HFS Hot Vendor:
Xage Security

Coverage initiated: Q3 2019

Introduction

The HFS Hot Vendors are an exclusive group of emerging players, each with a differentiated value proposition for the HFS OneOffice or HFS OneEcosystem. HFS analysts speak with numerous exciting startups and emerging players.

We designate a select group as HFS Hot Vendors based on their offerings' distinctiveness, ecosystem robustness, client impact, financial position, and the impact in our OneOffice and/or OneEcosystem Frameworks. The HFS Hot Vendors may not (at the time of writing) have the scale and size to be featured in our Top 10 reports, but they have the vision and strategy to impact and disrupt the market.

Xage Security

Q3 2019

Author: Josh Matthews

As the internet of things (IoT) expands, it simultaneously becomes a bigger target for cybercriminals. HFS has previously called on enterprises to ingrain cybersecurity in IoT projects before regulation comes down hard or innovation comes to a complete halt. Security executives and their providers' solutions face a growing disparity; they must defend entire device networks, whereas attackers must only find one weakness, however small, to access and propagate an entire ecosystem.

Xage Security has turned the IoT's weakness into a cybersecurity strength with its overarching "blockchain fabric," operating at the edge and helping to connect the IoT edge with the cloud. More devices in a network create a more secure network, not less. Clients like GE, Saudi Aramco, and the US Department of Energy (DOE) are already on board with Xage's solution. Blockchain's "51% rule" comes into play; in order to compromise a network, one must gain control of over 50% of its devices at once—a somewhat impossible challenge across massive, distributed industrial IoT (IIoT) networks. HFS has discussed a similar principle regarding the security of 3D printing in manufacturing.

Xage differentiates through its overarching "blockchain fabric," which operates at the edge of IoT networks with no inline dependency on remote IT resources like many traditional security solutions have. Xage's innovative use of blockchain enables operation across multiple connected edge, core, and cloud operations. Entire networks can thereby be protected, even ones that include many legacy devices (as most IIoT networks do), including many devices that don't even have simple password protection.

Xage's customers are aiming to improve managed access, increase automation, and enable data sharing across the IoT while also strengthening the cybersecurity of their ever-more connected operations.

HFS' take

For enterprises to be IIoT pioneers—especially if their networks have mixtures of new and legacy devices spread across a large physical distance—Xage's novel blockchain solution could hold a strong value proposition. Its edge security solution affords hackers not a single access point, versus traditional security operating at a network's core where malicious attacks may target legacy or far-removed devices to then propagate to the core operation.

While many firms find security difficult to quantify in terms of value and ROI, the risks are clear to see. A cyberattack on Norsk Hydro's aluminum manufacturing operations cost the firm an estimated $52 million in Q1 of 2019. A Xage oil and gas (O&G) client also hailed its newfound ability to build a strong marketing campaign around security innovation, speaking engagements, investments, and more.

Xage's fabric works across a wide variety of verticals and end devices. Competitors might have features protecting new, digitally-native equipment, but not for "hybrid" installation. In industrial settings, no two machines are alike—oil drilling, wells, and fields, for example—industrial processes are modified, integrated, and specialized over long lifecycles. Integrating and securing IIoT devices and data is the "heavy lifting" underpinning the innovative use cases that make up many modern marketing campaigns.

Company overview and funding

Xage Security was founded in 2016 in Palo Alto, CA, by Roman Arutyunov and Susanto Irwan, to build a "distributed, flexible, and adaptive security framework for industrial cybersecurity." Headquartered in Palo Alto, California, Xage has additional offices in Houston, Texas; Cleveland, Ohio; and Tokyo, Japan. The company was awarded a grant from the US Department of Energy in May 2019 for its blockchain-protected security fabric for infrastructure protection. To date, Xage has seven patents issued, with an additional seven pending. Xage is privately held and completed a $17 million Series A fundraising round in 2018. Among its key investors were General Electric (GE), Saudi Aramco, The Hive, Interdigital, City Light Capital, and March Capital Partners.

Product overview

Since publicly launching its software in December 2017, Xage has released several product updates, including the first tamper-proofing system for IIoT deployments, used in an industry-specific Xage For Energy offering (May 2018); Xage Policy Manager (August 2018), a capability enabling the automated replication of security policies across devices, applications, and users; and Xage Enforcement Point (February 2019), which delivers universal access control for industrial operations, extending protection to millions of previously exposed devices and control systems—many of which were the very definition of "legacy" and lacked any level of previous security.

Clients

Xage's products are in use by more than 1,000 companies worldwide, spanning major global industries such as oil and gas, utilities, manufacturing, and telecommunications, including GE Renewables, Saudi Aramco, NTT Communications, Sensus, GlobaLogix, Commonwealth Edison, ABB, and Itron.

Partnerships

- **GlobalSign:** Public key infrastructure (PKI)-based solution that supports Xage's device discovery process, identity management, and device authentication and authorization
- **Dell:** The Xage Security Suite creates an adaptive blockchain-secured IIoT communication fabric for cooperation, management, and data exchange among devices, applications, and people
- **Schlumberger:** Provides a tamper-proof fabric protecting machines, apps, and data, for identity management and access control in oil and gas operations from edge-edge, edge-center, and edge-cloud
- **Globalogix:** Delivering Xage identity-based access control, remote access, and data security solutions across upstream, midstream, and downstream oil and gas operations
- **Xage** has secured additional as yet unannounced partnerships with major electrical-utility vendors, industrial automation vendors, and system integrator

HFS

About HFS

Insight. Inspiration. Impact.

HFS is a unique analyst organization that combines deep visionary expertise with rapid demand side analysis of the Global 2000. Its outlook for the future is admired across the global technology and business operations industries.

Its analysts are respected for their no-nonsense insights based on demand side data and engagements with industry practioners.

HFS Research introduced the world to terms such as "RPA" (Robotic Process Automation) in 2012 and more recently, the HFS OneOffice™. The HFS mission is to provide visionary insight into the major innovations impacting business operations such as Automation, Artificial Intelligence, Blockchain, Internet of Things, Digital Business Models and Smart Analytics.

Read more about HFS and our initiatives on:
www.hfsresearch.com or follow
@HFSResearch