REPORT REPRINT

Unisys positions itself as a reliable partner for IoT infrastructure management

MAY 27 2020

By Katy Ring

The company claims to deliver 'end-to-end value' from installing and connecting environments to the cloud, as well as its managed services, security and cloud support of IoT infrastructure. These capabilities have been developed around its InteliServe digital workplace services, CloudForte cloud services and Stealth cybersecurity expertise.

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

Within its IoT organization, Unisys is focused on becoming the market leader for IoT infrastructure support. Unisys claims to deliver 'end-to-end value' from installing and connecting environments to the cloud, as well as its managed services, security and cloud support of IoT infrastructure. These capabilities have been developed around its InteliServe digital workplace services, CloudForte cloud services and Stealth cybersecurity expertise.

451 TAKE

Organizations are looking to improve operations and to manage new policies and regulations around physical distancing, as applied to production lines and device management and maintenance. Some will also be considering how to switch to new revenue streams, and how to ensure the efficacy of their supply chains and logistics. All of these involve IoT technologies, and Unisys is in a strong position to deliver such projects by leveraging existing capabilities in endpoint, cloud and security support.

Context

Unisys is a midsize service provider (revenue of $2.9bn in fiscal 2019) with a sweet spot servicing the Fortune 2000. A little over half of its business is generated in North America, with about one-quarter from EMEA and the rest from Asia-Pacific and Latin America. It organizes its sales in terms of four fairly evenly split segments: financial services, commercial, public sector and US federal. The commercial sector (travel and transportation, alongside commercial communications, life sciences and retail) is slightly larger than the others, accounting for about 30% of revenue. Unisys completed the sale of its US federal business (accounting for 25% of revenue) to SAIC for $1.2bn in March.

Unisys is now predominantly an IT services business, with growth coming mostly from its InteliServe Digital Workplace Services, Stealth security solutions and CloudForte managed services offerings (designed to support the secure adoption of cloud by its customers).

From 2003 until 2018, Unisys had stalled its growth. However, under the leadership of CEO Peter Altabef, who took the helm in 2014, Unisys closed FY 19 with a second year of revenue growth and profit. With the sale of its US federal business, it should have stronger capital footing going forward. In the spirit of this new beginning for Unisys, at the start of 2020 it added IoT to its existing endpoint, security and cloud capabilities.

Strategy

Unisys enjoys a strong position working with industry standards bodies, such as the International Society of Automation, around system segmentation for industrial cybersecurity, in addition to contributing to the development of regulations via its membership in the Digital Bill of Materials (DBoM) Consortium. As a result, it works with CIOs and CISOs as they build their digital transformation strategies. In this capacity, it acts as a trusted adviser, with credibility as a systems integrator possessing both OT and IT expertise. This credibility is demonstrated in the company's work in complex and large-scale operations, such as customs and border protection for the US Department of Homeland Security, to develop, operate and manage systems for risk assessments of people and cargo using biometrics and video analytics.

Organizations across industries and governments are looking to take advantage of connected devices, such as surveillance and thermal imaging cameras, baggage scanners, and medical devices, to improve productivity and gain operational efficiency, as well as to collect critical operational performance data. Like any other connected system, these devices are complex and vulnerable to security breaches. Proprietary platforms, legacy software, lack of resources and industry regulations often prohibit security changes to the devices themselves, limiting organizations to the built-in capabilities from device manufacturers. As security needs evolve or vulnerabilities are discovered, replacing noncompliant devices becomes costly and inefficient.

Consequently, organizations taking advantage of IoT devices need additional security controls to reduce the attack surface and contain breach impact. Ideally, organizations want security remedies that are scalable, cost-effective and rapidly deployed, without disrupting the network or requiring modification to existing hardware or software embedded in devices. In many cases, Unisys can offer its Stealth software to provide a capability called Smart Wire for installation on a virtual machine or IoT gateway that connects to IPv4-based wired IoT devices, extending protection with micro-segmentation so that the device can be secured without modification of the network or operating environment. In this way, Unisys has helped secure connected medical devices by isolating electronic health record servers and encrypting data in motion from Stealth installed on a VM or IoT gateway.

Unisys has also been working as an adviser and systems integrator in the IT/OT market space in Latin America, helping utility service provider EPM to securely deliver critical utility services to homeowners and businesses in Colombia, Panama, El Salvador, Guatemala, Mexico and Chile. Unisys is providing EPM with security information and event management to protect critical infrastructure, associated IT services and SCADA/ICS systems, using machine learning as a service to identify suspicious activity on the EPM network. The relationship involves security consulting to create a long-term security roadmap with EPM.

Unisys' cybersecurity expertise typically feeds into the development of its work with IoT projects. For example, Unisys provides managed security services, supported by its enterprise data partnership with Sightline for Industry 4.0 clients. This capability provides server performance monitoring, data analysis and problem diagnosis, reporting, capacity planning, and trend analysis. Unisys is focusing on providing 'smart processes' for industrial clients in healthcare working on medical device manufacturing projects, to secure the 'what, where and who' dimensions of data usage for the data generated by medical devices. It takes a similar approach to working on smart-spaces projects with its clients. Unisys believes it is easier to incrementally solve real business problems using IoT technologies than it is to build big-bang projects such as a smart factory or a smart city, which can be far more complex and time-consuming to deliver successfully.

IoT services

The foundation of Unisys' IoT capabilities lies with the company's strong enterprise support services powered by its InteliServe platform, which uses cognitive AI to transform the way users interact with the service desk and helps users resolve workplace issues – from tech and HR to legal and finance.

Unisys has a large network of field service engineers around the globe. With the use of emerging technologies like augmented reality for remote support, Unisys is able to expand its geographic coverage and extend services to new products – all while maintaining consistency on quality, first-time resolution and customer satisfaction. This capability allows Unisys field engineers to collaborate with clients and colleagues in real time.

With consulting and integration services, Unisys works closely with partners and clients to implement IoT technologies, while remaining technology-agnostic. Consequently, Unisys does not mandate a platform, but will build an integrated system with the customer-preferred cloud provider, typically AWS Greengrass or Microsoft Azure IoT. The company's strength is in maintaining a client's IoT infrastructure as ‘always-on’ through InteliServe managed services and support, as well as its CloudForte and Stealth offerings, so that Unisys can resolve any failures within the infrastructure.

Field service for devices is often the company’s project entry point for smart endpoints. The key sponsor that Unisys works with is typically the CTO, who is in charge of the transformation of the whole organization as it moves from physical to digital services.

Unisys is approaching the IoT opportunity sector by sector, addressing energy, medical, shipping and manufacturing, to develop horizontal capabilities that can be applied across sectors. One such initiative is the Digital Bill of Materials Consortium, created and led by Unisys to address supply chain fraud by determining the origin of device components. A certificate and distributed ledger system can be implemented to forensically track all steps in manufacturing. This means that there is visibility into chip design, chip fabrication, subassembly and code version, as well as the distribution, integration, consumption and decommissioning of device parts, for members of the consortium.

Competition

Competitors in the IoT service-provider space include Deloitte, Equinix, Harman Connected Services, IBM Global Business Services and Wipro. From the OT services side of the market, other players include ATS, Emerson Process Management, National Instruments and Rockwell Automation. From the field service engineering capability side, specialist players such as ServiceMax and Source Support also compete with Unisys from time to time.

SWOT Analysis

STRENGTHS

Unisys is well known as a service provider for security solutions and infrastructure management, and has analytics expertise in transportation and the public sector, with a library of predictive models. This, combined with a core competency in field services, suggests that Unisys is well positioned for commercial growth from projects with an IoT technology component.

WEAKNESSES

The budget holders for IoT projects are typically production managers looking to improve productivity, while Unisys is better known by IT budget holders and thus needs to become better known by the business-line decision-makers. This might be addressed by the creation of an advisory practice around process productivity.

OPPORTUNITIES

Connected devices create new threat vectors, which means that the secure IoT infrastructure management market holds lots of potential for Unisys in areas where it already has experience, such as the retail, transportation and public sectors.

THREATS

The deployment of IoT technologies requires a large ecosystem, including a wealth of niche specialist players. In order to bring some cohesion, global standards are needed. Unisys is active in this area with its DBoM work, alongside partners such as Bosch, which is helping to create policies around Digital Trust for bodies such as the EU.