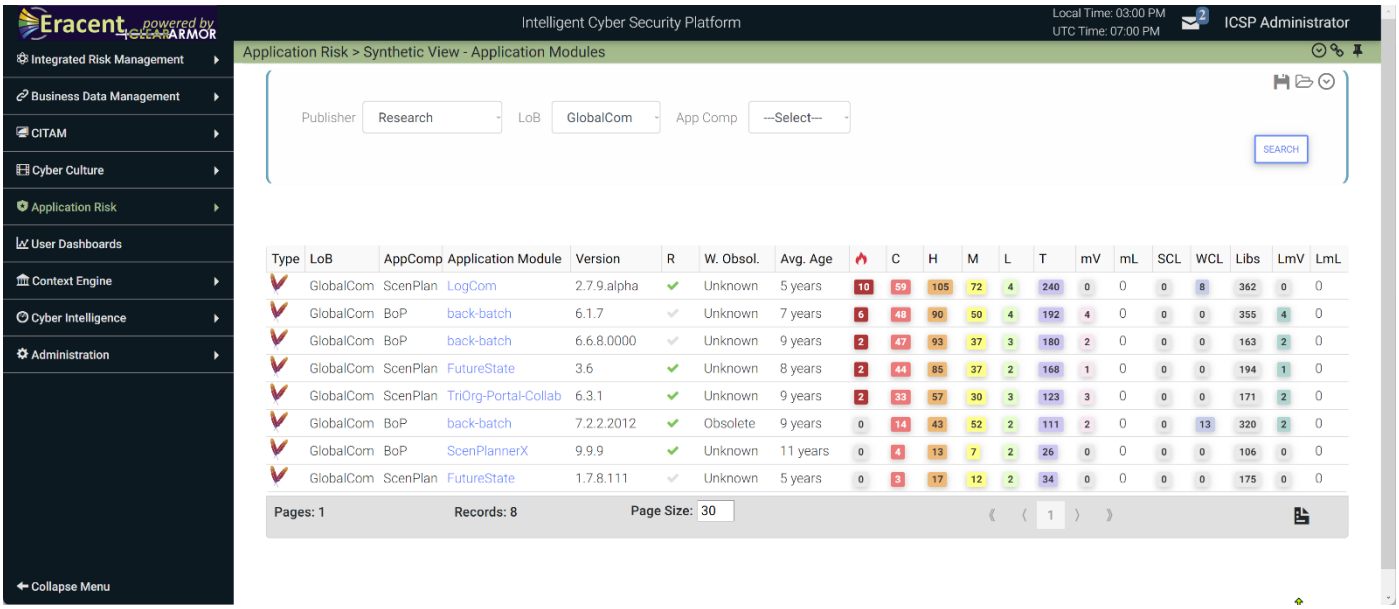
Custom, in-house developed, or limited distribution software creates a significant risk due to the use of Open Source libraries. Often these libraries can be compiled into a software package with no evidence that they are used. To address this risk, the concept of the Software Bill of Materials, or SBOM, has been adopted for cybersecurity purposes.

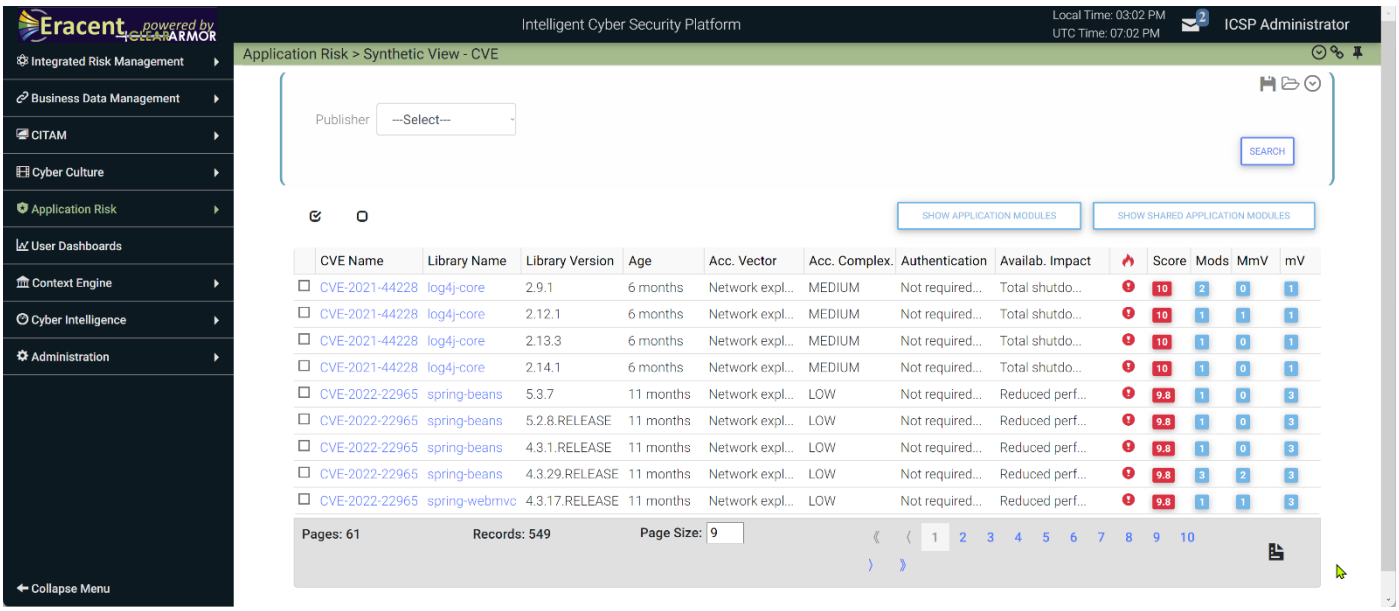
SBOMs act as an "ingredients list", providing detailed information about how software is constructed and any dependencies present. The Zero Trust Resource Planning (ZTRP) system comes with built-in Application Risk Analysis (ARM). ARM goes beyond simplified risk assessment of individual SBOMS and enables intelligent management of the entirety of an organization's SBOMs - and the risk they pose - as a whole. By using an intuitive and advanced process, the management and analysis of these types of assets is dramatically accelerated.



Critical Features of Application Risk Management

- **SBOM Ingestion** – Ingest and manage SBOMS in quantity, from a handful to many thousands.
- **Normalization** — Automatic normalization of publishers, names, and other details.
- **Vulnerability Discovery** — for all libraries utilized at the SBOM level, with propagation across all SBOMs.
- **Grouping** — of SBOMs in a hierarchy of associations.
- **Vulnerability Enrichment**—that brings in CISA / CVE flags and EPSS scores.
- **System Association**—Association of SBOMs with systems. With system association, if one system is created through multiple elements, the SBOM content for each element can be brought in. Using an ERP system as an example, 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 the potential risk.
- **Mitigation**—Vulnerabilities can be audited, refuted, and mitigated based on use.
- **Obsolescence**—of libraries is identified with graduated levels 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 powered by TotalARMOR
Intelligent Cyber Security Platform
Local Time: 03:00 PM
UTC Time: 07:00 PM
ICSP Administrator
Application Risk > Synthetic View - Application Modules
Integrated Risk Management
Business Data Management
CITAM
Cyber Culture
Application Risk
User Dashboards
Context Engine
Cyber Intelligence
Administration
Collapse Menu
Publisher
Research
LoB
GlobalCom
App Comp
---Select---
SEARCH
Type LoB AppComp Application Module Version R W. Obsol. Avg. Age C H M L T mV mL SCL WCL Libs LmV LmL
GlobalCom ScenPlan LogCom 2.7.9.alpha Unknown 5 years 10 59 105 72 4 240 0 0 0 8 362 0 0
GlobalCom BoP back-batch 6.1.7 Unknown 7 years 6 48 90 50 4 192 4 0 0 0 355 4 0
GlobalCom BoP back-batch 6.6.8.0000 Unknown 9 years 2 47 93 37 3 180 2 0 0 0 163 2 0
GlobalCom ScenPlan FutureState 3.6 Unknown 8 years 2 44 85 37 2 168 1 0 0 0 194 1 0
GlobalCom ScenPlan TriOrg-Portal-Collab 6.3.1 Unknown 9 years 2 33 57 30 3 123 3 0 0 0 171 2 0
GlobalCom BoP back-batch 7.2.2.2012 Obsolete 9 years 0 14 43 52 2 111 2 0 0 13 320 2 0
GlobalCom BoP ScenPlannerX 9.9.9 Unknown 11 years 0 4 13 7 2 26 0 0 0 0 106 0 0
GlobalCom ScenPlan FutureState 1.7.8.111 Unknown 5 years 0 3 17 12 2 34 0 0 0 0 175 0 0
Pages: 1
Records: 8
Page Size: 30

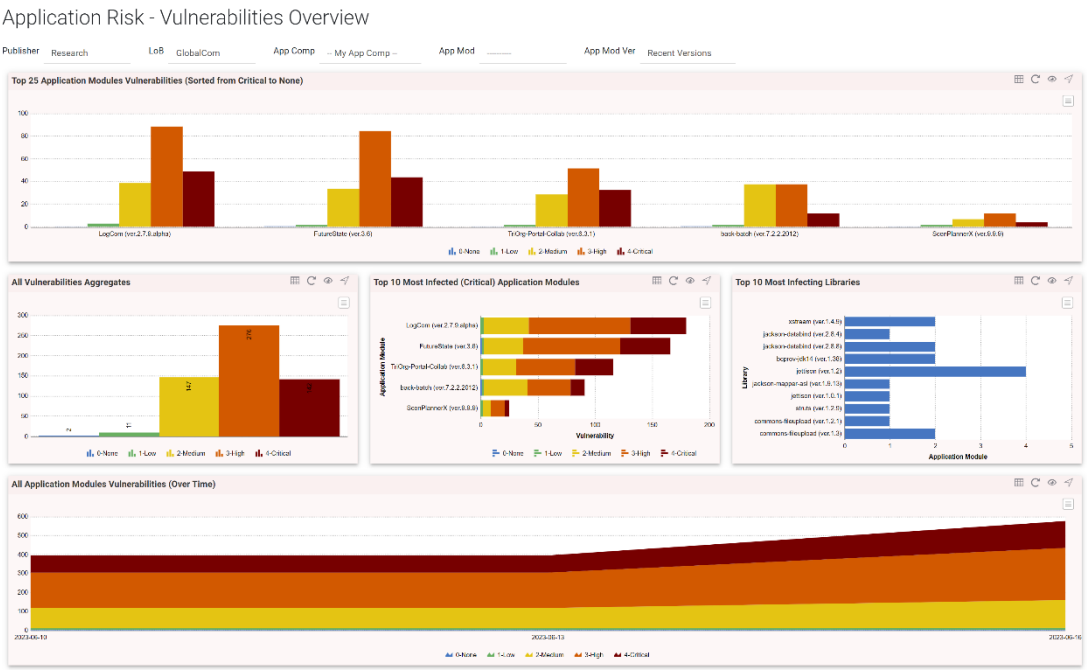

Eracent powered by TotalARMOR
Intelligent Cyber Security Platform
Local Time: 03:02 PM
UTC Time: 07:02 PM
ICSP Administrator
Application Risk > Synthetic View - CVE
Integrated Risk Management
Business Data Management
CITAM
Cyber Culture
Application Risk
User Dashboards
Context Engine
Cyber Intelligence
Administration
Collapse Menu
Publisher
---Select---
SEARCH
SHOW APPLICATION MODULES
SHOW SHARED APPLICATION MODULES
CVE Name Library Name Library Version Age Acc. Vector Acc. Complex. Authentication Availab. Impact Score Mods MmV mV
CVE-2021-44228 log4j-core 2.9.1 6 months Network expl... MEDIUM Not required... Total shutdo... 10 2 0 1
CVE-2021-44228 log4j-core 2.12.1 6 months Network expl... MEDIUM Not required... Total shutdo... 10 1 1 1
CVE-2021-44228 log4j-core 2.13.3 6 months Network expl... MEDIUM Not required... Total shutdo... 10 1 0 1
CVE-2021-44228 log4j-core 2.14.1 6 months Network expl... MEDIUM Not required... Total shutdo... 10 1 0 1
CVE-2022-22965 spring-beans 5.3.7 11 months Network expl... LOW Not required... Reduced perf... 9.8 1 0 3
CVE-2022-22965 spring-beans 5.2.8.RELEASE 11 months Network expl... LOW Not required... Reduced perf... 9.8 1 0 3
CVE-2022-22965 spring-beans 4.3.1.RELEASE 11 months Network expl... LOW Not required... Reduced perf... 9.8 1 0 3
CVE-2022-22965 spring-beans 4.3.29.RELEASE 11 months Network expl... LOW Not required... Reduced perf... 9.8 3 2 3
CVE-2022-22965 spring-webmvc 4.3.17.RELEASE 11 months Network expl... LOW Not required... Reduced perf... 9.8 1 1 3
Pages: 61
Records: 549
Page Size: 9
1 2 3 4 5 6 7 8 9 10

Intelligence—Unlocking the Value of the ZTRP System

The Zero Trust Resource Planning system comes with a complete, built-in Cyber Intelligence engine. The management and configuration of data queries, filters, drill-down queries, time series metric collection, transform / load queries, export queries, and dashboard content are all controlled from within the ZTRP interface.

Cyber Intelligence Elements

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

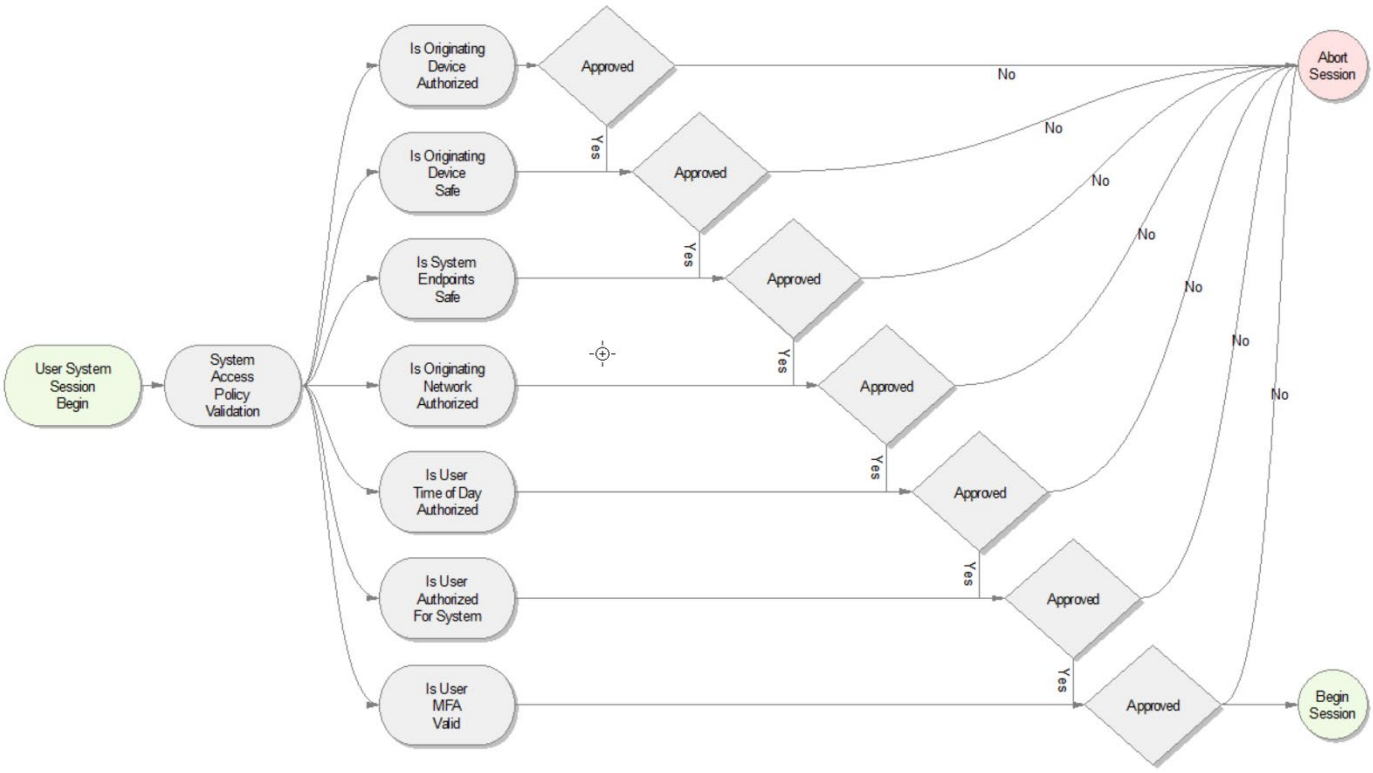


ZTRP Use Case—Dynamic Authorization to Access

The implementation of Zero Trust Architecture requires an orchestration of multiple key areas related to Cybersecurity. One critical area is the authentication of who is accessing systems, and from where. This use case asks the question, what if a valid person with valid credentials - but other critical defects - attempts to log into a high-risk system?

If their access point has critical vulnerabilities, are they allowed to have access to the system? What if the vulnerabilities are on the CISA / CVE list? If an endpoint associated with a high-risk system has critical vulnerabilities, is it allowed to operate? By exposing this information, the data can be correlated with policies. If elements are non-compliant, exposing that level of detail to the access system allows for more control and provides the ability to assess items that are critical to Zero Trust.

Zero Trust considers multiple sources of information:

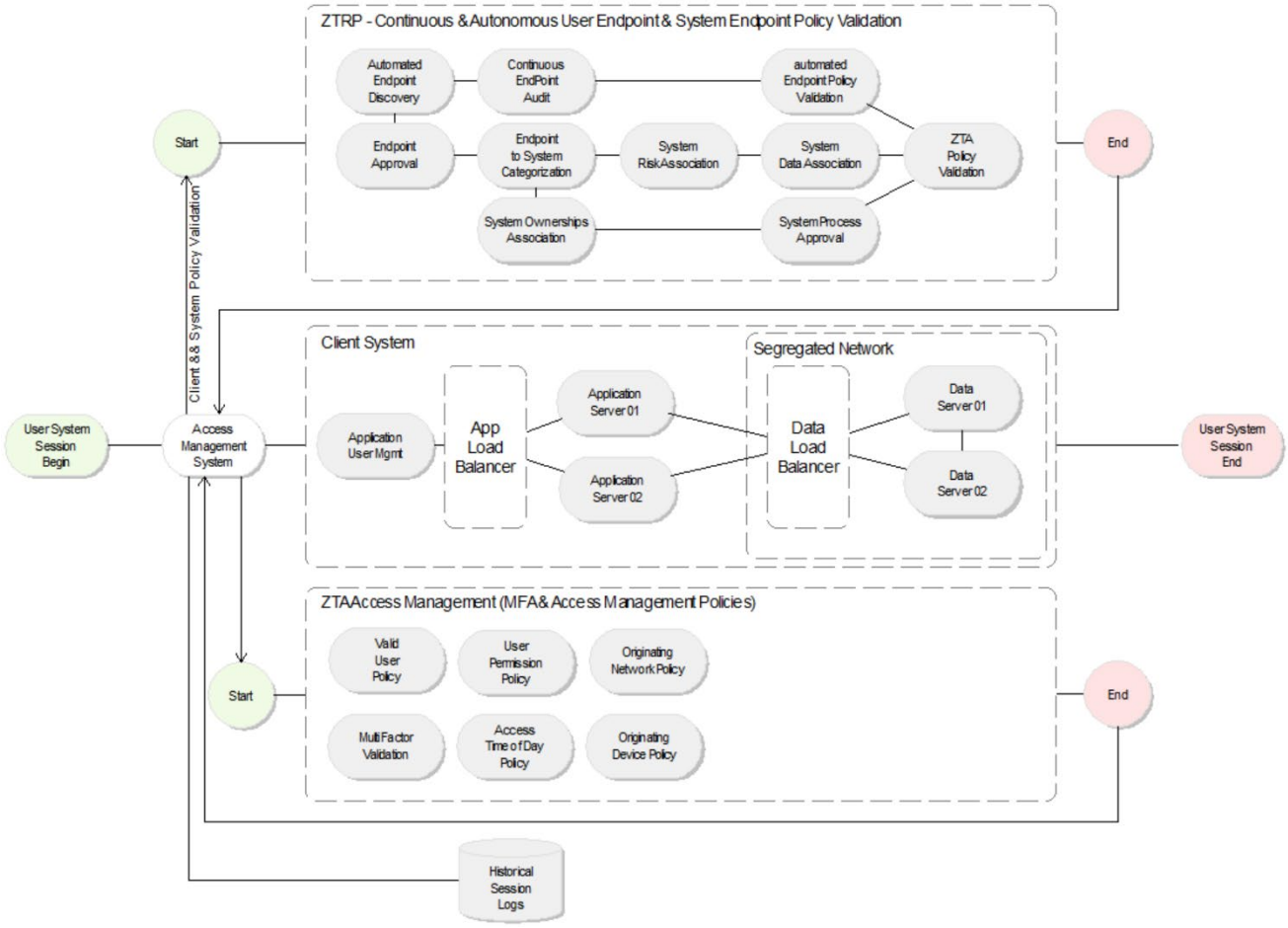


ZTRP Use Case—ZTRP Place in System Access

Zero Trust Resource planning allows for various cyber-related policies to be controlled through a centralized system. Critical to Zero Trust is understanding which policies may be in place and deciding if those are used to control user sessions that are accessing systems. In this variation on our access use case, we can see that autonomous audit of the endpoints allows discovery to run if an endpoint moves the user workstation or system endpoints out of compliance.

Additionally, since other artifacts are identified in a Multi-Factor Authentication (MFA) system, a Cyber ITAM system, and various other sources, the potential for a more controlled Zero Trust is possible. The key takeaway is that if high quality, accurate information exists, it can be utilized.

Zero Trust considers multiple sources of information:



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.

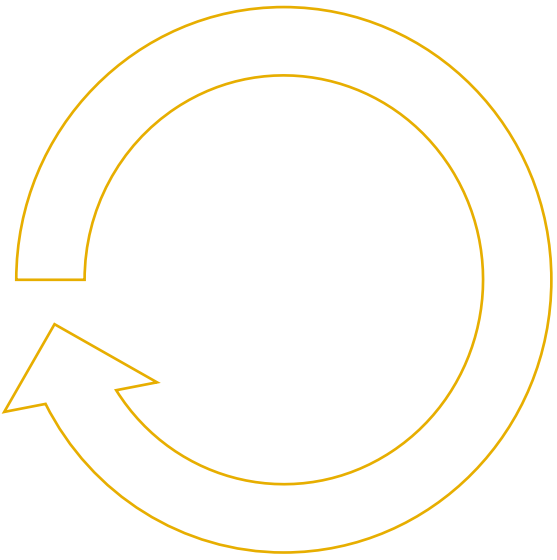
Buying and implementing tactical "Zero Trust" security detection and mitigation tools without a strong data foundation and a thorough management plan to tie it all together will not result in adequate protection.

Eracent Armored Zero Trust Resource Planning provides you with the tools and process to achieve and sustain successful Zero Trust.

Never Trust, Always Verify

"Never Trust, Always Verify" becomes just another Cybersecurity platitude without embracing key requirements. A successful program assigns ownership, details the objectives, discovers Core Data, correlates context data, works toward objectives, and audits the results. The Zero Trust Resource Planning system provides this structure through the Zero Trust Framework.

Fortify your organization's security with the ICSP Zero Trust Resource Planning (ZTRP) system. To learn more about the process and see a demo of ZTRP in action, contact Eracent today.



Eracent, Inc.
519 Easton Road, P.O. Box 647
Riegelsville, PA 18077 USA

info@eracent.com
+1- 908-537-6520
www.eracent.com