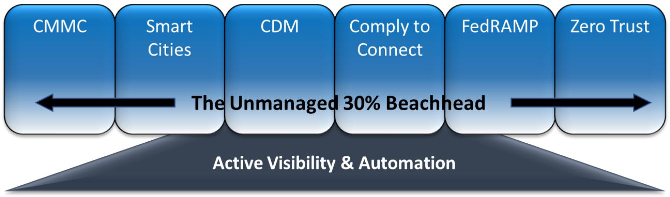
WHITE PAPER

Zero Trust and Beyond

The Catalyst For Solving Compliance Programs and Initiatives

In recent years programs like Smart Cities, Continuous Diagnostics and Monitoring (CDM), Comply to Connect (C2C), Cybersecurity Maturity Model Certification (CMMC), Federal Risk and Authorization Management Program (FedRAMP), and Zero Trust Architecture (ZTA) have worked to secure interactions between people, systems, and applications. These programs and initiatives recommend a strong foundation for hardening an organization's overall IT services and operations. The success of deploying and managing these solutions across an organization requires a fundamental change in how asset intelligence is obtained. Organizations attempting to implement these programs or frameworks are faced with three common problems:

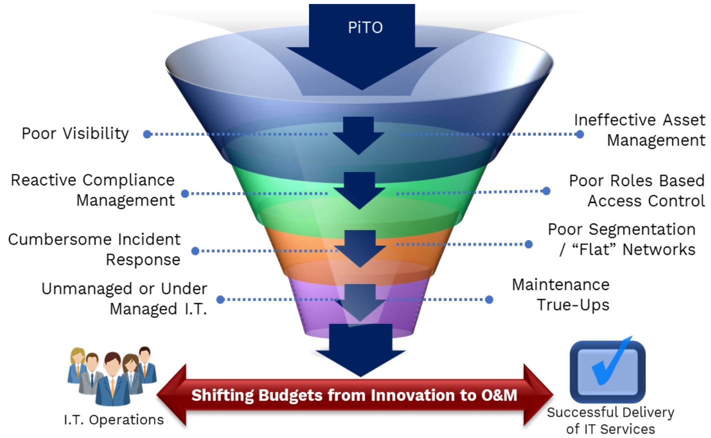
- **Inaccurate Data** Most organizations have, on average, 30% of connected assets that are unmanaged or undermanaged, thus reducing the effectiveness and confidence in solution effectiveness
- **Too Much Data** Even if only 70% of assets are visible and generating data, the amount of information in the existing managed systems is extremely cumbersome and difficult to understand without tools.
- **Cumbersome Data** The processes needed to analyze the data to derive meaning are arduous and expensive and have a high risk of failure due to the lack of ability to connect the data to support an effective understanding of what is happening in an IT environment.



The unmanaged population of IP addresses should be considered the beachhead for our adversaries; that beachhead is the launching point for gaining control over an organization's networks. In situations where there is poor asset visibility, attempting to proactively introduce new solutions to improve incident responses is like shooting at a target in a dark room, blindfolded. It is not possible to effectively manage invisible assets; organizations mistakenly replace one tool with another only to wind up with little or no actual improvement in the security or quality of service because the new tool cannot manage what it cannot see. While incomplete, the mountains of available data that are generated are still too large and cumbersome to process manually. This leads to needles of the truth getting lost in haystacks of incomplete data. Organizations need a simple and consistent model to work with to achieve a solution that allows every transaction to be trusted.

The days of non-compliance in IT operations are quickly coming to an end because today's threatscape is outpacing many organizations' ability to defend. Often, they are unsure how to best proceed because the number of avenues of attack and overall attack surface grows annually. The increased pressure for secure operations coupled with new emerging threats rapidly pushes many organizations to blindly add new solutions or rip and replace existing ones with the hope they successfully address major gaps in the organization's security posture. In too many cases, those efforts result in little or no improvement.

Compliance is challenging as it is often subordinate to business needs which require organizations to keep pace with major technological trends. This is so they can adapt and innovate to maintain competitiveness. Those trends include working from anywhere, bringing your own device, cloud computing, decentralized app development, and integration with secondary tools and service providers. In the digital economy, transactions occur around the clock, every day of the year. The continuous nature of the transaction environment results in a massive volume of transactions happening at the speed of light. In this global sea of transactions, adversaries patiently wait for that insecure transaction to provide access to your network. Understanding this condition, the best possible way to achieve secure, compliant, IT service operation and consumption is to develop an active approach to monitoring every transaction. A key challenge faced by any organization will be trying to react to or prevent cyber-attacks while leveraging traditional point-in-time snapshots of information.


PiTO
Poor Visibility
Ineffective Asset Management
Reactive Compliance Management
Poor Roles Based Access Control
Cumbersome Incident Response
Poor Segmentation / "Flat" Networks
Unmanaged or Under Managed I.T.
Maintenance True-Ups
I.T. Operations
Shifting Budgets from Innovation to O&M
Successful Delivery of IT Services

Point-in-Time Operations (or PiTO) is one of the most pervasive challenges all organizations face today when delivering IT services. This is because if point-in-time snapshots are leveraged for situational awareness, the information gaps reduce or eliminate the effectiveness of a solution. All too often operations teams relying on that data are hamstrung by point-in-time operations, responses, and executions against problems and incidents.

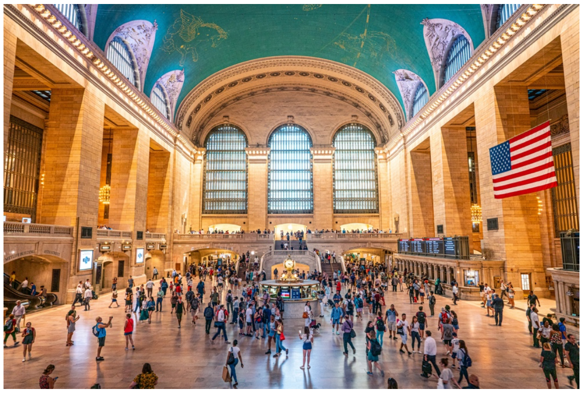
PiTO is a primary driver for technical debt in an organization which can be defined as any cumulative gaps in personnel, process, or technologies working to deliver a service. Examples of technical debt include stop-gap solutions that leave unresolved requirements for the organization to accept, maintenance windows that are not completed on the first attempt, and unmanaged or rogue assets, to name a few. PiTO has a cumulative effect on organizations and has the effect of siphoning budgets from innovation to operations and management so that the lights can be kept on. That effect can be treated as technical debt, which is a shortcoming in a solution or service that is accepted by an organization. Building on the example previously mentioned, let's assume a stop-gap solution that solves 7 of 10 problems until a new solution can be procured. The residual three problems that were not satisfied are examples of technical debt. As these instances accumulate inefficiencies in the organization over time, ultimately having a stopping effect on innovation and efficient IT operations. Like a shovel pushing too much snow, PiTO will slow innovation and in severe cases IT operations in general, grind to a halt.

Let's look at a real-world example where the consumers and staff do generally trust every transaction.

Located in New York City, Grand Central Terminal (GCT) serves over 750,000 people on average and up to one million people per day during the holidays. Each person potentially engages in dozens of transactions while moving into, through, and out of GCT. Transactions include purchasing coffee, eating breakfast, buying a newspaper, and of course, getting on and off trains. Each one of these transactions is completely trusted by the patrons, who are generally unaware of the level of monitoring and security involved to protect them.

Some examples of security systems include:

- 24x7 Video surveillance
- Sensor technology to detect chemical and biological threats
- Radiological Emergency Management System (REMS)
- Metal detectors and bag inspection checkpoints
- Regular patrols covering coordinated areas
- Fully Staffed Police, Fire, Rescue, and Maintenance services



GCT is a very successful amalgamation of people, processes, and technology, working together as a cohesive security and support system, and actively and proactively providing support. Let us now consider a situation where GCT decided to replace its video surveillance cameras with snapshot cameras. Instead of having real-time situational awareness provided by a video camera, snap-shot photographs would be scheduled in five-minute increments. How well would those other systems and teams of staff function? For example, if a radiation detector went off in between snapshots, where exactly would the appropriate responders go? How well would other problems be addressed, even something as innocuous as dispatching maintenance to address a spill? How much risk would be incurred by simply leaving floors wet for an extended period while maintenance is waiting to be notified by the snap-shot surveillance system? How effectively could police respond to crimes and how useful would the new snap-shot camera system be for investigations and problem-solving? It makes sense that GCT wants real-time surveillance of its systems and facilities because real-time monitoring allows appropriate teams to respond promptly, thus minimizing the damage or unintended side effects of events. Understanding the importance of real-time intelligence ask yourselves:

How safe would the transactions be in GCT if we replaced video cameras with snap-shot cameras?

The IT services running in a data center, or cloud computing are not at all, unlike GCT. The patrons could be considered similar to data packets coming in and out of GCT, just as real data packets do in data centers or computing clouds. Instead of biometric surveillance, radiation detectors, police, fire, and rescue staff, data centers, and clouds leverage patch management, vulnerability scanners, configuration management systems, incident response solutions, dashboards, and antivirus software. Unfortunately, for most data centers and computing clouds, the reality is they are using snapshots to develop their situational awareness. As with the GCT example, using a point-in-time method for data discovery and analysis will likely increase the risks of untrusted transactions causing harm, intentionally or otherwise.

None of the popular programs (FedRamp, C2C, CDM, ZTA, etc.) will be very effective without an active approach to discovery and situational awareness of assets connecting, connected, and disconnecting from an organization's network. Invisible assets cannot be secured, managed, or accounted for. Trusting transactions involving unaccounted or unmanaged assets is a gamble; that is why unmanaged or unaccounted-for assets remain the largest risk to the implementation of any successful IT management and security program.

Organizations need an active approach to solving three key challenges that can stop a program like CDM, C2C, or ZTA dead in its tracks. Those three challenges are asset visibility and automation, event stream processing and management, and asset relationships management relationship management.

We recommend the following, cumulative, approaches to secure a network:

- A more Proactive Approach to Asset Visibility and Automation
- A more Proactive Approach to Event Management
- A more Proactive Approach to Relationship Management

The remainder of this paper discusses these foundational approaches in greater detail of how taking an active approach helps eliminate the PiTO condition.

Taking a Proactive Approach to Asset Visibility and Automation

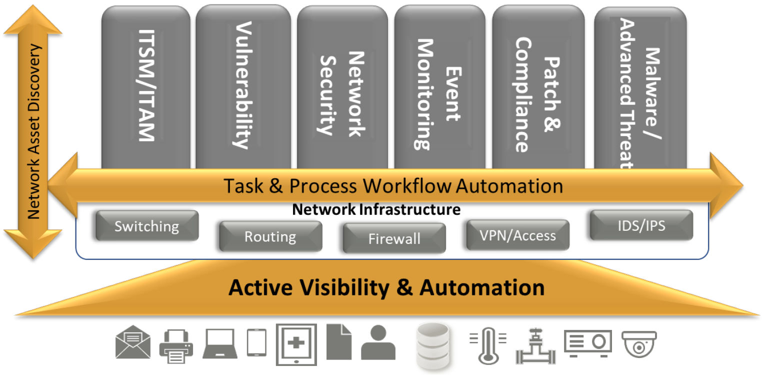
Organizations generate mountains of data spread across thousands of endpoints, apps, and users, all connected in a complex web of interactions, leveraging some combination of on-premises, hybrid, cloud, or multi-cloud architecture. There are billions of potential interactions between these assets, dramatically increasing the organization's attack surface and making it more vulnerable to cyberattacks from criminals with different capabilities and intentions. Taking an active approach to visibility is ensuring all assets are continuously discovered, assessed, and categorized into their respective roles and expected behaviors. Furthermore, active visibility is the genesis of automation, as the active visibility solution is the trusted source of discovery data about connected assets because it categorizes endpoints and determines whether those endpoints operate in an approved manner.

The next step towards active visibility is the ability to share a trusted source for asset intelligence with other third-party solutions leveraging point-in-time discovery, in the environment. Ensuring every asset is accounted for and working from a shared source of situational awareness is the first step toward achieving Active Operations. Otherwise, organizations are faced with a cumbersome, inaccurate, and incomplete data set to be used for information analysis.

As with the GCT example, the constant data feed video cameras provide is vital for services to run efficiently and effectively. Consider another example where a video camera would be far more valuable than a snapshot camera. Imagine two race drivers tasked with racing through a timed obstacle course using only cameras to navigate instead of looking through their windshields. One driver uses an old, black-and-white camera with poor resolution. The other driver uses a state-of-the-art camera that tracks temperature, humidity, and time of day, and supports full HD color photos; however, the newer camera can only take a picture once every 15 seconds. Who do you think is going to win the race?

It is common for organizations to spend millions of dollars procuring and deploying complex technologies, and hiring and training new staff, only to end up failing to meet expectations. One of the primary reasons why systems fail to meet expectations is that they suffer from compounding delays because they are built on “snapshot” camera pipelines. Data is collected periodically instead of in real-time, then passed in batches to secondary systems that process or augment that data to be used in decision-making processes or automation controls. The delays in processing are long enough for malicious actors to enter and gain a foothold in networks. In many cases, without properly addressing asset intelligence and task automation, programs like ZTA and its batch of associated tools can also fall prey to the common rip-and-replace fallacy that new technologies fix old problems. This can create a cycle where every three to five years, programs like CDM, C2C, and ZTA fail, causing organizations to continue the technical refresh cycle in hopes that the next suite of tools will work.

We can break that cycle by requiring an active approach to visibility and automation. Active management closes out any blind spots those tools may have while simultaneously providing real-time data that supports rapid resolutions to threats. Full visibility and rapid response immediately improve the effectiveness of tools and realizes the full potential of programs.



Visibility companies, including Armis and Forescout, report that on average, nearly 1 in 3 assets on customer networks are unmanaged or under-managed. Those unmanaged assets serve as beachheads for adversaries to land and expand control over our networks. Unmanaged assets also experience diminished performance because they are not regularly patched and many patches address performance issues.

Complete visibility and asset situational awareness enable two things – improved performance of existing IT systems and automation. Accurate asset information can be shared with existing IT services, including but not limited to: IT Service & Asset Management (ITSM/ITAM), vulnerability, network security, event monitoring, patch and configuration management, asset detection and monitoring, and advanced persistent threat. These systems will perform better and generate more accurate information when the underlying data is accurate. Full asset visibility also enables the automation of simple and repeatable tasks. Automated tasks should be documented and implemented into the existing Zero Trust Architecture. Doing so before that milestone is accomplished can be very dangerous, and akin to trying to hit a target in a completely dark room while wearing a blindfold – you don’t know what systems or applications will be affected when automation is implemented on networks with partial visibility. Automating even simple low-risk tasks without understanding what is connected to a network is one of the most common mistakes customers make when rolling out any automation solution or technology.

Alchemy Global Networks Recommends the Following Vendors for Visibility and Automation

Vendor	Website
Armis	armis.com
Forescout	forescout.com
Cisco Identity Services Engine (ISE)	cisco.com/site/us/en/products/security/identity-services-engine/index.html

Taking a Proactive Approach to Event Management

The next step, after organizations achieve full visibility, is to actively monitor the behavior of those assets by feeding logs to an event manager. Event managers can be considered the "brains" of IT operations because, like a brain, they gather, aggregate, and correlate data to derive the meaning of a given situation or condition. Although event managers are essential for managing IT environments, they are poor tools for asset discovery. Using event managers as asset discovery tools has plagued event managers since their inception; organizations struggle to correlate other asset data through third-party integrations, procurement records, and the memories of staff as to what is connecting/connected/disconnecting from the network. By integrating event managers with a trusted source of information about the assets generating the events, organizations can almost immediately reduce the complexity of their solutions while greatly improving the accuracy of information feeding the event manager on asset intelligence.

Integrating an event manager with a trusted visibility and automation tool is the first step toward delivering an active approach to event management. An active event manager has full purview of the connected assets, due to its integration with the visibility and automation solution. Due to the nature of the event manager and how many other solutions it typically integrates with, its dataset must be accurate. Imagine trying to ascertain a situation or condition with only 70% of the data, and then sharing that context with others.

Consider the graphic on the right where 30 of 100 words are missing. Using the GCT analogy, having accurate and up-to-date intelligence on the passenger transactions in the station is through superior visibility. Active event management is the real-time monitoring and management of the patrons entering and leaving the station; it is not possible to manage their transactions safely and accurately if 30% of them are unaccounted for. However, this is the situation most IT staff face - 30% of assets are unmanaged.

The Importance of Full Asset Intelligence

It is spring of three during
Standing among hundreds of new soldiers at
Camp Grant, in Illinois, just 18 years old,
waits as a by. A full field pack is randomly
tossed to each soldier. thinks, as
he Litrenti, marked on each item in his
pack. "How did me when they tossed the
pack?" He was impressed! my father was
tossed a field pack from World father's.

The same is true for our event managers and the staff that leverage them. Incomplete data provides little value in understanding the full situation. Therefore, IT staff are forced to manually backfill data to make informed decisions; this manual labor increases costs for IT services while simultaneously providing worse service because manual operations cannot grow fast enough to keep pace with the rapidly increasing number of assets on a network.

Take another look at the same story, but with full visibility, note the differences, and that no effort is needed to comprehend the situation beyond what is written in front of us.

The Importance of Full Asset Intelligence

It is spring of nineteen hundred and forty three during World War II. Standing among hundreds of new soldiers at Camp Grant, in Illinois, my father, Sam, just 18 years old, waits as a truck slowly drives by. A full field pack is randomly tossed to each soldier. “How strange,” my father thinks, as he sees his last name, Litrenti, marked on each item in his pack. “How did they know it was me when they tossed the pack?” He was impressed! Beating all odds, my father was tossed a field pack from World War I—his own father’s.

The next step towards realizing the full potential of your event management is to expand its automation capabilities beyond traditional tasks that are commonplace today such as “open a ticket, pull a report”. Put simply, opening a ticket in service management software is simply an event broker triggering an event in a secondary system. Using that same mechanism, organizations can have the event broker feed trigger events to other third-party systems to automate simple, repeatable tasks such as quarantining a device that has gone rogue, performing an out-of-cycle scan for laptops that have been offline for extended periods, or installing a missing patch. Unfortunately, many of these tasks are now done manually or not at all when the device is part of the 30% of assets that are unmanaged.

Third-party solution true-up is one of the single biggest impacts an active approach to visibility and automation can have on a customer’s security posture as it ensures all assets are accounted for and properly managed. Customers can also leverage an active visibility and automation approach to drive down operational costs through capacity expansion. This is accomplished through automation workflow development; Alchemy will work with your engineers to identify candidate tasks that can be automated. From there, our engineers will implement those capabilities into the AAVA solution. This allows repeatable tasks to be completed faster and with fewer instances of human error, while also being candidates to have those tasks transferred from potentially a Tier 3 group to a Tier 2 or a Tier 1 group, further extending potential labor savings.

Alchemy Global Networks Recommends the Following Vendors for Event Management

Vendor	Website
Splunk	splunk.com
LogRhythm	logrhythm.com
DataSet (formerly Scalyr)	dataset.com/platform/

Taking a Proactive Approach to Relationship Management

In cyber warfare, delays and errors are costly; cyberattacks happen in hours or days, yet most investigations, incident reports, and responses take months. The average direct cost of a cyber-attack is around $5 million, which strongly correlates with the time needed to respond. After organizations have activated their visibility, automation, and event stream management systems, the next step is improving how your teams interpret the large volume of data generated by those systems. The goal is to understand how well your cybersecurity services are performing as it relates to protecting your IT assets, their users, and consumers. The solutions need to provide results in a manner that allows for real-time feedback on changing system conditions, including how users, systems, applications, and data are impacted.

Asset visibility is foundational to any cyber program; however, implementing full asset visibility often creates a secondary problem – data overload. Data overload occurs because asset visibility tools generate lists in the form of spreadsheets, reports, and incident findings. It can take hours, days, or weeks of analysis to fully accumulate, synthesize, review, and understand data from multiple sources. Additionally, IT assets do not function in a vacuum; instead, they interact through a matrix of connections. Their interactions represent the asset-to-asset relationships that must be managed to fully understand the condition or compliance of transactions. Unfortunately, asset inventory tools do not do an adequate job of tracking and managing those relationships. There needs to be a solution that helps people automate the data collection and analysis so that effective decisions can be made faster.

Consider a similar situation where law enforcement teams constantly sort through mountains of data, trying to solve a mystery. These teams often leverage a best practice tool and a series of processes allowing a team of people to create and communicate a comprehensive picture of events through a crime board. This tool allows the rest of the team to quickly process data and track the larger picture much more effectively than a set of disparate lists.

Detective teams assemble data from witnesses, forensic evidence, news reports, and digital recordings. All that data needs to be organized into a visualization so the team can see the context of a given situation. Crime boards are essential tools because they reduce the time required to solve a crime and apprehend the criminal. The same thing holds true for cybersecurity: the connections or relationships between people, systems, and applications matter. Cybersecurity teams need a similar tool to reduce incident response times because cyber attackers exploit the time it takes to collect and organize data to form a response. Organizations need to be able to track, in real time, how their assets interact to quickly identify gaps in their security.

An approach to active relationship management is built on active visibility and event management; visibility and event management tools generate a substantial amount of valuable data. However, that data is not organized. The lack of organization makes it difficult for staff to respond quickly to incidents because they spend energy bringing the data together to evaluate the context of alerts. Active relationship management leverages technology to assemble data. This approach to active relationship management is the modern version of the crime board – it addresses the problem of information overload by connecting disparate lists of assets into a connected view of your environment for maximum situational awareness. Active relationship management is built on the automated generation of information and leverages technology to draw and visualize the relationships in your data. The purpose is to free up your staff's time and mental energy so they can focus on interpreting the information and making decisions that impact your organization's security posture.

Alchemy Global Networks Recommends the Following Vendors for Active Event Management

Vendor	Website
Grafana	grafana.com
Neo4J	neo4j.com
vArmour	varmour.com

Organizations leveraging active visibility, event, and relationship management are in the best shape to proceed forward to take on new programs such as C2C, ZTA, CMMC, FedRAMP, and others. Not taking an active approach to these functions can result in similar outcomes, because ripping and replacing tools has not worked in the past, and there is little reason to believe it will improve without first actively understanding what is connected to your networks, what those connections are doing in near real-time, and how quickly can we adjust the solution given feedback data results.

Alchemy Global Networks

Alchemy Global Networks LLC provides cybersecurity and network solutions to clients to meet the challenges of the ever-changing cyber threatscape. Alchemy Global Networks has a team of consultants and engineers with decades of professional experience designing and delivering asset intelligent solutions for service consolidation efforts. Alchemy Global Networks consistently finds the best solutions for organizations, who appreciate our experience, passion, and commitment to understand their real-time needs and goals. As a trusted provider with Federal, Civilian, Defense, Intelligence Agencies, and Commercial clients, Alchemy Global Networks supports over 5.1 million endpoints. For more information on Alchemy Global Networks' Managed Engineering Services, visit www.agn.tech.