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

Securing the Enterprise in the Age of IoT

The 451 Take

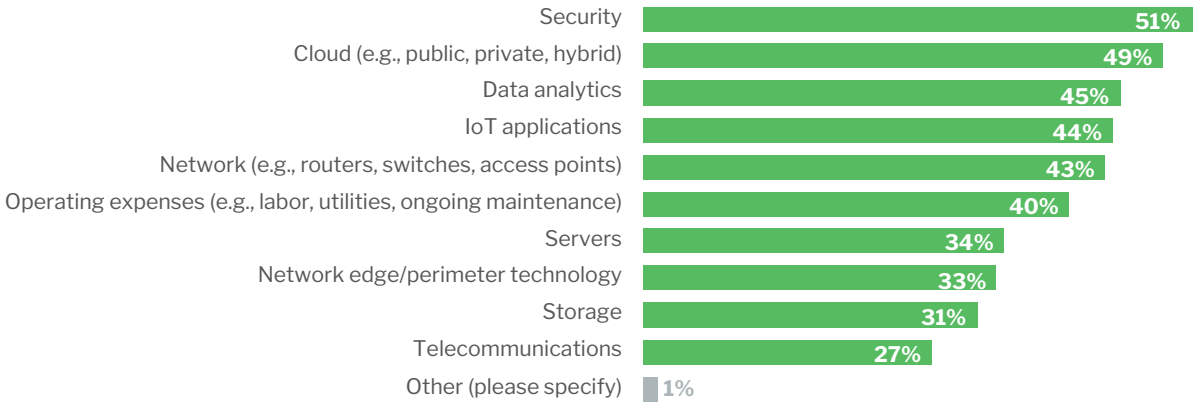
The Internet of Things (IoT) increases operational efficiencies and helps target customers for new products and services, but it also leaves organizations vulnerable to security risks. While enterprises recognize the inherent business benefits of IoT as key drivers for adoption, they also recognize the considerable challenges in securing their connected IoT environments. The sheer increase in the number of IoT devices presents a much larger attack surface, and the diversity of IoT devices complicates vulnerability management and often introduces new vulnerabilities. Older IoT and operational technology (OT) devices are often compute-constrained, run outdated operating systems, are susceptible to older malware, and difficult if not impossible to patch or upgrade. All of these factors can contribute to a general decline in security posture.

Nearly all sectors have IoT projects that call for embedding a variety of IoT endpoints into their network infrastructure. The IoT endpoints range from robust compute devices to OT equipment with limited embedded computation that monitors and controls systems and processes. Unprecedented interest in IoT adoption paired with the convergence of IT and OT processes is a major driver of industry business transformation. Far from aspirational, IoT is already in use by 46% of respondents to a recent 451 Research survey, with a further 23% of respondents in proof of concept with IoT projects and an additional 18% planning to deploy in the next two years.

IoT Budget Spending by Category

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

Q: Thinking about your organization's 2020 IoT spending plans, in which of the following categories will IoT budget dollars be spent? Please select all that apply. (n = 444)



Business Impact

PERIMETER SECURITY LEADS CONCERNS AND PURCHASE INTENT. The majority of respondents to 451 Research's survey said that they plan to purchase IoT security devices to provide protection from network threats, leveraging policy controls to limit network resource access to and from those IoT devices.

IoT DEVICES ARE ATTRACTIVE TARGETS FOR ATTACKERS. IoT devices come in many forms, from compute-constrained thermostats and security cameras to large factory equipment. Many are developed without any governing standards or information security best design principles, and these devices monitor and control critical infrastructure including power plants and life-supporting medical devices. They may have access to core production networks and other devices, and may capture proprietary production, control or health data that may be subject to regulatory restrictions. Compromising any of these devices not only exposes this sensitive data to bad actors, but also provides a potential stepping-stone for lateral compromise of other connected devices and systems.

Business Impact (continued)

THE DIVERSITY OF IoT DEVICES CHALLENGES EFFECTIVE GOVERNANCE. While some IoT use cases, such as vehicles, are relatively new and use over-the-air updates and security patches, the majority of IoT devices have inconsistent software updates or patching behaviors. Their proprietary or unsupported operating systems and insufficient onboard compute may lack the ability to support an endpoint agent. Even the newer IoT devices may lack standards for control over OS hardening and are largely unregulated. Patch management and updates are inconsistent, and systems may not be well supported by IT, security management tools or the vendor that created them.

IoT DEVICES ARE INCONSISTENT. IoT endpoints have emerged across a variety of industries and use cases, and there is inconsistent implementation of device authentication. For example, in a mixed-vendor deployment of security cameras, each vendor may have its own mechanism to secure (or not) the camera, making it difficult to enforce a consistent security policy across all cameras. This exposes organizations to risk of unauthorized access to sensitive operational environments and the critical information they handle. It may further expose organizations to compromise by exploits and provide a back door into enterprise networks.

IoT SECURITY IMPLEMENTATION SHOULD BE CONSISTENT. Threat detection technologies include behavioral and signature-based approaches. Organizations should consider tools that identify a large array of devices, and they need systems that can help identify where security updates and patches are needed and deploy updates without interfering with critical functionality or availability. Ideally, approaches should incorporate threat protection and enforcement of security policies that integrate well with the organization's existing security practices. Most security teams face constraints with availability of personnel or relevant expertise. Security support for the IoT environment may, therefore, be more successful if it integrates seamlessly with daily operations and is interoperable with existing security teams and technology. This can help eliminate fragmented security for IoT, reduce the burden of changing operational processes and additional training on new products for an already overworked team, and help to improve the organization's risk posture through consistent implementation.

Looking Ahead

As industries digitalize, a deluge of data will be produced from a diverse collection of newly connected equipment. Organizations need to build their transformation efforts on a firm foundation of systemic, pervasive security. This begins at the endpoint, the device generating the data itself, and moves onward from there to all points where the data is analyzed and archived, and controls are managed leveraging this insight. The traditional agent-based security approach does not work well for many OT and IoT devices. These devices need an agentless approach that supports device discovery and full visibility into IoT device traffic for real-time risk mitigation. The network is the common denominator in this equation and can be used as a vehicle to help ensure that critical functionality and data are consistently and reliably protected from cyber risk exposures. Management of IoT security should be a part of network security practices, segmentation policies and enforcement controls that exist today, and to do that, organizations must expand capability but not operational overhead. Ultimately, manufacturers that create new IoT devices should be expected to recognize the increased risk of cyberthreats in this realm and introduce stronger security measures, creating a condition across all industries that elevates the standards of privacy and security throughout the IoT landscape.