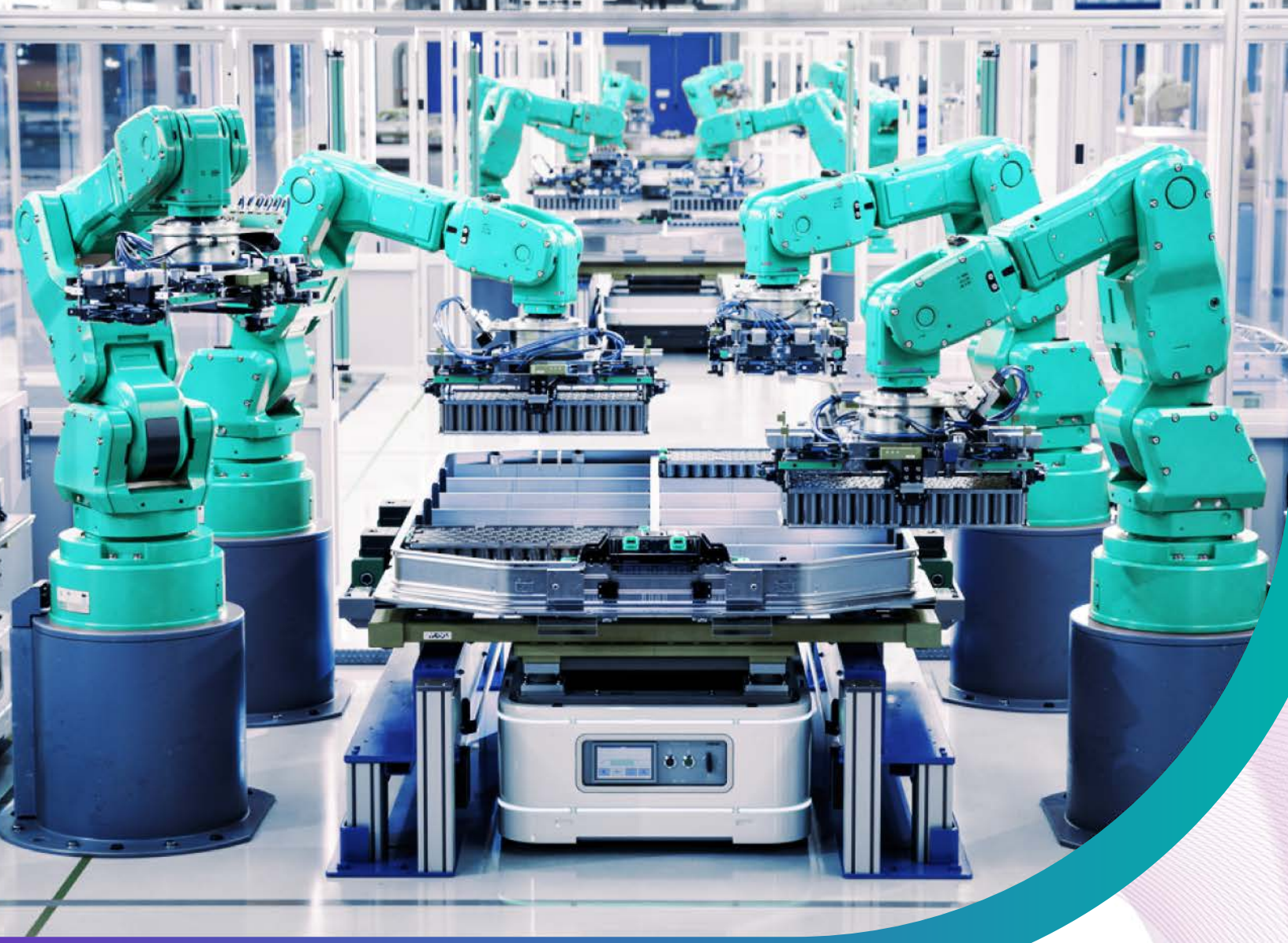


WHITEPAPER

Enabling Manufacturing and Supply Chain Transformation with a Unified SASE Approach

aryaka

TABLE OF CONTENTS

Executive Summary

The pandemic and digital transformation have rapidly accelerated changes in manufacturing and the global supply chain. Technologies like cloud, big data, social, mobile, hybrid worker support and IoT are powering a transformation that is often labeled Industry 4.0.

Optimal network connectivity remains the fundamental enabler of a successful digital business transformation. Unlike traditional enterprise WAN and SD-WAN approaches, which were overall static solutions that cannot adapt to the speed of digital business, a Unified SASE as a Service approach can. In our current, fast-changing business environment, the DIY approach (do-it-yourself) to SD-WAN and SASE (Secure Access Service Edge) has many challenges, such as the need for expensive resources as well as CAPEX-intensive OEM contracts. Carrier provided SDWAN services may be an option, but are hampered by last and first-mile lock-in, long rollout times, no single SLA and multiple contracts for end-to-end connectivity.

Aryaka's solution is tailored to the needs of digital transformation. Aryaka's Unified SASE as a Service solution is delivered as a fully managed and/or co-managed service that includes out-of-the-box direct cloud connectivity, application acceleration, WAN optimization and SASE enablement. As an end-to-end service provider, Aryaka also manages your first and last-mile connectivity. Unlike other solutions, Aryaka's SLAs are applicable from the first day of commercial operations.

Introduction: The Pandemic's Lesson about Adaptability

Over the last few years, we have learned that the enterprise architecture needs to be able to adapt to disruption as quickly as possible.

Few organizations were adequately prepared for the sudden challenges that emerged in 2020. The confluence of a global health pandemic, social and political unrest, and worsening climate events upended the private and public sectors around the world. Mounting challenges since that time have expanded the concept of preparedness in ways many leaders did not anticipate. While the global pandemic was an unprecedented event, clearly organizations must be better prepared.

According to a report by Deloitte[1],

"More than six in 10 of those business leaders surveyed said they think we're likely to see either occasional or regular disruptions of this scale going forward, and three quarters said they believe the climate crisis is of similar or greater magnitude compared to the COVID-19 pandemic."

Clearly, this will drive dramatic changes in enterprises' approach when it comes to their digital enterprise architecture, which includes business process, application, data and network technology architectures. After all, the network plays the central role in connecting and securing every end point in the enterprise architecture, allowing customers, employees, and business partners to access critical applications and data – securely, anytime, and from anywhere.

The pandemic has been a disruptive event due to its macro-economic impact across the entire global geography. However, there are other recent events that exemplify the global manufacturing and supply chains' vulnerability due to security breaches or lack of up-to-date visibility. This often results in enterprises' inability to properly react to quickly changing - but predictable - circumstances.

Let us highlight a **recent example** that crippled the global supply chain – completely unrelated to the challenges posed by the global pandemic:

'Ever Given' was traveling through the Suez Canal, when it was caught in a sandstorm and ran aground due to poor visibility and lack of effective control. As a result, it blocked other vessels from transiting the waterway, one of the world's most important maritime trade routes.

March 26

Almost 300 vessels were reported by Bloomberg to have queued up.

March 29

'Ever Given' finally set adrift after moving over 30,000 cubic meters of sand.

April 13

"Ever Given" was seized by a court in Ismailia after a request for compensations exceeding **916 million US dollars.**

Economic impact

Lloyd's List estimated during the blockage the value of the goods delayed **each hour at US$400 million** and that **every day** it took to clear the obstruction would disrupt an additional **US$9 billion** worth of goods.

As we saw above, and we shall see confirmed again in this white paper by several studies, the global manufacturing and supply chain system - which sits at the very core of the $95 Trillion global economy - is not just vulnerable to singular events like the global pandemic. On top of the Suez Canal example, we hear on a near weekly basis of disruptions to **critical pipelines** or **healthcare systems.**

We can contend such devastating business issues are caused by four major issues:

Insufficient visibility

In complex, hyper-connected systems, complete vertical and horizontal visibility is key to gain the necessary insights to take immediate - and ideally pre-emptiveaction as a remedy.

Limited control

Any complex system consists of separate domains, and domain experts only have limited ability to diagnose and resolve issues. They need to reach out and collaborate with separate domain experts, which slows down response time and turns it into a potentially error-prone collaborative swivel-chair integration effort.

Complex workflows

The more complex a system, and the fewer effective abstractions it provides, the less manageable it becomes. This results in non-integrated, often manual, and thus error prone workflows. Unforeseen circumstances completely overwhelm such systems and their operating staff.

Security vulnerabilities

Security represents a critically important topic: it can render the three issues on the left irrelevant. Security can result both in data breaches as well as a complete inability to operate the underlying infrastructure if hijacked by certain types of attacks.

In this white paper, we will examine what this means for the emerging network and security infrastructures in manufacturing and the global supply chain. Finally, the paper will highlight the risks of embarking on a digital transformation initiative without considering the enterprise WAN infrastructure.

Digital Transformation

The call for digital transformation had started to sound a bit cliché prior to the pandemic. However, the imperative for digital transformation initiatives was proven and accelerated during the pandemic, as evidenced by Gartner in "COVID-19 Response: Top 7 Cost Reduction Actions for I&O Leaders"[1]. Digital transformation holds the power to make or break organizations. Organizations of all sizes and in every sector had already embarked upon some form of digital transformation (DX) initiative, and those happen to be some of the few initiatives that were not de-funded, but in fact accelerated during 2020 and 2021. Unfortunately, before 2020 many organizations still refused to recognize the relevance of the underlying network and network security layers as strategically important elements of a secure and adaptable digital infrastructure. A well-designed enterprise WAN must support successful DX initiatives. However, a poor WAN architecture for cloud, big data and mobile has the potential to derail the process – as many enterprises discovered during the pandemic or during security breaches that overwhelmed the capabilities of traditional systems.

IT leaders today have a good understanding of the role that technologies like cloud, big data, social and mobile play in digital transformation. These higher-level technology stacks get most of the attention, while foundational areas like enterprise WAN connectivity were often ignored. This has started to change during the pandemic, which has accelerated WAN transformation projects as enterprises rush to adopt SASE (Secure Access Service Edge) architectures.

In the pre-digital transformation era, the CIO was the sole decision maker in all technology-related issues. This traditional decision-making structure has unraveled with the arrival of new stakeholders. In the post-pandemic world, and with SASE planning in full effect in over 50% of enterprises according to Aryaka's 2021 State of the WAN report[2] CIOs, CSOs, CMOs and CDOs must come together to drive an effective enterprise architecture strategy.

Departments such as supply chain, logistics, manufacturing, and others must collaborate to implement focused digital initiatives. Clearly, without CIOs', CSOs' and network architects' participation, the impact of these digital transformation projects is not factored into the WAN design, leading to questionable alignment with overall digital business needs due to poor application performance.

Business Continuity in the Global Supply Chain

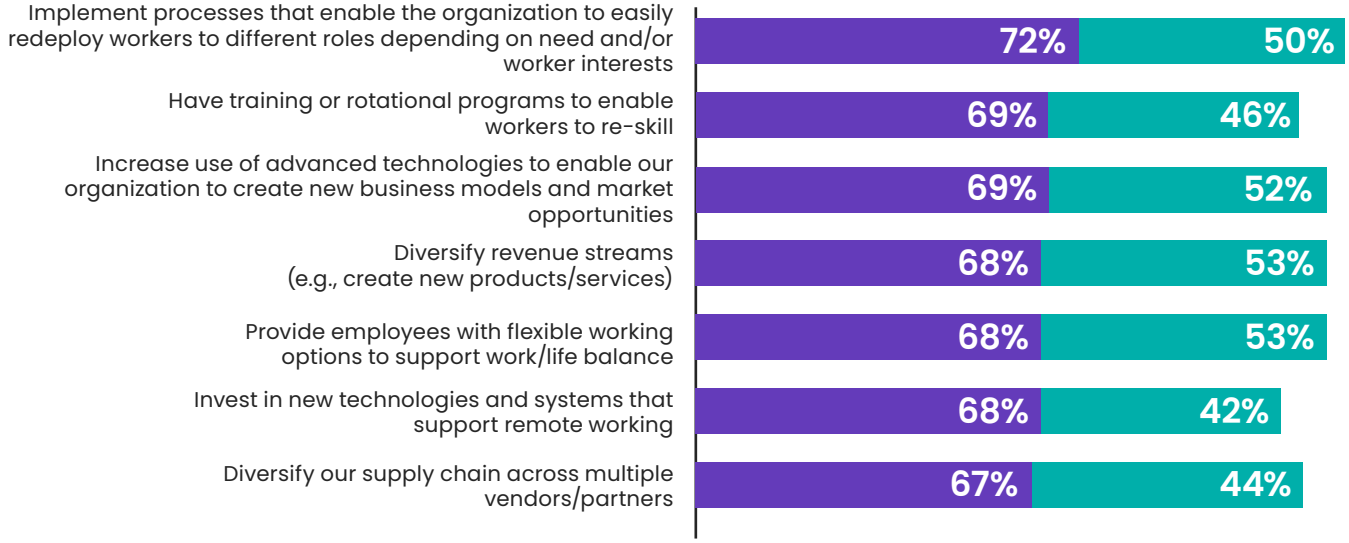
"The biggest benefit of deploying Aryaka has been gaining the ability for our overseas locations to communicate freely within the network and access to content sharing, files and communication."

- **Network Engineer, Large Enterprise Industrial Manufacturing Company**

The global pandemic has highlighted how enterprises that had advanced digital initiatives were better prepared for a disruptive event, as highlighted in the graphic below, from Deloitte Global Analysis[3].

Companies that took key actions before 2020 were more likely to say that they are weathering the pandemic well or very well

Percentage of CXOs who said their organizations are weathering the events of 2020 well/very well, as compared to their competitors/peers:



Source : Deloitte Global Analysis

Pacesetters: Done prior to 2020

Planning to do in the next 1-5 years

What are the key strategic considerations for "preparedness" according to the respondents to the Deloitte report? What were the strategic organizational characteristics they drove in their organizations before 2020 as they advanced their digital transformation initiatives?

Prepared: More than 85% of CXOs whose organizations successfully balance addressing short - and longterm priorities felt they had pivoted very effectively to adapt to the events of 2020, whereas fewer than half of organizations without that balance felt the same.

Aryaka's OnePass™ architecture is always prepared: Enforcing policy consistently and without user performance impact across global scale deployments.

Adaptable: Leaders recognize the importance of having versatile employees, especially after a year like 2020. To that end, flexibility and adaptability were, by far, the workforce traits CXOs said were most critical to their organizations' futures.

Aryaka's Flexible Delivery options allow organizations to implement the solution their way, at their pace and to choose from self-managed, co-managed and Aryaka - managed service delivery.

Collaborative: CXOs indicated the importance of collaboration within their organizations, noting that it sped decision-making, mitigated risk, and led to more innovation. In fact, removing silos and increasing collaboration was one of the top strategic actions CXOs took before and during 2020.

Aryaka Services cover a comprehensive and integrated set of Unified Policy, Network Security, SD-WAN, App Acceleration, Observability, integration services and 3rd party solutions.

Pulse A YAGEO Company

"Aryaka increased the productivity of our end-users and enabled digital transformation initiatives and Industrial Internet of Things (IIoT) Projects."

"Collaboration is key in this new world. The people who will succeed in the future are those who are focused, not just on their own jobs and agendas, but on the bigger-picture goals, as well. They are able to listen, collaborate, and understand what others are trying to accomplish. It's about working together to achieve mutual goals which, in turn, benefits everyone."

- **Rahim Hirji , Chief Risk Officer, Manulife**

Trustworthy: CXOs understand the challenge of building trust. More than a third of responding CXOs were not confident their organizations had done a good job developing trust between leaders and employees. Those who are succeeding are focusing on improving communication and transparency with key stakeholders, as well as leading with empathy.

Aryaka's Zero Trust WAN is A global private network backbone that delivers security and performance from the first to the middle to the last mile of the network - designed to support the architectural and regulatory needs of any organization.

"Trust is built in normal times, but it's really tested during the hard times. When you can stand by your people and your clients in times like these, you really earn that trust and strengthen your relationships more than ever before."

- **Linda Seymour, CEO, HSBC Canada**

Responsible: Most CXOs acknowledge that the business world has a responsibility beyond the bottom line. Eighty-seven percent of surveyed CXOs who said they have done very well at balancing all their stakeholders' needs also felt that their organizations could quickly adapt and pivot in response to disruptive events. That is nearly 50 percentage points more than the proportion of CXOs who said the same at organizations that haven't done well at balancing their stakeholders' needs.

Aryaka's high net promoter score (NPS) of 65 and 4.8/5 star rating on Gartner Peer Insights represent the quality of customer experience and trust.

"We have a responsibility to a large ecosystem of stakeholders to advance a more equitable, just and sustainable economy. So we're focused on minimizing the negative impact of our business and making a positive impact across the company's entire value chain for the long term."

- **Hollie Castro, Senior Vice President, Talent & ESG, YETI**

Clearly, these cultural traits in an organization need to be supported by the underlying technology infrastructure. For example, effective collaboration and trust cannot exist if network and technology architectures do not deliver on availability or end user experience.

The pandemic revealed that critical business process success depends on employees, business partners and customers having the ability to successfully communicate over a reliable infrastructure that delivers on an enterpriseclass user experience. If participants in the business process lose trust in the infrastructure they rely on to effectively drive collaborative business outcomes forward together, they may well disengage over time – or seek different business peers and partners to collaborate with whose infrastructure is up to par.

The network and network security infrastructures are the foundation to such collaborative business processes and to enable the over-arching adaptability to change we have established as a key requirement in digital transformation.

Digital Transformation is Driving Network Transformation

Irrespective of the industry sector, the key areas of digital transformation are:

Customer Centricity

Customer experience has always been central to businesses. In order to gain a better understanding of customers, firms have primarily relied on market research, and customer surveys conducted offline with a small representative sample space. However, now, with the almost universal adoption of social media and other digital channels, organizations must leverage their ability to reach customers directly, enabling them to understand customers better and ultimately deliver better products and services. Digital channels also provide more direct and realtime feedback that traditional market research never did. To fully exploit this opportunity, firms need a robust IT infrastructure built on a solid enterprise WAN foundation to deal with the terabytes of data collected from these interactions.

Streamlined operations

While a plethora of digital channels give organizations a solid understanding of customer requirements, to act on those requirements and deliver the products and services requires operational efficiency and agility. Operational agility is achieved in several ways: the move to cloud technologies and adoption of Software-as-a-Service are some of them. Others include the use of big data analytics and AI to generate business insights or the deployment of IoT in areas such as logistics and supply chain management. Adoption of these new technologies has a direct impact on the enterprise WAN and security. The WAN must now be capable of securely carrying vast amounts of data in real time while having the ability to distinguish business-critical application data and real-time data from non-critical ones. The performance of many AI algorithms is directly dependent on network quality of service.

Constant innovation in business models

The industry landscape is replete with examples of companies that once dominated their sectors, only to be beaten by nimble startups with innovative business models. For example, Netflix would never have achieved its success without an ability to rely on a global networking and content-delivery infrastructure based on cloud delivery. The much admired and often copied Netflix recommendation system relies on a cloud architecture for collecting, saving, and analyzing massive amounts of customer data. None of this would be possible without a robust and secure global WAN.

IT and OT integration

Digital transformation is resulting in a huge increase in the data that traverse the enterprise WAN. This data increase comes from two sources, information technology (IT) systems and operational technology (OT) systems. IT is used for data-centric computing while OT is used to monitor events, processes and devices and adjust in enterprise and industrial operations. Traditional MPLS networks were designed to handle IT traffic primarily from the user to the inhouse datacenter. Owing to the rapid adoption of Software-as-a-Service, most WAN traffic is from the network edge to the cloud provider. Traditional Enterprise WAN architectures leveraged MPLS as a backhaul technology to centralized headquarters, and hence were never designed to handle the volume, variety, and velocity of this traffic.

Technologies like social, mobile, big data analytics, cloud and IoT help organizations improve customer experience, simplify operations, and introduce new business models. The massive amounts of data collected, stored, and analyzed by these technologies requires a robust Unified SASE architecture with state of art network and security technology integration. That does not only ensure a superior user and customer experience, but also ensures regulatory compliance as well as the ability to build a solution optimally tailored to flexibly address the needs of any enterprise architecture.

The data deluge that characterizes digital technologies requires sophisticated network policy-based routing policies as well as data security in place. At first sight, this seems to solve the network bandwidth and data integrity challenges discussed previously. However, due to the virtual overlay nature of traditional SD-WAN architectures, latency, jitter, packet loss and security issues remain. The SD-WAN overlay model - which remains an integral part of most vendors' SASE architectures just outsources QoS and SLA guarantees to the underlay. It offers no real tools to enforce a superior user and customer experience, which is a fundamental IT requirement in the digital era.

In essence, the key deliverables of digital transformation - namely, customer experience, operational excellence, new business models and IT/OT integration - are achieved through the deployment of innovative new technologies. These technologies, in turn, require an innovative and Unified SASE architecture that converges networking and security onto one seamlessly integrated platform. Aryaka is unique in providing such a Unified SASE solution, delivered as a service.

Unified SASE (Secure Access Service Edge) Must Enable Digital Transformation in Manufacturing

Manufacturing and Supply Chain have accelerated their digital transformation initiatives in recent years, influenced by both a rapidly changing industry landscape as well as the lessons learned from the global pandemic.

As Forrester mentions in "Predictions 2021: Smart Manufacturing; October 28th, 2020", manufacturers have learned lessons from the pandemic and are actively investing to deliver greater flexibility, resilience, and adaptability as well as innovation. SASE architecture is among the tools that the supply chain and manufacturing vertical is heavily investing in.

COVID-19 dramatically accelerated the hybrid workforce movement, but it was not quite enough: headlines about panic buying of toilet paper and pasta and shortages of personal protective equipment reminded the world that the often-invisible manufacturers and logistics companies that keep everything moving were not quite prepared. Other vulnerabilities like the Suez Canal incident and several other security breaches - including ransom-ware attacks-further proved it.

Going forward, ossified and inflexible business processes designed over years to standardize cost control, efficiency, and predictability will be replaced by processes that emphasize flexibility, adaptability and resilience. As they plan forward, manufacturers and supply chain companies will have internalized the lessons of the pandemic, doubling down on technology-enabled strategies to deliver flexibility, resilience, and innovation.

According to Modor Intelligence, digital transformation in manufacturing is expected to register a CAGR of over 19% from 2024-2029[4]. Digital transformation is being incorporated into every aspect of the manufacturing process, from the factory floor to R&D, supply chain, logistics, operations, sales, and marketing. The essential forces driving digital transformation in this sector are the deployment of industrial internet of things, cloud adoption and big data. These are the major transformational elements of what is called Industry 4.0, with many leading industry analysts already suggesting we are moving on to Industry 5.0[5].

Smart Factories

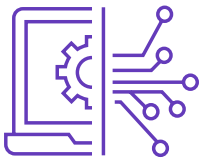
Manufacturing is headed into an agile world where end-users or partners customize and perhaps even design a product. The manufacturing chain is then smart and responsive enough to tailor the production process to the very specific needs of that customer. We are still in the era of mass manufacturing and economies of scale, but we are inevitably moving to an environment where the ability to customize individual products to client requirements will become vital. Some industry verticals like - for example - the automotive sector already allow for fast customization.

Smart Manufacturing is focused on delivering ubiquitous Industrial IIoT in the factory floor, integrating it with supply chain systems and production systems. IoT can provide real-time feedback and alerts; with predictive analytics, it can even flag faults before they occur. These critical yet straightforward implementations of IoT reduce cost and waste. Given the scales involved in manufacturing, even a single percentage saving can result in enormous benefits.

However, integrating IoT into the manufacturing eco-system results in an enormous increase in the amount of data carried over the enterprise WAN and therefore SASE infrastructure.

Dark Factories

The global pandemic is also fostering the concept of "dark factories", which are "dark" because automation does the actual manufacturing and workers can be remote or operate from control rooms. This is already an established practice in environments that require sterile, uncontaminated facilities.



Big Data, Artificial Intelligence and Machine Learning

Where there is data, there must be data analysis to turn data into insights. The benefit of IoT and smart factories is the availability of vast amounts of clean, structured data. Not many sectors can boast of having access to such highquality data. AI and MI algorithms are used to streamline supply chains, as well as predict and prevent faults before they occur. For manufacturers, sensor data from the factory floor or from digital twins once the widget is in the hands of the customer is not the only source of data.

The real benefits accrue when this data is combined with information from marketing, sales, customer service and other departments. Collecting, storing, analyzing, and securing this volume of data is critical to success. SASE infrastructures must deliver on the strict network SLAs and end-to-end security required to enable AI-enabled workflows.

Manufacturing Execution Systems Moving to the Cloud

Cloud migration is a recurring theme that we have seen in all industry sectors, be it retail, banking, healthcare, and manufacturing. Today's SaaS applications like Microsoft 365 or Salesforce are ubiquitous. However, what makes the cloud both challenging and exciting for the manufacturing and supply chain ecosystem sector is the migration of Manufacturing Execution Software (MES) to the cloud. MES is critical software that enables global manufacturers to manage and control manufacturing and shop floor operations and, provides access to real-time manufacturing data to make quick and informed decisions.

This becomes critical given the global nature of the manufacturing and supply chain ecosystem: the factory may be in China, Taiwan or Japan, while the designers and managers are located in the US or Europe. Transferring plans and other information between these locations is a bandwidth-intensive activity.

When such critica systems are spread geographically and operate in a Software-as-a-Service model, the enterprise WAN that connects them becomes very critical. Furthermore, supply chain ecosystems are starting to explore how highly distributed emerging DLT (distributed ledger technology) Blockchain-based solutions can streamline operations.

Hybrid Workforce

81% of IT professionals surveyed in Aryaka's 2024 Secure Network Transformation Report say that hybrid work drives demand for SASE and Zero-Trust networking. The global pandemic has forced every industry vertical - including manufacturing - to accommodate a hybrid workforce approach. Far more effective support for remote employees is required in an environment that - going forward - must be able to quickly pivot when it comes to supporting many workers being remote at any time.

WAN and Security Transformation with Unified SASE

There is one common dependency for all the trends we discussed above: they rely on an agile, high performance network and security infrastructure. Prioritizing mission-critical data amidst this data deluge, securing, and isolating the IoT devices as well as providing a low latency path are requirements that are addressed only by the WAN capabilities within a Unified SASE architecture. These must deliver on performance, agility, simplicity and security to accelerate critical applications, route sensitive data into secure microsegments and provide a low latency path for real-time data traffic.

"We now have the infrastructure in place to handle the upcoming cloud migration and can deliver data and applications to every end-user, as if it lived in this local data center. We're able to provide our customers with machine tool information, and pricing, in a much faster rate. Instead of taking six to seven hours to get that information from Japan, we were able to provide that to our customers within 20 minutes."

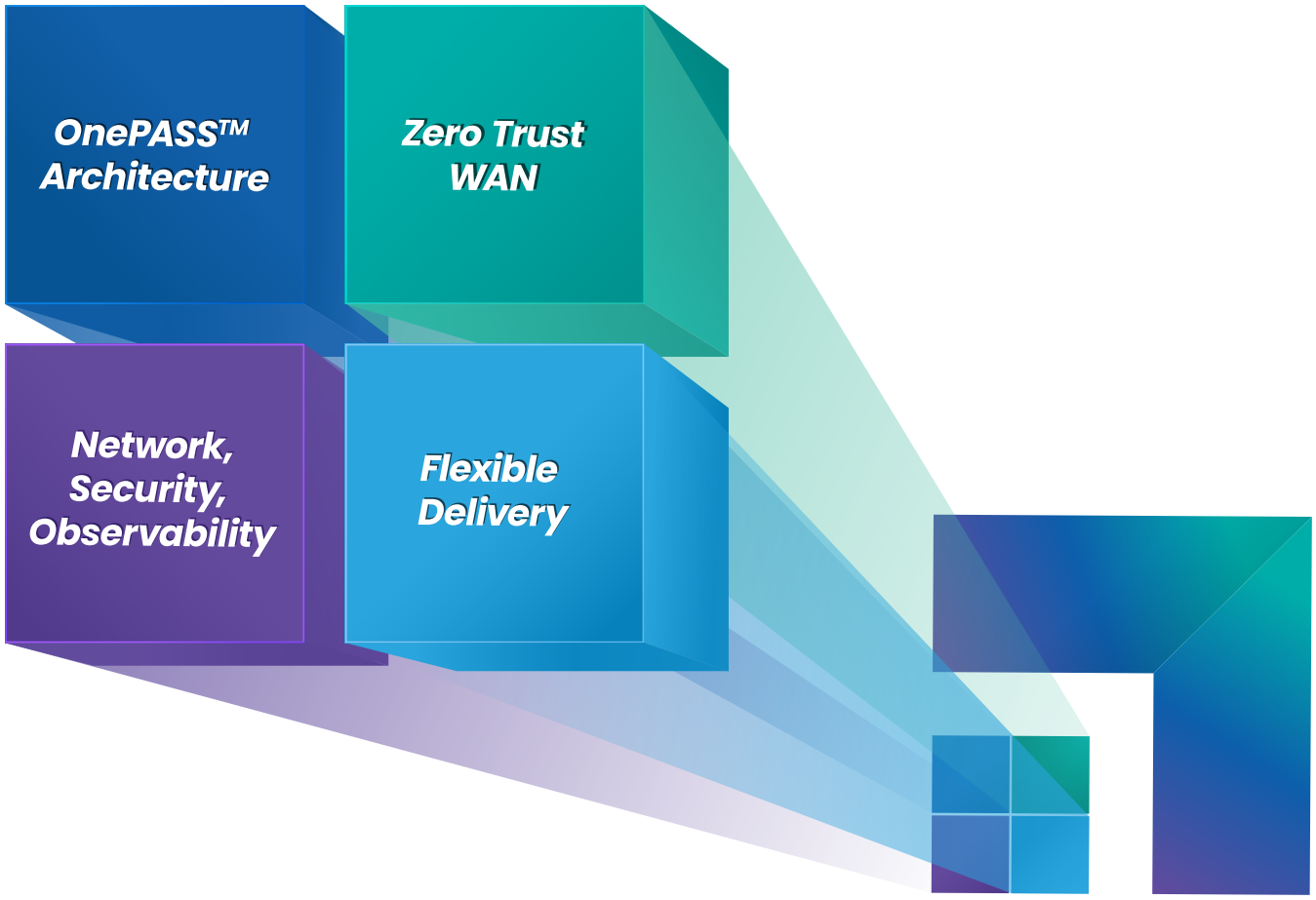
- **Glenn Hensley, IT Infrastructure Manager, Makino.**

As a global leader in metal-cutting and manufacturing with locations in Europe, North America, Japan and other regions of Asia, Makino needed a better way to expediate the exchange of massive schematics between distributed R&D groups and tech centers. What's more, the company plans to move 90% of its applications to the cloud, so it needed a WAN option that would guarantee application performance and accommodate that migration. Although Makino had used WAN Optimization hardware to try to meet its performance needs, deployment was cost prohibitive and difficult to scale or manage. They also looked at Internet-based SD-WAN options, but realized latency issues between the United States and Asia locations would scuttle performance. Instead, Makino went with a fully managed SD-WAN as-a-service with the features mentioned above. This resulted in dramatic improvements. Files that used to take 6-7 hours to synchronize, now take 22 minutes. New sites may be added to the network in 2-3 days, compared to the weeks and months it would take with MPLS. And the company now has the platform in place to painlessly accommodate the shift to the cloud.

MAKINO

Aryaka's Unified SASE Delivers the Foundation for Digital Transformation in Manufacturing

Network and network security transformation are foundational enabling technologies for digital transformation. While digital transformation use cases differ by sector, there are similarities in the network transformation needs like cloud application performance, speed of rollout and security. Other aspects of similarity are the east-west traffic from IoT devices or machine-tomachine traffic and operational simplicity. In this section, we explore Aryaka's unique answers to these challenges.



Cloud Application Performance

As manufacturing companies increasingly move to the cloud, cloud application performance becomes of paramount importance. Cloud applications can refer to SaaS applications like Microsoft 365, Salesforce or emerging MES solutions, as well as other applications running on IaaS platforms like Amazon AWS, Alibaba Cloud, Google Cloud, Microsoft's Azure, or Oracle Cloud. Increasing cloud adoption has a direct impact on traffic optimization and network security.

71% of surveyed manufacturing organizations said Aryaka accelerates their global application performance.

Aryaka's fully managed Unified SASE as a Service comes with direct connectivity to all major IaaS platforms. When connected to Aryaka's Zero Trust WAN, customers have a secure expressway to IaaS platforms. For users of SaaS applications, Aryaka provides a 'Virtual Office' solution. With a Virtual Office connection, application traffic is transported over Aryaka's private core to the PoP that is closest to the SaaS provider, dramatically accelerating application performance. In addition, features like built-in WAN optimization and data de-duplication ensure that users always experience great application performance.

Speed of Rollout

As a Unified SASE solution, Aryaka can deliver connectivity in just a few days rather than months. This helps manufacturing companies to extend their global reach at the speed of digital business and optimize the connectivity of the supply chain system.Also, Aryaka guarantees end-to-end performance with Day 1 SLAs with 5-9s availability – no need to wait for "network stabilization."

"Aryaka gives us an all-encompassing solution with their own network, POPs, managed services, SASE, etc. The other vendors had excellent technology, but they were just selling boxes."

- **Technical Architect, Global Transportation Company**

Security

Increased traffic and internet access from the branch increases flexibility and performance. However, it also creates a security loophole. Aryaka enables enterprises to deliver on a Unified SASE architecture that converges all networking and security components optimally tailored to any manufacturing enterprise's particular architecture and regulatory needs.

93% of IT organizations agreed with the following statement:

"I prefer Aryaka's flexible approach to security that allows me to select my own security vendors to fit my organization's needs."

IoT and M2M Traffic

IoT is used extensively in sectors like healthcare, manufacturing, retail, and logistics. Traffic from sensors and other devices are bursty, often mission-critical and very sensitive to latency. Aryaka's SD-WAN can identify over 3,500 applications and map them into very granular routing and security policies according to business needs.

Operational Excellence

As the complexity of the SASE infrastructure increases, the complexity of associated operations also increases dramatically. Specialized resources are required to design, configure and monitor the network. Commercial contracts and billing become complex. Thus, the agility of the IT team to respond to business requests is diminished.

With Aryaka's Unified SASE as a Service, customers have a single point of contact for all issues related to the WAN and security with proven capabilities as validated by Gartner Peer Insights, Forrester, Dell'Oro, NPS, and others.

Aryaka's solution includes the first and lastmile management along with link procurement services. The MyAryaka Cloud Portal provides the status of the entire WAN, including the first and last mile. Customers can also easily monitor the performance of cloud as well as on-premise applications from the MyAryaka portal.

Key Benefits of Aryaka's Unified SASE as a Service Solution

Hybrid Workforce

Aryaka's SmartSecure Private Access solution leverages the performance of Aryaka's Global Layer 2 Core Network with its architectural Cloud-First approach to provide the optimal solution for enterprises seeking an optimal approach to remote worker connectivity: a solution that combines flexible utilization of deterministic, dedicated network resources to both branch as well as remote workers over a high performance network. Aryaka's Private Access solution always delivers on maximum performance - irrespective of traffic shifts between branch and remote worker traffic - with consolidated visibility into network and application performance across enterprise core connectivity as well as VPN domains.

Complete architectural integration of visibility, control and orchestration tools

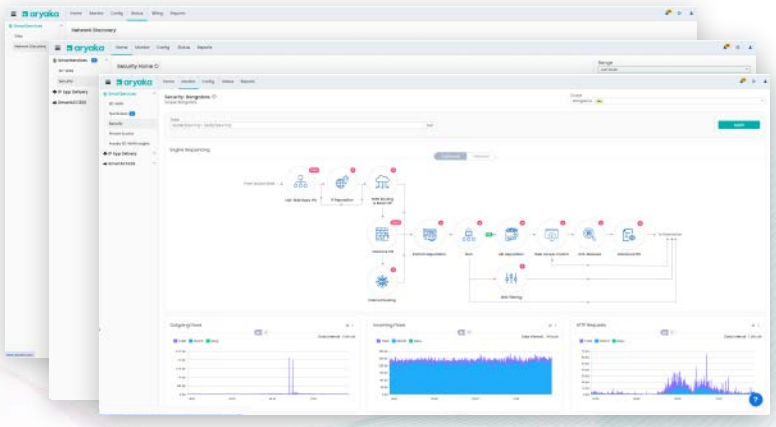
The Aryaka Global L2 Core network provides strict deterministic behavior with SLAs that are always guaranteed. This avoids the visibility and control opacity that afflicts traditional SD-WAN architectures.

Strict QoS Guarantees

Network SLA guarantees are never outsourced to an underlay transport network the policybased routing engine has no control over. The Aryaka global L2 core network always delivers on guaranteed performance.

Complete Visibility into Network and Application Performance

The MyAryaka portal provides complete vertical and horizontal observability into every element involved in packet delivery, including the last mile, middle mile and any physical or virtual resource.



Simple Workflows

With Aryaka, network architects don't need to perform swivel chair integration between different visibility and control tools to diagnose issues and implement the configuration changes required to fix those. The MyAryaka portal provides the complete visibility, configuration, and orchestration functions to drive immediate optimization, whenever needed.

50% More than half of manufacturing enterprises report a decrease in their staffing and training costs by up to 50% after deploying Aryaka SmartServices.

Conclusion

In the previous sections, we saw how the compounded effect of the 2020-2021 pandemic and digital transformation have accelerated changes in manufacturing and the global supply chain. We had a glimpse of the business challenges addressed and the new opportunities created by digital transformation. Further, we explored the central role played by technologies like cloud, big data, social, mobile, hybrid worker support and IoT. Finally, we acknowledged the importance of addressing these issues with the right architecture: A Unified SASE solution that merges network connectivity and security into a single, cloud-driven framework, delivered as a service.

We noted that traditional WAN and SD-WAN architectures were not flexible enough, expensive and in many cases incapable of handling the demands of a modern enterprise. Direct cloud connectivity, application acceleration, end-to-end security, and true WAN optimization - with complete visibility and control - are features that are only available with the addition of operationally costly new hardware or software tools in alternative solutions. A Unified SASE as a service approach - as Aryaka's - is the only viable solution that meets all the requirements for digital transformation.

The network transformation journey is not easy, given the critical nature of connectivity and the consequences of any network outage or security breach. Optimal and secure network connectivity remains the fundamental enabler for digital business transformation. Unlike traditional enterprise WAN and SD-WAN approaches, which were static solutions that didn't adapt to the speed of digital business, Aryaka's Unified SASE approach delivers an optimal solution that delivers on the needs of any enterprise. In such a fastchanging dynamic environment, the DIY approach (do-it-yourself) to SD-WAN has many challenges, such as the need for expensive resources, box-centric workflows as well as CAPEX-intensive OEM contracts. Carrier provided SD-WAN is often seen as an option, but comes with

fundamental flaws, such as slow response times, last and first-mile lockin, no global SLAs and multiple contracts for end-to-end connectivity.

Aryaka's solution is tailored to deliver on the needs of successful digital transformation. Aryaka's Unified SASE solution is delivered as a fully managed and/or comanaged service that includes out-of-the-box direct cloud connectivity, application acceleration, WAN optimization and comprehensive SASE enablement. As an end-to-end service provider, Aryaka also manages your first and lastmile connectivity. Unlike other solutions, Aryaka's SLAs are applicable from the first day of commercial operations.

References:

[1] COVID-19 Response: Top 7 Cost Reduction Actions for I&O Leaders

[2] Aryaka 2021 State of the WAN Report

[3] Deloitte Insights – Building The Resilient Organization

[4] Digital Transformation in Manufacturing Industry Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)

[5] International Society of Automation: Welcome to Industry 5.0

About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

Schedule a Free Network Consultation with an Aryaka Expert

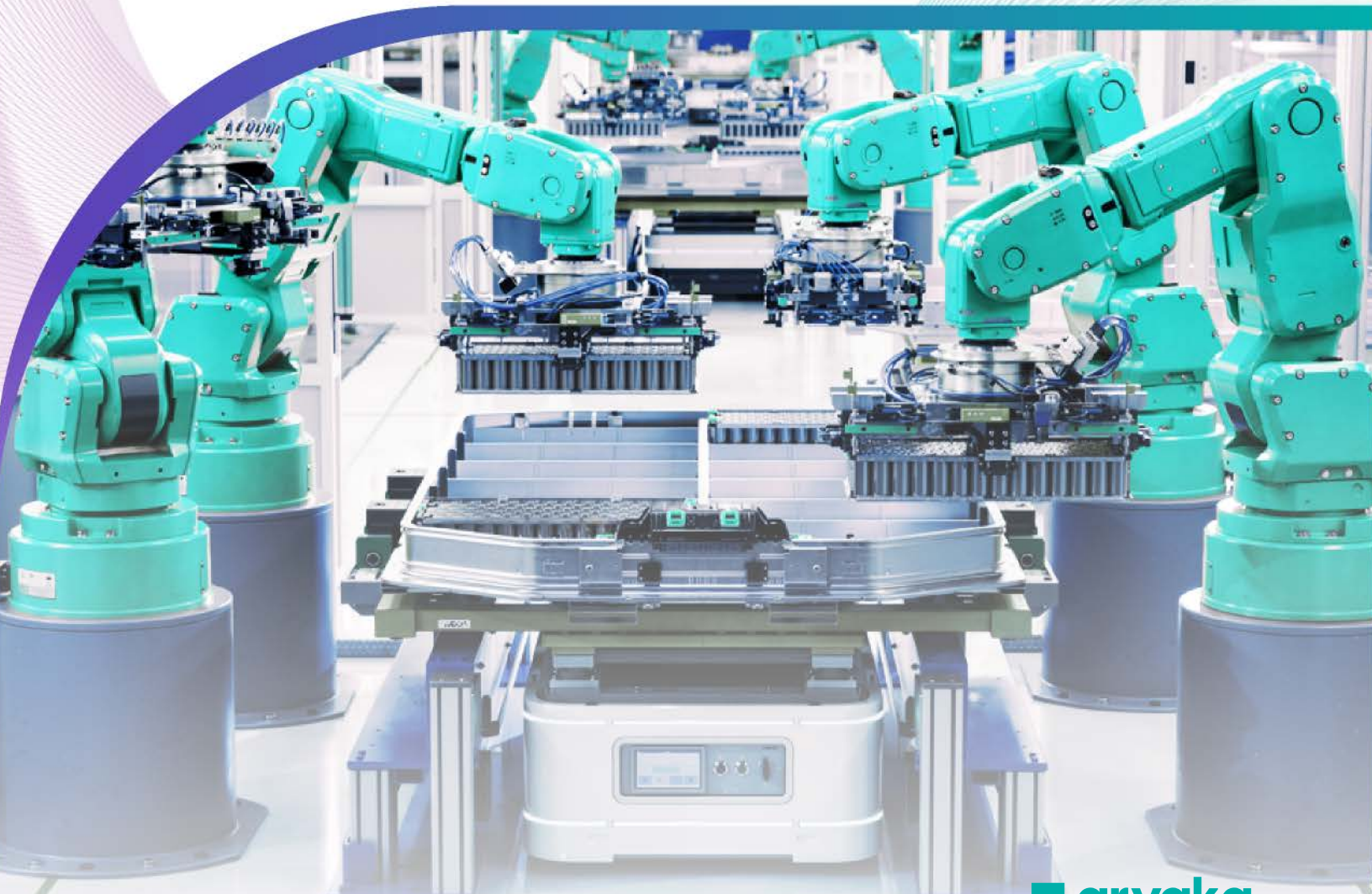
See How It Works Live →

Experience Aryaka's Unified SASE as a Service

View Interactive Demo →

Contact Us

+1.888.692.7925 info@aryaka.com



aryaka