451 Research

S&P Global
Market Intelligence **Business Impact Brief**

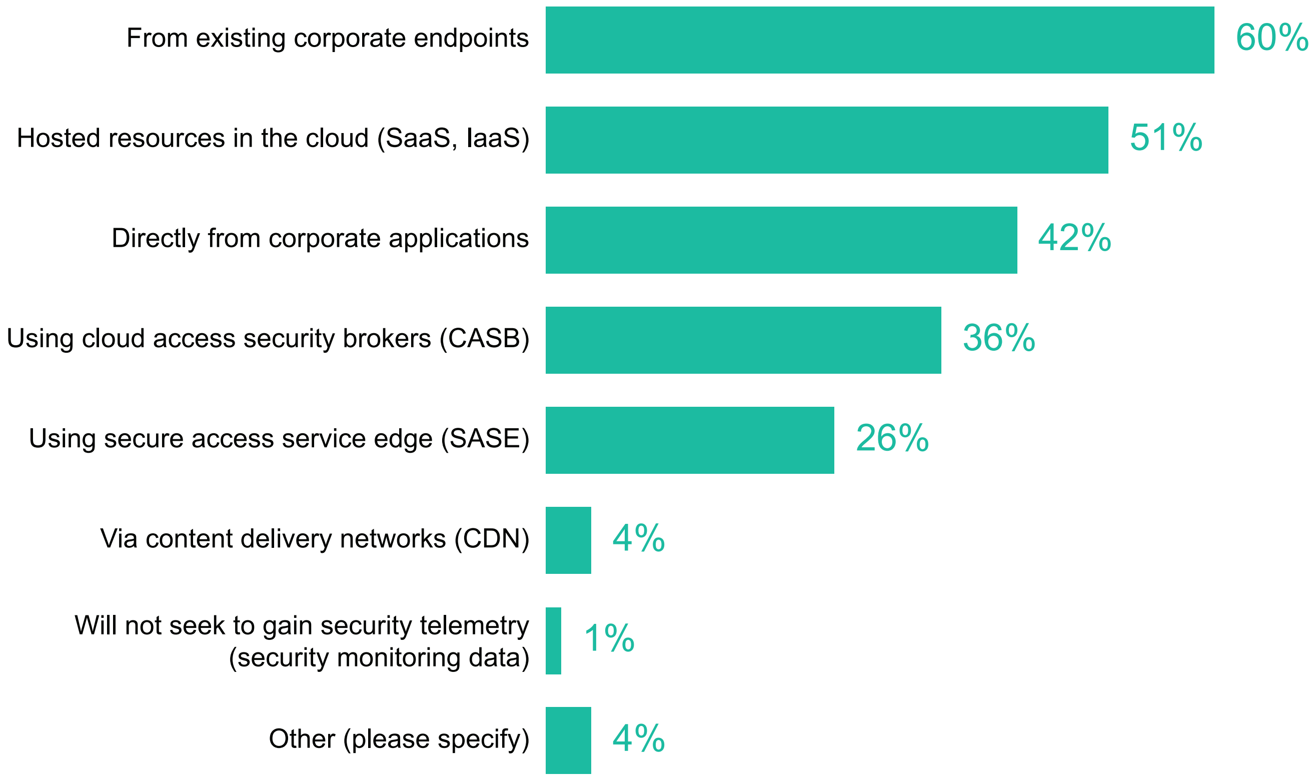
Asset Visibility Key in Distributed IT and Further Growth of IoT

The 451 Take

In many ways, the Internet of Things (IoT) has been a driving technology for many companies to overcome the challenges of the pandemic and ensure business continuity. As the world went into lockdown, instrumented equipment and connected devices allowed remote operations. For many companies, IoT has been a blessing and helped accelerate their digital transformation. At the same time, the surge in work-from-home (WFH) initiatives with the accompanying hike in remote access dramatically increased complexity for security teams as it expanded the attack surface and added to the existing challenge of full asset visibility in a hybrid world.

Asset visibility across the entire organization has become a top security pain point as we move from stationary IT to distributed technology. The centralized IT infrastructure has gradually dispersed through mobile devices and was augmented by bring-your-own-device (BYOD) policies. Many companies expect WFH initiatives will increase and be extended for a long time as a lingering effect of the COVID-19 pandemic. As such, the number of assets that need to be monitored and managed outside the office will increase.

The Fragmented Landscape of Security Telemetry



Q: If remote working becomes permanent, how you will your organization seek to gain security telemetry (security monitoring data)? Please select all that apply.
Base: Respondents whose organization is experiencing a loss of security telemetry as more employees work from home during the COVID-19 outbreak (n=73)

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Although the number of IT assets operated outside the office infrastructure will grow, they still operate in relatively similar context, unlike the IoT devices, which operate in myriad environments. Meanwhile, security teams are trying to keep track of all these devices and gather telemetry from endpoints, cloud access brokers, secure access service edge and content delivery networks. In the fragmented security landscape, this often means a variety of tools from different vendors.

In this fragmented landscape, full asset visibility is paramount to take appropriate action. One can only protect the visible assets, and the invisible assets are areas of exposure. More importantly, security teams need to be able to rationalize and consolidate the security telemetry. Often, vulnerabilities are known to application managers, but in a consolidated view, they provide context and uncover potential attack routes.

Business Impact

Unknown or unclear asset inventory means no realistic estimate of exposure. This means that the business has no real idea how much investment is truly required to mitigate risk. The impact of incidents arising from the exploitation of unknown assets can affect more than the organization itself. The impact on other relying parties – such as partners and customers – can significantly amplify damage.

Visibility across the entire organization becomes increasingly complex. Full asset visibility moves beyond monitoring laptops, mobile devices and IoT sensors. It encompasses the entire digital infrastructure that is spread across a complex and fragmented hybrid world of cloud, on-premises and, increasingly since the pandemic, the remote workplace within employees' homes.

As IoT adoption continues to grow and unmanaged devices are deployed at scale, much effort is put into primary asset discovery to locate these devices. However, secondary asset discovery, or asset information, is equally important for an accurate vulnerability assessment. Secondary assets include all network infrastructure such as cables, routers, cooling systems and servers, but also the firmware, antivirus version, VMs and other agents running on the primary assets. The asset inventory must be dynamic as well as comprehensive. If an inventory cannot be kept reasonably current, then yesterday's estimate of exposure may bear little resemblance to today's reality.

Asset visibility is important to map the organizational threat landscape but can also bring short-term benefits in cost saving on licenses and application rationalization. Moreover, security teams will benefit from a unified view as asset information is fragmented across a variety of tools that often only provide partial insight.

Looking Ahead

In the converging IT and operational technology (OT) environments, many security vendors have made an effort to discover a wide range of OT assets such as industrial supervisory control and data acquisition (SCADA) systems and programmable logic controllers, but as cyberattacks grow more sophisticated, it is often the lack of visibility of secondary assets on managed devices that is the primary concern of CISOs. They often don't know what exactly is running on their network, and they don't have the ability to detect which versions of agents are running on devices, or if the correct user is accessing the device. This is especially true in a WFH scenario in which critical infrastructure is managed from the kitchen table; traditional network access controls fall short, and it becomes paramount to know which secondary assets are installed on the primary managed device.