THE ESSENTIAL GUIDE TO

IOT ANALYTICS AND SECURITY

Operational Assurance for the IoT Lifecycle

nyansa

THE UNSTOPPABLE ADVANCE OF IOT

Marketing leading enterprises are no longer taking a 'wait-and-see' approach to adopting Internet of Things (IoT) technology. Worldwide IoT spending is expected to be $745 billion in 2019, a 15.4 percent increase over 2018, and exceed $1 trillion in 2022 according to the latest research from analyst firm IDC1. The driving factor is the ability to impact business outcomes across diverse industries such as healthcare, manufacturing, retail, and logistics.

Mainstream IoT adoption is not just accelerating, it's becoming mission critical. According to the 2019 Vodafone IoT Barometer2, 34 percent of businesses worldwide are using IoT in daily operations, up from 29 percent a year ago. These companies are using IoT as a competitive advantage with 76 percent classifying IoT as mission critical, and one in 12 saying their "entire business now depends on IoT". And the investment is paying off with 95 percent of adopters reporting measurable benefits.

As the promise of IoT is being realized with tangible business results, complementary technologies are maturing that will accelerate adoption. Advances in big data analytics, Artificial Intelligence (AI) and Machine Learning (ML), sensors, edge computing, and security are all fueling IoT growth. As 5G networks roll out, businesses will be quick to take advantage of the improved connectivity, lower latency, and greater range to further fuel IoT adoption. In many industries, IoT is the cornerstone to the overall digital transformation strategy.

INDUSTRY CASE STUDY

- Healthcare

BUSINESS SCENARIO

- Managing multiple hospitals network with clinical 'workstations on wheels (WOW) for mobile patient care and administration.

PROBLEM: WOWS FAILING AND LOSING NETWORK CONNECTIVITY

- Required staff to reboot the systems
- Major impact on clinician productivity, patient experience
- Delays in the Emergency Department
- Poor reliability for hundreds of expensive assets
- Existing tools and available data unable to identify the root cause and resolve

SOLUTION: DEPLOY AN AIOPS PLATFORM

- Correlate data across the infrastructure and sites
- Analyze historical and real time data
- Data analytics from the network to the device level

RESULTS

- Proved the network was not the problem
- Isolated root cause to a faulty hardware component
- Upgraded systems and returned to full availability

UNICORNS AND DINOSAURS

As with any disruptive technology, there will be winners and losers. Leading enterprises will go beyond improving the operational efficiency of existing processes. Adopters in the Vodaphone report emphatically agree, with 60 percent believing IoT will completely disrupt their industry in 5 years. The race is on to create competitive advantage: new services, new revenue streams, better customer engagement, and new business models.

Cloud computing, mobility, sophisticated analytics, and new applications have provided the foundation for new business models. Thanks to these technologies, industries have undergone a digital transformation. The way we get a ride to the airport, consume movies and TV, or find a place to stay on vacation is completely different that only a few years ago.

Digital transformation is putting pressure directly on CEOs and CIOs. IDC warns that companies who fall behind will see two-thirds of their traditional addressable market disappear3. While new industries are being created, and 'unicorn' companies with billion-dollar valuation are emerging, laggards will find themselves in the position of dinosaurs and video rental shops.

THE PROMISE OF IOT

The promise for CEOs and line of business leaders is to further evolve IT into a revenue generating function rather than a cost center. With the right tools, companies can quantify the impact of IoT deployments on business outcomes and properly prioritize network investments. This requires a tailored approach to the IoT lifecycle that addresses security holistically: everything from device inventory, connectivity, anomalous behavior, alerting, and containment. The enterprise needs operational assurance for these mission critical systems. For example, a hospital CEO needs confidence that his systems will detect a biomedical device that is violating a security policy and automatically take action prior to compromising patient health or privacy.

The IT department and CIOs are looking to align themselves with lines of business to drive better customer experience and improve decision making. IoT initiatives provide a direct avenue to achieve these goals through the operational nature of these devices and the data they provide. Unfortunately, IT teams are already drowning in a sea of data and facing an order of magnitude greater problem as millions of new devices are deployed. The winners will have the right strategy to harness new tools, automation and AI/ML to capitalize on this wealth of data for better operations, engineering, incident response, and security.

Security is a critical component of an IoT strategy as the proliferation of devices radically changes the threat environment. The attack surface and threat variety is expanded exponentially, and the devices themselves are often outside the physical and virtual security of a data center.

Consider a healthcare industry example. Hospitals invest millions of dollars in biomedical devices designed to make clinicians more productive and deliver excellent patient care. A network of three hospitals managed hundreds of 'workstations on wheels' (WOW) for mobile patient care and administration.

When these systems fail, it has a direct impact on operational efficiency and patient treatment. Executives see poor reliability and underutilization of expensive assets.

This hospital was dealing with ongoing WOW failures that required staff to reboot the systems by removing the battery to return them to service. The Emergency Department, where speed is especially critical, was experiencing notable disruptions. Existing tools and available data were insufficient in identifying a root cause.

Tackling this modern IoT problem required a modern AIOps platform. Historical and real time data was analyzed and correlated across the network and hospital sites. IT staff were able to drill down to specific devices and isolate the exact time when the problem occurred.

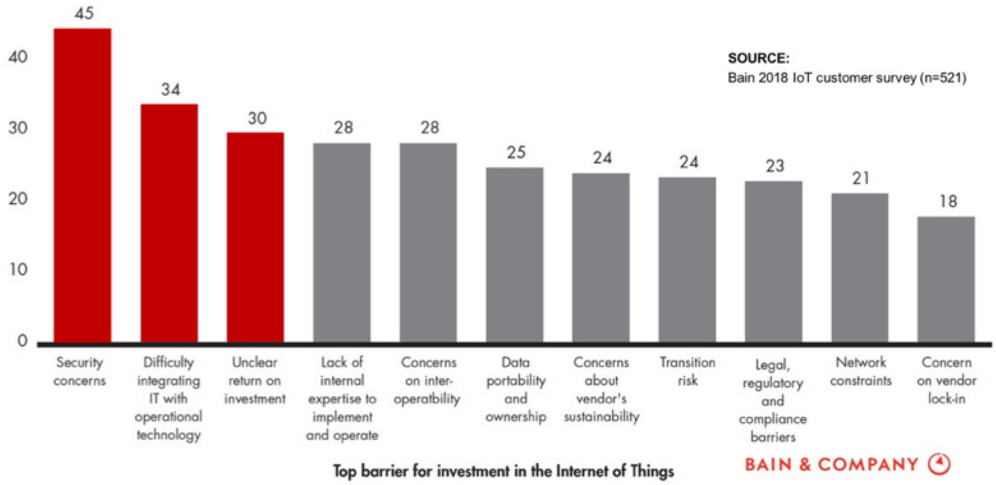
Using this information, network engineers were able to verify the problem was not with the network but with the device itself. Further analytical insight isolated the problem to a faulty Network Interface Card (NIC) and staff were able to work with the vendor on correcting the defect. Once the WOWs were upgraded the problem was solved and the systems were returned to full availability.

OVERCOMING OBSTACLES

As organizations deploy non-traditional networked devices to address business critical initiatives, they face new challenges of how to codify and control the behavior, performance and security of these devices. For instance, connected infusion pumps, EKG machines, and smart temperature sensors in healthcare; smart robots, connected tools and barcode scanners in manufacturing and distribution, and even esoteric connected devices such as smart lights, speakers, digital frames, 3D-printers, etc. in any industry. These modern IoT devices create unique threats that differ from other connected devices, rendering traditional security tools ineffective.

These devices are typically limited- or single-function devices with embedded operating systems and software. Installing a software agent is rarely possible and the device is effectively a 'black box'; security and networking stacks are often weak points. The biggest obstacles to IoT adoption fall under the category of operational assurance. Research from Bain & Company4, shown in the chart below, identified top three barriers as:

1. Security Concerns
2. Difficulty Integrating IT with operational technology (OT)
3. Unclear return on investment (ROI)



SOURCE:
Bain 2018 IoT customer survey (n=521)

Figure 1: Top barrier for investment in the internet of things

The Bain data shows that while there are a range of obstacles, an enterprise IoT strategy must specifically address the need to securely integrate with existing IT infrastructure and processes, plus have a methodology to measure ROI. Leading companies are increasingly turning to artificial intelligence for IT operations (AIOps) as a way to address this and other digital transformation issues. AIOps is an evolving approach that applies sophisticated analytics, artificial intelligence (AI), and machine learning (ML) to improve and automate network operations at scale.

AN AIOPS PLATFORM FOR IOT SUCCESS

As the industry's only vendor-agnostic analytics solution, Voyance goes beyond simple security to give IT, cybersecurity, and line of business owners true insight into IoT operational assurance. This includes asset inventory, connectivity, performance and root cause analysis, vulnerability management, risk assessment, and policy compliance. It also helps organizations extend their cybersecurity programs by aligning its core features to the NIST 800-53 and ISO 27K Cyber Security frameworks.

Voyance addresses all stages of the IoT operational lifecycle. Devices are automatically inventoried and classified. Connectivity is monitored along with performance. Using AI and ML, the platform automatically establishes a performance baseline for normal behavior. Alerts and recommendations are automatically generated for devices deviating from normal behavior both at the individual device level and for devices within a similar group. Network changes are tracked so results can be verified, and the platform ensures IoT devices are properly segmented to mitigate potential issues.

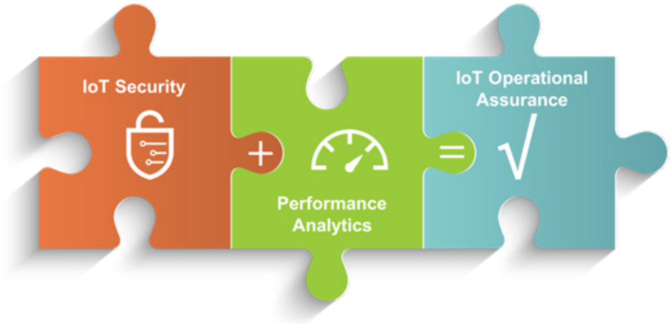


Figure 2: The operational assurance equation

Enterprises now have an AI-based solution that delivers unmatched IoT operational assurance with the integration of IoT security and device performance analytics in a single platform. This equates to big benefits for CEOs, CIOs and CISOs:

- Quantify impact of network technologies on business outcomes
- Prioritize IoT and network infrastructure investments
- Ensure IoT connectivity and usage for the LOB
- Inventory devices; identify risks and vulnerabilities
- Automatically enforce IoT policy within cyber security strategy

The IT department now has a more efficient way to improve and partially automate a range of manual IT operations. For example:

- Performance monitoring
- IoT security
- Event correlation
- Data analysis

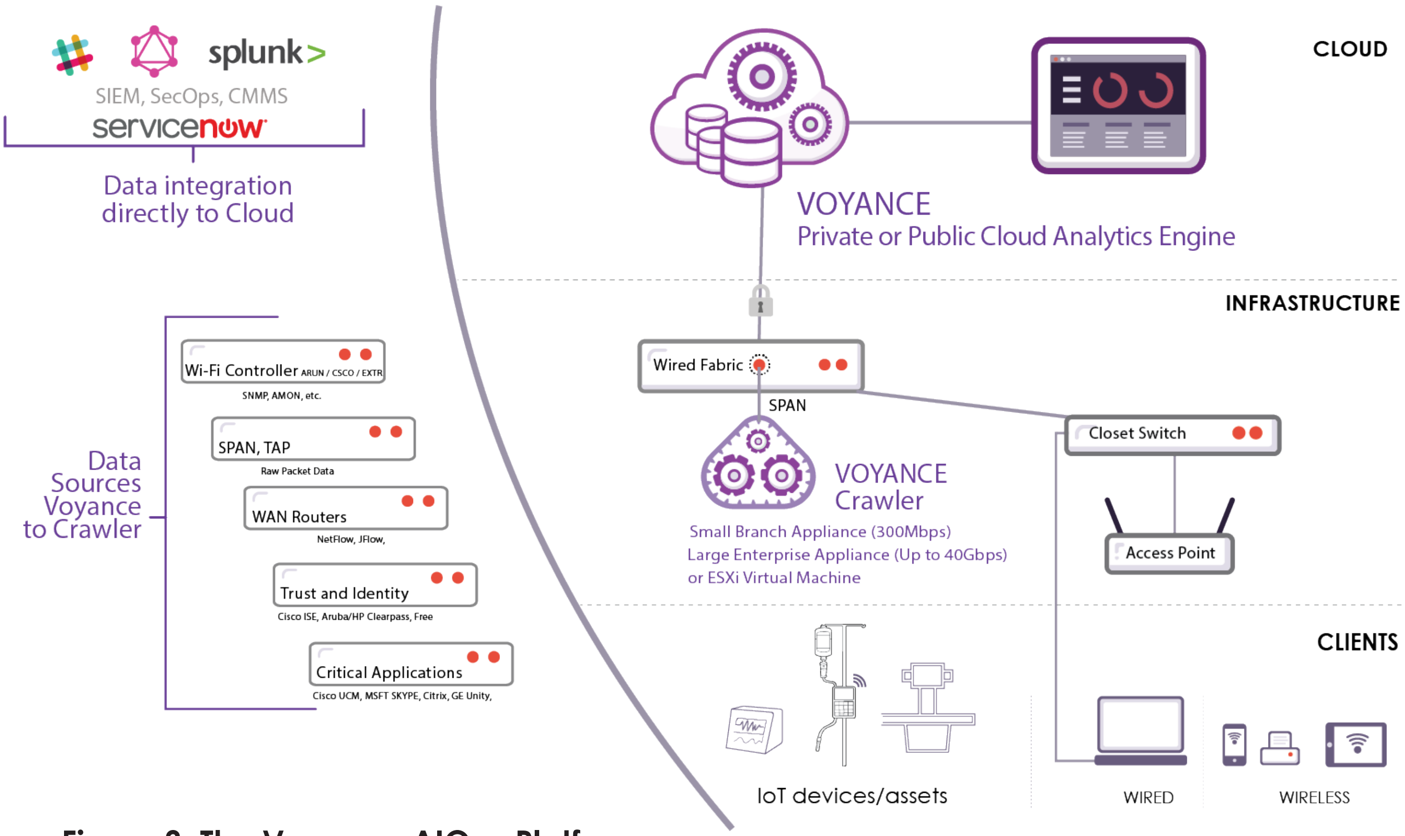

splunk>
SIEM, SecOps, CMMS
servicenow
Data integration directly to Cloud
CLOUD
VOYANCE
Private or Public Cloud Analytics Engine
INFRASTRUCTURE
Data Sources Voyance to Crawler
Wi-Fi Controller ARUN / CSCO / EXTR
SNMP, AMON, etc.
SPAN, TAP
Raw Packet Data
WAN Routers
NetFlow, JFlow,
Trust and Identity
Cisco ISE, Aruba/HP Clearpass, Free
Critical Applications
Cisco UCM, MSFT SKYPE, Citrix, GE Unity,
Wired Fabric
SPAN
VOYANCE Crawler
Small Branch Appliance (300Mbps)
Large Enterprise Appliance (Up to 40Gbps)
or ESXi Virtual Machine
Closet Switch
Access Point
CLIENTS
IoT devices/assets
WIRED
WIRELESS

Figure 3: The Voyance AIOps Platform

BEYOND BASIC SECURITY – IOT OPERATIONAL ASSURANCE

Voyance allows enterprises to automatically inventory and classify IoT devices, employing a machine learning based, hierarchical device classification system that uses the detailed behavioral signature of each detected device. Beyond automatic classification, customers are also afforded the flexibility of tagging critical devices and assets for continuous analysis within the Voyance IoT security lifecycle management framework.

The Voyance platform supports the most extensive list of data sources compared to any comparable AIOps solution on the market. More data means blind spots are eliminated and machine learning models are better optimized. Data sources are correlated from device to application and across the network stack to give real time insight to device and client performance.

Operational Assurance results from covering all stages of the IoT device lifecycle.

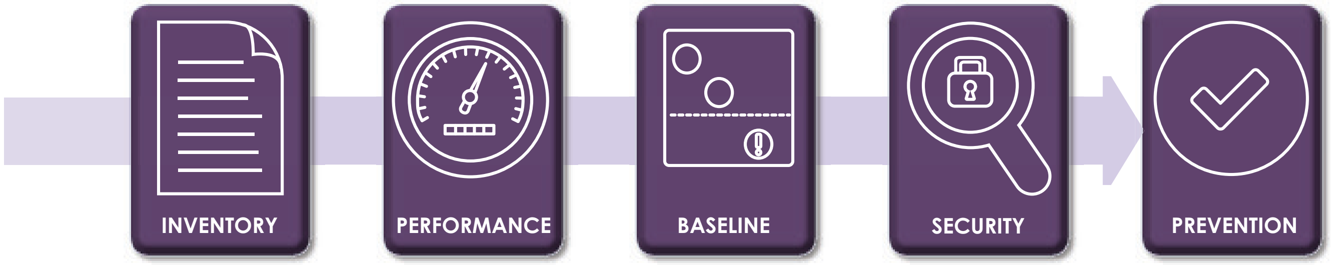


Figure 4: IoT operational lifecycle

AUTOMATICALLY DISCOVER, INVENTORY, AND CLASSIFY CRITICAL IOT DEVICES

Voyance is an agentless security platform for IoT and unmanaged critical devices that collects data passively, via a software crawler sitting out-of-band on customer's network. This vantage point enables the platform to monitor every single client transaction on the network to automatically identify known and unknown IoT and critical connected devices. Device identification is accomplished by employing a machine learning based, hierarchical device classification system that uses the detailed behavioral signature of each detected device. Beyond automatic classification, customers are also afforded the flexibility of tagging critical devices and assets for continuous analysis within the Voyance IoT security lifecycle management framework.

BASELINING IOT DEVICE BEHAVIOR FOR RISK ASSESSMENT AND THREAT DETECTION

By looking at similar IoT devices in a single environment, as well as across multiple customer environments Voyance automatically 'learns' what the normal, baseline behavior of a particular device should be. With over 20 million devices currently under observation, the Voyance system continuously updates the unique pattern for each family of devices across the entire Voyance installed base, minimizing false anomalies.

In addition to automatically detecting deviations in baseline behavior the Voyance platform also measures the risk profile for each connected device. This includes recognizing when critical assets share network segments with non-critical and/or user devices, or when network credentials meant for critical devices are misused, as well as recognizing when devices talk to suspicious URLs or IPs. To this end, the solution incorporates over 300 billion global threat data points from a constantly updated URL and IP threat intelligence database.

AUTOMATING SECURITY ENFORCEMENT TO RESTRICT ACCESS TO MALICIONS OR COMPROMISED DEVICES

If an abnormality is detected, Voyance platform seamlessly integrates into a customer's cybersecurity workflow via their SIEM or other Network Access Control (NAC) and identity systems, such as Cisco ISE via pxGrid. This allows customers to enact corrective action directly within Voyance such as quarantining, revoking access, or other customer defined actions through direct integrations to their existing infrastructure.

ENABLING GLOBAL INDUSTRY VIEWS INTO IOT THREATS, BEHAVIORS, AND PERFORMANCE BENCHMARKS

With patented cloud-native technology that provides anonymized insights for all customers into IoT device global behavior and threat data, Voyance IoT allows customers to compare device behavior to other anonymous Voyance customers to gain objective answers to questions surrounding IoT performance and security. By leveraging our anonymized industry baselines, customers can quickly create a path to improve your security program maturity.

TRACKING UTILIZATION AND PERFORMANCE OF IOT DEVICES TO PROVIDE KEY OPERATIONAL INSIGHTS

The highly scalable and mature Voyance device performance analytics solution is deployed in hundreds of enterprise access networks and gives customers detailed knowledge of every single IoT device in their environment, where they are located, and their level of use. Customers also gain insight into problematic devices that are having issues connecting to their application with detailed root-cause analysis and remediations.

A RICH SET OF INTEGRATIONS

Voyance provides a flexible and secure API using GraphQL allowing customers to integrate with other solutions or custom applicaitons to fit within the overall enterprise security framework. The platform also offers extensive set of vendor and technology integrations, allowing customers to get the most out of their existing infrastructure and software investments:

- Network Access Control (NAC) and identity systems: Cisco ISE, Aruba/HPE ClearPass, FreeRADIUS, Microsoft RADIUS
- Security threat control platforms: Cisco's Platform Exchange Grid (pxGrid). Voyance is a certified solution on the Cisco pxGrid ecosystem
- Wireless LAN: Cisco, Aruba/HPE, and Extreme Networks
- CMDB: ServiceNow native integration
- SIEM: Splunk and others via extensible Voyance platform APIs
- Netflow: for wired infrastructure

CONCLUSION

The growing wave of IoT devices brings both big challenges and huge business opportunity. The right AIOps platform can ensure a successful IoT strategy for mission critical deployments at internet scale. Security and Network teams have the most comprehensive view of IoT deployments from the enterprise level to the individual device. Going beyond basic security and tailoring it to the unique nature of the IoT lifecycle provides operational assurance and delivers the following benefits:

- Quantifying utilization, risk & performance of critical IoT assets
- Wired and wireless device support; vendor agnostic platform
- Baselining IoT device behavior for threat-detection and risk assessment
- Proactive enforcement of IoT security policies
- Extensive set of vendor and technology integrations via extensible Voyance platform APIs
- Role-based access control (RBAC) to customize product views and controls to address the needs of different personas - IT, cybersecurity, and line of business owners

The Voyance AIOps Platform

The Nyansa Voyance AIOps Platform is the industry's first full-stack vendor agnostic platform for network performance and IoT operational assurance with the integration of IoT security and device performance analytics in a single platform. Employing context relevant machine learning and big data analytics, the Voyance platform collects and analyzes extensive data including packet and flow data, wireless metrics, system log metrics, global threat and IP enrichment data.

About Nyansa

Credited with developing the industry's first cloud-based enterprise network analytics platform, Nyansa is a fast-growing innovator of advanced IT analytics software technology and operates the world's largest and the only vendor-agnostic public analytics service – observing and analyzing traffic across hundreds of production sites with more than 20 million client devices around the world.

The Nyansa Voyance platform is the industry's first full-stack vendor agnostic platform for client experience and critical asset protection.

Employing context relevant machine learning and big data analytics, the Voyance platform collects and analyzes extensive data including packet and flow data, wireless metrics, system log metrics, global threat and IP enrichment data. Nyansa's Voyance product is available as a public SaaS service or as a pre-configured private cloud solution.

Customers range across a variety of industries including companies such as MuleSoft, Stanford University, Uber, Tesla, Mission Healthcare System, San Francisco International Airport, American Eagle Outfitters, and the Mayo Clinic.

Voyance is available for proof of concept demonstrations at no cost. The system is typically deployed and operational in under one hour.

1. IDC: Worldwide Semiannual Internet of Things Spending Guide
2. Vodaphone IoT Barometer 2019
3. IDC FutureScape: Worldwide IT Industry 2019 Predictions
4. Bain & Company IoT Customer Survey 2018