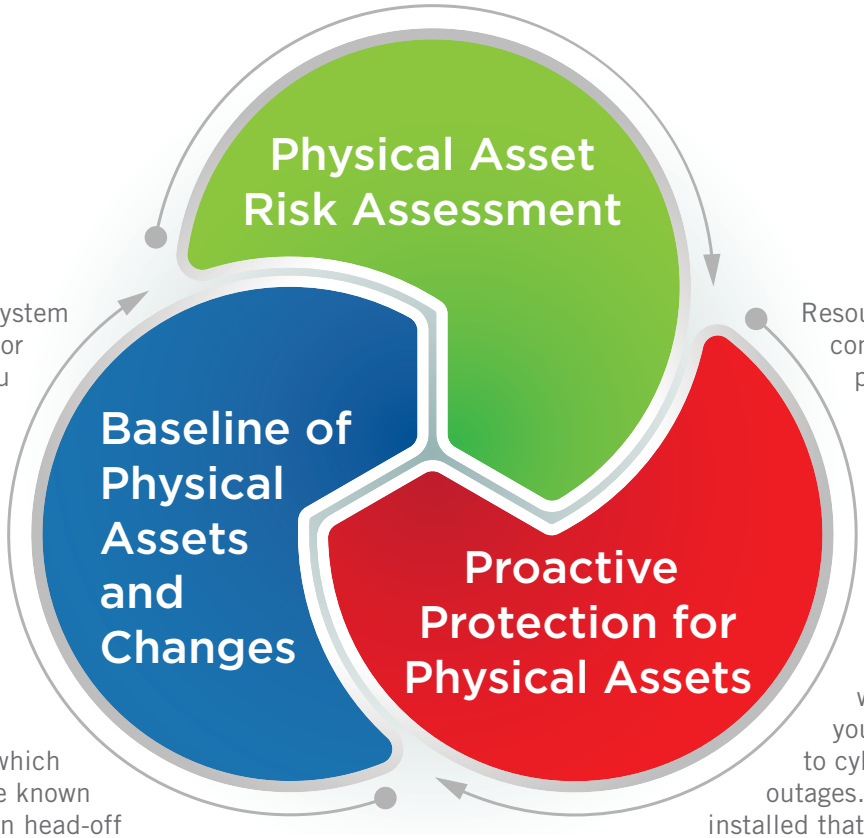
NIyte Software

Asset Integrity Monitoring

Ensuring the Physical Integrity of Your Compute infrastructure

SOLUTION BRIEF

Ensuring the Physical Integrity of Your Compute infrastructure



Offering a streamlined system that creates a baseline for all the critical assets you want to manage, NLYTE ASSET INTEGRITY MONITORING enables you to harden your physical compute environment by proactively evaluating the resiliency of your asset tracking and management. AIM identifies versions of software and firmware, which are unauthorized or have known vulnerabilities so you can head-off issues before they occur. AIM brings awareness of all devices attached to your networks, monitors for changes and compliancy providing the ability to report and respond to unauthorized assets, software, and changes.

Ultimately all the applications and data your organization manages depend on a stable and secure physical infrastructure. Whether this infrastructure is located in your own data centers, in colocation or Edge facilities, you must be certain these resources are not intentionally or unintentionally compromised.

Resources can become compromised when personnel make unplanned and/or unrecorded changes to assets. They may add or remove assets, such as servers or blades, without approval or without recording the information centrally, which can then leave your organization open to cyber-attack or to critical outages. Devices can be installed that don't meet security or safety standards.

Additionally, new security threats are constantly being identified and require the latest firmware and software patches are applied to hardware to close these vulnerabilities. Yet many organizations do not have a comprehensive list of all hardware and the versions of firmware and software running on assets throughout their network which results in these systems being open to cyber-attack.

Asset Integrity Monitoring

AIM takes a 4-phase approach:

1) **Discovery – Identify all assets connected to the network**
2) **Change Management Process – Establish a baseline of all assets, power systems, and processes (ITIL, ITSM, DCIM)**
3) **Monitoring – Compare current asset state against baseline inventory and change management compliance**
4) **Alerting and Reporting – Notify security teams of vulnerabilities and noncompliant assets, validate resource availability SLAs**

Discovery Phase – You can't protect what you don't know exists

The first phase of Asset Integrity Monitoring is starting with a baseline of assets. This starts with your DCIM inventory database augmented by a thorough discovery scan across your network. This compiled asset list becomes the single source of truth including, power, compute, software and firmware, network connections, edge and IoT devices.

Change Management Phase – Prior Process Planning

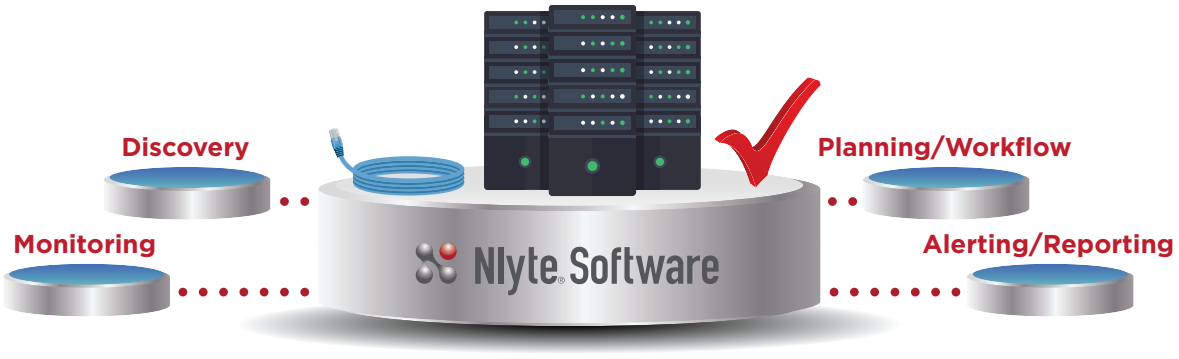
Phase 2 establishes change management practices and protocols. These may be in line with NIST best practices, an ITIL framework, and integration with ITSM CMDB and systems. To reduce human error and risk from repetitive tasks, adopt a DCIM solution that automates standardized infrastructure change management workflows. Lastly define reporting and enforcement procedures across IT Operations, Security, Finance, and HR systems.

Alerting and Reporting Phase – Share the knowledge

Correlating changes to the physical compute environment and reporting them to concerned groups provides many benefits. IT Operations can see who is a repeat offender in making unauthorized and undocumented changes. This can avoid unexpected changes to power, introduction of potentially harmful equipment and software, leading to disruption or catastrophic events. Security teams can monitor for vulnerabilities introduced by unauthorized devices, applications, and network connections. Finance can accurately audit and validate inventory ensuring support, maintenance, and license expenses are accurately accounted for.

Control the Integrity of Your Physical Assets Before Someone Else Does with Nlyte Asset Integrity Monitoring (AIM)

Nlyte's comprehensive Asset Integrity Monitoring solution includes custom-built reports and dashboards to ensure your physical infrastructure is closely managed. These integrity reports are shared easily with interested parties including IT Operations, Business Owners / Customers, Security, Finance, and HR. Additional benefits of an Asset Integrity Monitoring solution includes simplified audit compliance, cost management for unregulated assets, and asset efficiency monitoring.



The solution is comprised of Nlyte's Asset Optimizer and Discovery software offerings. Secondary approaches offered by Nlyte to increase resiliency include:

- Contingency Planning based on evaluating and monitoring power needs and risks with Nlyte Energy Optimizer
- Physical issue prevention with Nlyte Machine Learning
- CPU utilization history along with ghost and zombie servers at risk for exploitation, with Nlyte System Utilization Monitor

FOR MORE INFORMATION

- Contact Us: **info@nlyte.com**
- Visit Us: **www.nlyte.com**

About Nlyte

Founded in 2004, Nlyte Software is recognized as the industry leading data center infrastructure management (**DCIM**) solution provider. Nlyte's DCIM provides unmatched functionality that supports all data center processes across the entire "dock to decom" lifecycle. With a 98% customer retention rate, Nlyte's DCIM solution is used by many of the world's largest and most sophisticated data centers, as well as many small and medium sized organizations. Customers can quickly deploy the Nlyte DCIM solution and begin to immediately enjoy reduced costs and increased efficiency across all data center processes. For more information, visit **www.nlyte.com** or follow **@nlyte** on Twitter.