451 Research® Now a Part of S&P Global Market Intelligence | Business Impact Brief

Taking on IIoT with Secure Networking

The 451 Take

The world of industrial IoT (IIoT) faces significant security challenges. There is a pressing need for secure connectivity in a world where the devices and infrastructure supporting them are ill-equipped to deliver it. The need to move data and manage systems across expanding landscapes has outpaced techniques such as VPNs and firewalls. Organizations that are looking to fully leverage the potential of their IoT environments must seek out more modern techniques that can handle the demands of operational technology environments and provide the security and scale to deliver rugged network connectivity.

Security and Deployment Hold Back IoT

Source: 451 Research's Voice of the Enterprise: Internet of Things, Budgets & Outlook 2019

Q: Which of the following are inhibitors to IoT initiatives at your organization? Select all that apply.

Base: All respondents (n=515)

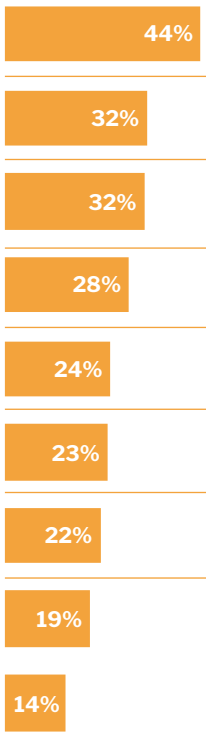
WHAT'S THE CHALLENGE?

IT challenges – **security worries and technology deployment challenges** – rank as the largest barriers to IoT deployment.

Enterprises deploying IoT are challenged to find **budget** and are uncertain that IoT will deliver a strong **return on investment.**

Skills concerns and shortages have become less of a sticking point as IT pros pick up IoT and supporting infrastructure skills.

It is very good news for the present – and future – of IoT that **corporate resistance** ranks dead last in IoT inhibitors.



INHIBITORS BY INDUSTRY

60% of **finance** respondents cite security as a challenge.

Budget is an inhibitor for 51% of **government** respondents

Integration challenges 40% of **utility** respondents.

26% of **manufacturers** cite a lack of in-house IoT skills.

30% of **healthcare** respondents lack demand for insights.

The world of IoT holds tremendous promise, but it also makes significant demands for connectivity that can challenge the abilities of traditional approaches to security. The need for connectivity is driven both by the requirement for more timely control and interaction with a diverse and distributed set of systems and the much larger volumes of data that they produce. The challenges that IIoT presents are threefold: connectivity across a range of environments, robust security requirements and the ability to operate reliably at scale. These have to be accomplished in a world where the sophistication of attackers and their techniques are increasing at a rate that's almost as high as that at which IIoT devices are proliferating. The additional demand for reliability is clear because the nature of many industrial applications is safety and often life-critical.

The 451 Take (continued)

To address these needs, any successful approach must operate with flexibility and simplicity while maintaining industrial-grade security. Traditional approaches for connectivity can be managed securely, but they can't be managed efficiently at scale. At the same time, the information security world continues to face chronic shortages of skilled practitioners, further increasing the need for any option to be resource-efficient. Traditional VPN or firewall-based approaches fail on both counts. Acceptable approaches have to handle high scale with juditious use of precious security staff.

IIoT connectivity approaches also need flexible deployment options. Integration into software or hardware would be ideal, but it is simply impossible in many situations with existing equipment or closed systems. They have to be able to address the needs of installed equipment that can't be modified. That means that in addition to software or agent-based capabilities, they'll also need to have gateway deployment options to securely link networks that were often protected by air gaps. Access to a variety of deployment options would allow implementors to effectively address the full range of situations.

While it may seem challenging, there are important benefits to getting IoT and IIoT connectivity right beyond the basic gain of making data and control flow well. With effective security in place, critical assets can be managed while being shielded from attack with technologies like identity-based protocols rather than the more open address-based protocols. Security protections should also reduce the attack surface, limiting the number of options attackers have for launching attacks. Limiting lateral movement within the network, with micro-segmentation, is vital. This is a benefit that has outsized rewards because it also allows protections and controls to be focused on a smaller set of possibilities, improving security scalability.

Business Impact

IMPROVED SECURITY – Purpose-built IoT security technologies go far beyond traditional approaches and can address the specialized requirements of of securing IoT environments at scale.

AGILITY – Breaking free of the constraints of firewalls and VPN architectures enables greater agility. Multiple deployment options allow adaptation to varied environments.

SECURITY AT SCALE – Traditional security approaches struggle with the scale of IoT deployments. IoT-focused approaches can deliver the scale, and security, needed.

OPERATIONAL SIMPLICITY – Effective network security approaches can simplify the operations of IoT environments by consolidating policy controls and streamlining security operations.

Looking Ahead

The future of the connected world is already being tied to advantages that IoT has the potential to deliver. The key to realizing this future is the ability to build secure and connected environments in which IoT's potential can flourish. We're just starting to see the transformative potential of 5G connectivity and feel out new use cases. The power of IoT coupled with 5G will push into ever more remote and challenging environments, and businesses need to make the investments today that will enable growth later. Those investments will reach endpoints that have great value but even greater risks in communications and attack. Attackers and techniques will gain sophistication, requiring improved defenses. To be successful, organizations have to put more sophisticated communications infrastructure in place that is ready for the scale and ruggedness the future of IoT demands.