Enterprise Strategy Group™ by TechTarget

WHITE PAPER

SD-WAN for IoT

Securing Devices in Branch

By Bob Laliberte, Principal Analyst
Enterprise Strategy Group

April 2023

Contents

Abstract

Organizations continue to digitally transform and gain business advantages by leveraging data generated at the edge. IoT initiatives and deployments are gaining traction to ensure critical processes are monitored and the requisite data is collected. However, organizations also need to be aware of the risks associated with deploying and scaling IoT environments, including a lack of visibility, inherent vulnerabilities, and the need to apply the appropriate security policies for all devices. Palo Alto Networks introduces the industry's first SD-WAN with integrated IoT security. This recent Prisma SD-WAN innovation ensures streamlined end-to-end visibility and the ability to collect and transport data securely over the WAN. It also provides tightly integrated security policies for IoT devices in branch environments.

Organizations Gain Business Insights from the Edge

Organizations must adapt to succeed in a modern, global economy. To do so, organizations are embarking on and maturing digital transformation initiatives. According to TechTarget's Enterprise Strategy Group (ESG) research, over three-quarters (77%) of organizations are either in the process of implementing or have already implemented several digital transformation initiatives.[1] And while these transformation initiatives include people, processes, and technology, organizations require modern and innovative technologies to underpin or enable new processes and workforces. The shift to cloud-native applications distributed across data centers, multiple public clouds, and edge locations drives agility and business benefits but also increases IT complexity.

For that reason, it shouldn't be a surprise that, for IT decision-makers, the top goals of transformation include becoming more operationally efficient (54%), developing new data-centric products and services (47%), and providing better and more differentiated customer experiences (45%). Operational teams need to leverage new technology solutions that enable them to manage a highly distributed and complex environment more efficiently. It is worth noting that this has been the goal most cited by ESG research respondents for the last five years. In addition, as organizations deploy more sensors, cameras, and IoT devices, it is imperative that the business is able to monetize that information. Lastly, in an "always on" environment with ample competition, delivering positive customer experiences has become a competitive differentiator.

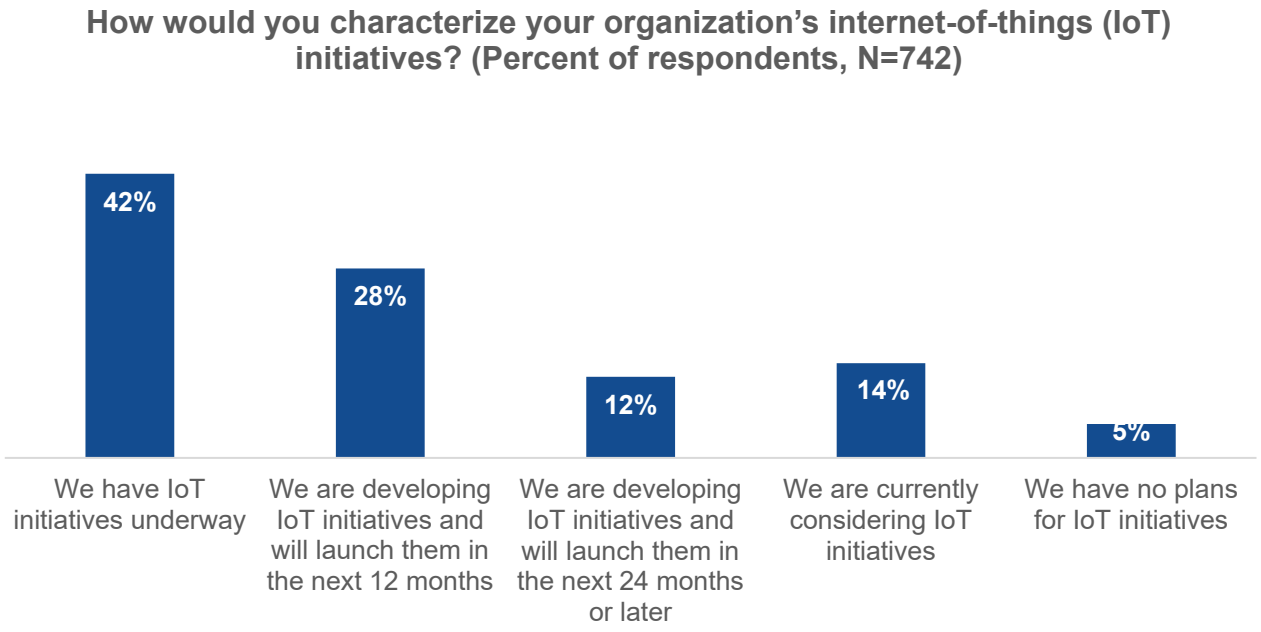
These goals are subject to change based on industry. For example, healthcare industries have repeatedly cited that a better and more differentiated customer experience is their top priority for digital transformation efforts. Those in retail are more focused on developing new data-centric products and services to engage customers, and in finance the focus shifts back to improving customer experience as well. These industries also tend to have a lot of remote or regional locations that are required for servicing their customers. Increasingly, organizations are deploying IoT devices to ensure better experiences, improve a process or workflow, or get better insights into their business. Examples across these industries include the use of IoT devices to support digital signage or location-based services (e.g., customer proximity, medical devices, or autonomous robots), as well as to support facility or sustainability initiatives related to reducing power, cooling, and lighting costs.

IoT deployments are only expected to grow as well. ESG research shows that over nine out of ten respondents have IoT initiatives underway, will launch them over the next 24 months, or are considering them. Currently, 42% of organizations already have IoT deployment underway (see Figure 1), with those in the financial and retail industries besting that average (48% and 47%, respectively). Healthcare organizations are close behind, with 39% claiming IoT deployments are underway. Moving forward, another 40% of organizations believe they will launch IoT deployments in the next 12-24 months. Once again, financial and retail are on target with the

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022. All Enterprise Strategy Group Research References and Charts in this white paper are from this report unless otherwise noted.

overall group at 40% and 39%, respectively, and healthcare comes in at 32%. It should be noted that the healthcare verticals often have to be more careful in their use of technology due to compliance and regulations, as well as ensuring there is no impact to essential services.

Figure 1. Growth of IoT Initiatives



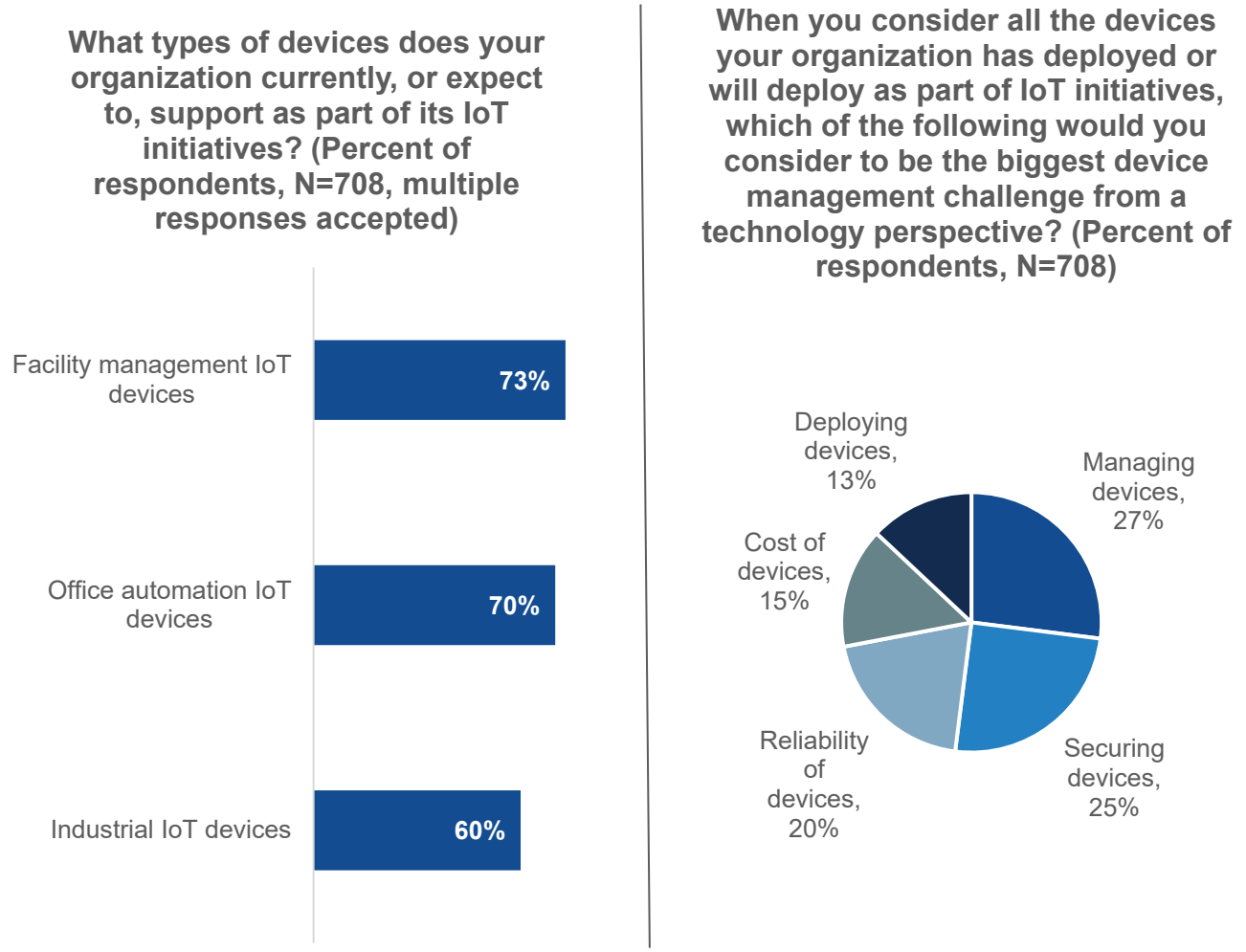
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

IoT Device Types and Challenges

While IoT devices can bring a number of benefits to organizations across all industries, it is important to understand how the IoT device will be used and the potential challenges and risks associated with them.

First organizations need to decide where the devices will be deployed and for what purpose. Enterprise Strategy Group (ESG) research highlights that organizations deploy a diverse array of IoT devices that span facility management, office automation, and industrial use cases (see Figure 2). Given the overlap, it is clear that many organizations are deploying devices to satisfy all these use cases. From an industry-specific perspective, organizations in the retail space lead in facility management, with 86% reporting they have deployed devices in that capacity, followed by financial (79%) and healthcare (57%). The next use case, office automation, finds financial organizations adopting at a higher rate (81%), just slightly surpassing retail at 80% and healthcare at 59%. Not surprisingly, in the industrial IoT deployments, 70% of retail organizations—with their need for warehouses, as well as transportation and logistical requirements—lead finance (58%) and healthcare (57%) industries.

Figure 2. IoT Device Types and Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 2 also highlights some of the challenges associated with deploying IoT devices. While organizations cite challenges related to the cost, deployment, and reliability, the top two challenges are related to managing and securing IoT devices. Indeed, security is very important for healthcare, where an attack could threaten human life and not just personal data. This is indicative of the slower adoption rate by healthcare and the almost doubled response to security as a challenge (47% versus 23% for all other industries). Financial and retail organizations were in line with the overall response, at 27% and 25%, respectively. So why is managing and securing IoT devices so challenging? There are a number of reasons, including:

- **Lack of visibility:** It is a well-known axiom that you can't manage what you can't see. Operations teams require visibility into all the devices connected to the network in order to properly manage them. We have seen that even something as simple as a fish tank thermometer could be used to breach a company's network, and the Target breach occurred via an HVAC device.
- **IoT devices are inherently insecure:** Typically, IoT devices are not regulated and often use nonstandard operational systems, which may not be patched nor updated on a regular basis. Another factor to consider are potential supply chain vulnerabilities. Is your organization auditing the components in the IoT devices to ensure

there are no “built-in” vulnerabilities? Depending on how these devices are acquired and deployed by IT, facilities, or even operational technology (OT) staff, they may not have the proper network segmentation or appropriate level of security.

- **Security issues are exacerbated by lack of skilled security resources:** ESG research highlights that security continues to be the top area of skills shortage, with almost half of the respondents (45%) citing it as problematic.[7] This challenge is compounded by the fact that many IoT devices are deployed in remote or edge locations.
- **Increased complexity due to deploying devices at the edge:** With over half (53%) of the respondents to our technology spending intentions survey claiming their IT environment is more or significantly more complex than two years ago, we asked what was driving that complexity. The number two most selected response was an increase in number and types of endpoint devices.[8]
- **Multiple collection and management devices:** Early IoT deployments have required separate collection management or security appliances to be deployed in order to secure or manage IoT environments. This creates room for errors, as operations teams need to employ manual, "swivel chair" management to correlate data. There is also the possibility of increasing risk and impacting experience with each additional tool the data traverses. Plus, there are additional costs (e.g., power, cooling, maintenance, etc.) associated with more devices at the edge.
- **Backhauling all traffic to a corporate data center:** Typically, the data generated by these IoT devices at the edge will be sent to a centralized location for additional processing or historical analysis. However, often this data is unencrypted and susceptible to being intercepted.
- **Lack of segmentation of IoT devices:** Often, IoT devices are connected to the same corporate network that hosts business-critical or personally identifiable information. This creates substantial risk for a business, as any successful attack on an IoT device also provides access to everything on the corporate network. Organizations need to consider the appropriate level of segmentation or microsegmentation to ensure continued operations in the event of devices being hacked.

Prioritizing for IoT

Given the growing adoption of IoT devices and the number of challenges managing and securing them, organizations need to ensure they are taking steps to overcome obstacles and provide the appropriate levels of visibility and security in their IoT environment.

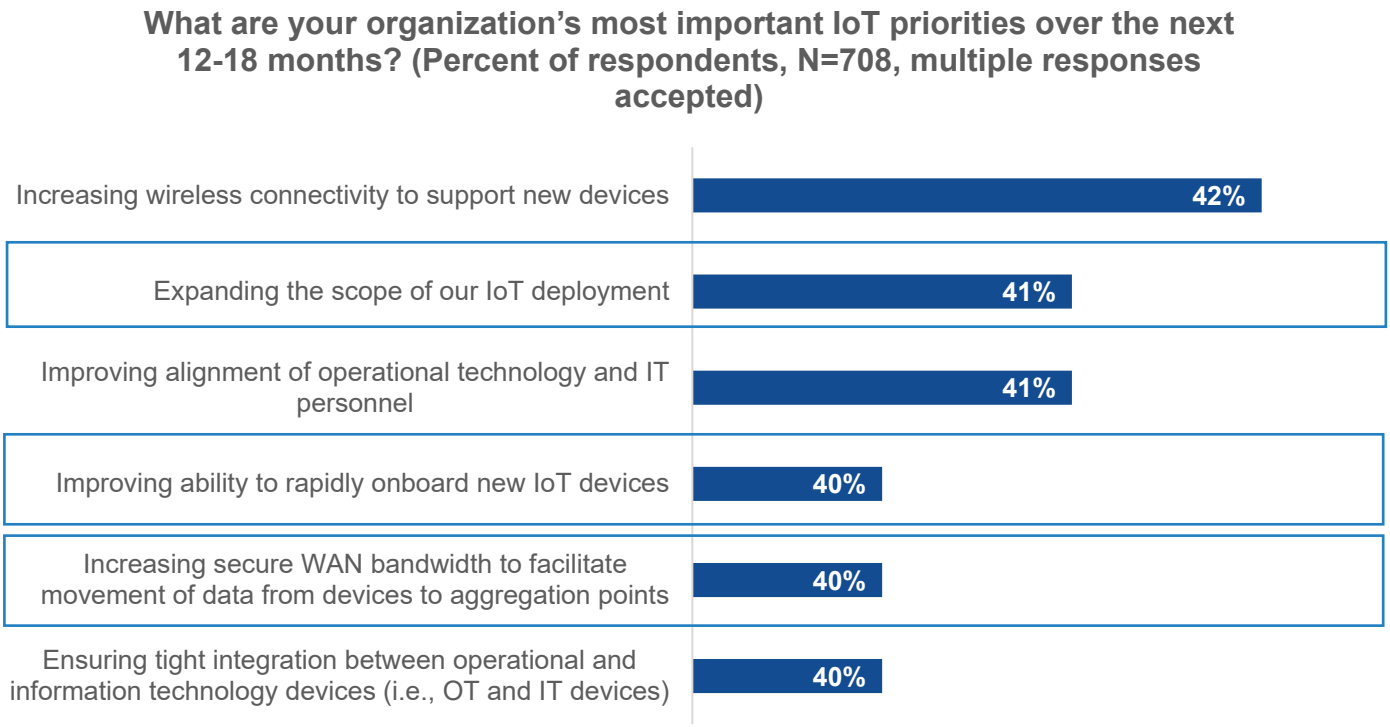
In particular, organizations need to focus on prioritizing the following objectives:

- **Ensure complete visibility into all IoT devices:** IoT initiatives and deployment are rapidly gaining momentum. In fact, 41% of organizations cited expanding the scope of IoT deployment as their top IoT priority over the next 12-18 months (see Figure 3), so the ability to identify existing and any new devices will be required. Operations teams need to be able to quickly identify all devices on the network. Especially with a majority (58%) of organizations reporting that they have 1,000 or more IoT devices deployed worldwide,[2] the ability to have end-to-end visibility will be crucial for finding vulnerabilities.
- **Rapidly onboard new devices:** This is another top five IoT priority, cited by 40% of surveyed organizations. While visibility is a big first step, so is being able to apply the appropriate policies, including who has access to these devices. Also, the ability to do this from a centralized, cloud-based console will enable organizations to accelerate deployments in remote locations. The ability to rapidly onboard new devices is even more important for financial organizations (cited by 48%).

[2] Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Digital Ecosystems*, August 2022.

- **Ensure secure WAN bandwidth:** Also a top five priority (40%), this is important as organizations will need to transport all the data that is generated and potentially analyzed at the remote site to a centralized data lake or ocean. It will be critical to ensure that the data is kept secure in transit. Organizations in retail (49%) and healthcare (45%) industries were more likely to prioritize this requirement.

Figure 3. Top 6 IoT Priorities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

- **Apply security policies consistently and correctly:** In highly distributed IoT deployments, operations teams must be able to ensure that security policies are enforced at the edge in the same way for every device or device type. Organizations need to focus on leveraging zero-trust models to ensure policy enforcement. This could include tightly integrated Secure Access Service Edge (SASE) solutions, which leverage zero-trust network access (ZTNA), as well.
- **Streamline data collection and security:** Organizations require solutions that remove complexity and streamline the collection and secure movement of IoT data. By reducing the number of devices required in the end-to-end process, organizations can regain control and drive operational efficiency into a rapidly growing, highly distributed and complex IoT environment. This process also includes leveraging automation when possible.

Palo Alto Networks Prisma SD-WAN with Integrated IoT Security

Palo Alto Networks has been bringing innovative security and network solutions to market for almost two decades. From its next-generation firewalls to its single-vendor Prisma SASE solution, it has enabled organizations to remain agile and accelerate transformations while also mitigating risk, driving operational efficiencies, and delivering enhanced experiences.

Palo Alto Networks invested in SD-WAN several years ago and continues to differentiate itself with next-generation capabilities. Specifically, Prisma SD-WAN—an integral part of the Prisma SASE solution—provides an industry-first integrated IoT visibility and security solution for branch or edge locations. By delivering this capability, Palo Alto Networks customers can streamline their remote IoT environments, drive operational efficiencies, and mitigate risk.

The Palo Alto Networks Prisma SD-WAN with integrated IoT security provides:

- **Comprehensive end-to-end visibility into IoT environments at branch or edge locations:** Organizations can leverage existing Prisma SD-WAN deployments and footprint to gain visibility into existing and planned IoT deployments at remote sites. The ability to "see" all IoT devices limits vulnerability and risk.
- **A centralized cloud management console:** This enables organizations to leverage a centralized zero-trust model with policy enforcement for IoT devices at branch locations.
- **Secure WAN connectivity:** This offers the ability to encrypt all IoT and other traffic from the branch office to aggregation points in data centers or public clouds.
- **Optimized security policies:** Based on the type of device discovered, organizations can enforce customized security policies for each IoT device and leverage the intelligence. This will enable organizations to roll out a new IoT environment in less time and with less risk. IoT devices are discovered, and the optimal security policy is automatically applied.

The Palo Alto Networks Prisma solutions are focused on delivering three key business outcomes:

1. **Enhanced user experiences:** Leveraging Prisma SD-WAN's application focus, operations teams can ensure real-time application performance service-level agreements (SLAs), with Palo Alto Networks claiming as much as a 10x improvement in performance and, hence, enhanced end-user experiences.
2. **Simplified operations:** Organizations with existing or rapidly expanding IoT deployments can now automatically identify all IoT devices at branch locations, without additional appliances or tools. This reduces cost and complexity at locations that lack skilled IT resources.
3. **Improved security:** Highly distributed environments increase the attack surface for bad actors as well as risk. Prisma SASE extends zero-trust security models to branch locations and IoT devices, providing the ability to create centralized policies for IoT device types and apply them automatically to minimize risk.

Conclusion

Organizations continue to digitally transform in order to compete in a global economy. To succeed, they need to deliver differentiated customer experiences, operate in highly distributed IT environments with greater operational efficiency, and effectively leverage the data generated at remote and branch locations more effectively.

Organizations have responded by deploying applications across public clouds and edge locations, as well as accelerating their use of IoT devices to improve processes, deliver better experiences, and operate more effectively. And while the data generated from these expanding IoT deployments can bring significant benefits, organizations must be aware of the challenges and increased risk associated with them. This is especially true for the financial, retail, and healthcare industries.

End-to-end visibility is a must-have capability for IoT deployments, and operations teams need appropriate IoT security policies in place for facilities, office automation, and industrial environments to ensure optimized protection and leverage zero-trust architectures.

Palo Alto Networks Prisma SD-WAN delivers the requisite end-to-end visibility and security to enable robust IoT environments in branch locations.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com