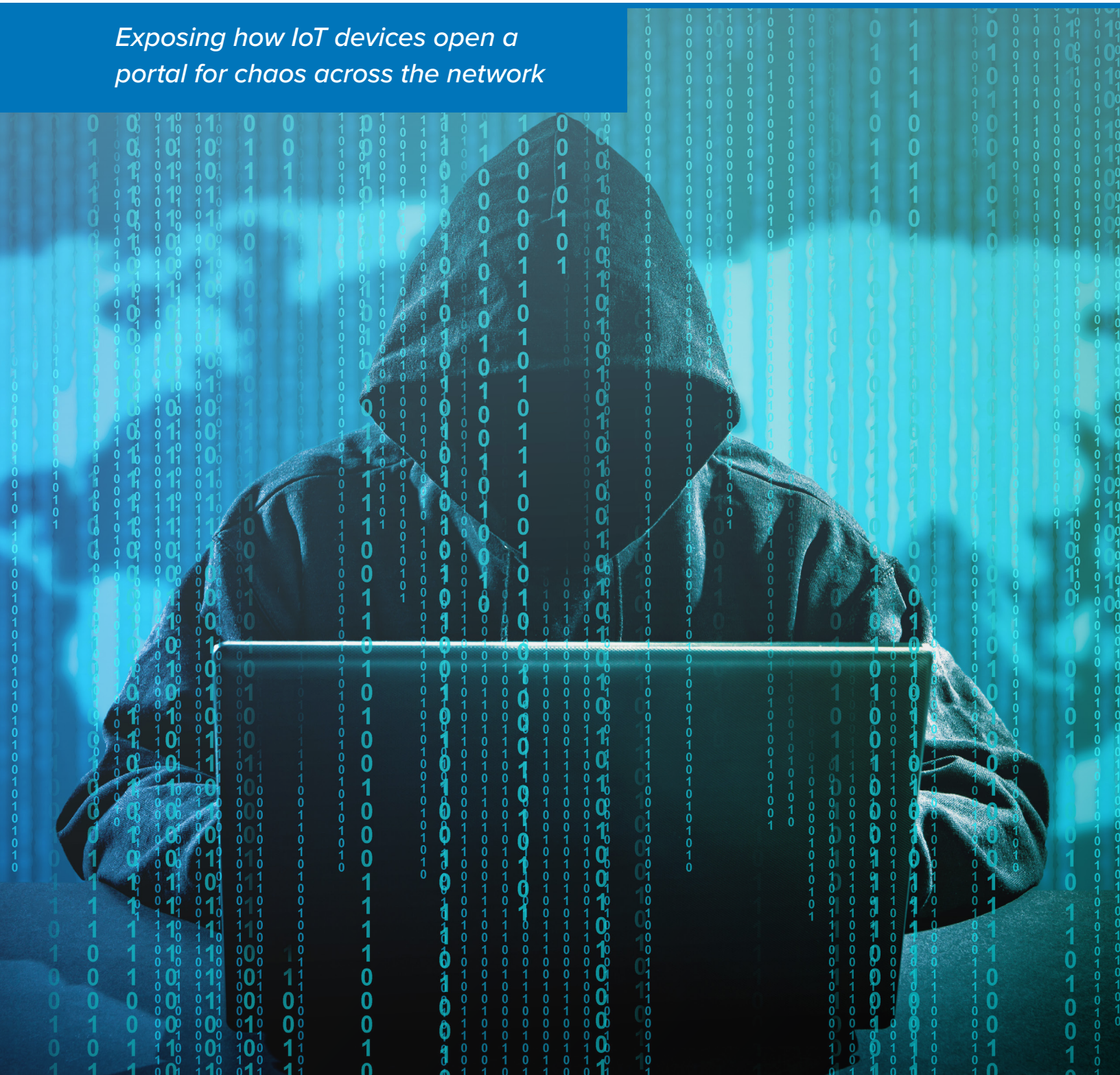
Infoblox
NEXT-LEVEL NETWORKING

REPORT

What's Lurking in the Shadows 2020

Exposing how IoT devices open a portal for chaos across the network



Foreword by Malcom Murphy, technical director, EMEA at Infoblox

"Although awareness of the risk of shadow IoT devices has grown since we started reporting on it, the complexities around managing these unsanctioned IT operations are still a significant stressor for many organizations. While as a whole the industry is making strides, some regions are still far behind others.

"As workforces evolve to include more remote locations and branch offices, and enterprises continue to go through digital transformations, organizations need to focus on protecting their cloud-hosted services the same way they do at their main offices. If not, enterprise IT teams will be left in the dark and will not have visibility over what's lurking on their networks. With limited security in most IoT devices, organizations will continue to be a target for cybercriminals looking for a way to easily exploit the network. Ignoring these precautions will only leave them defenseless against evolving threats and can have a critical impact on their business network."

Overview

Infoblox has commissioned this report to gain a better understanding of the challenges that IT teams face in securely managing shadow IoT devices across enterprise networks. Shadow IoT devices are connected devices or sensors that are in active use within an organization's network environment without IT's knowledge. Shadow IoT devices can be any number of connected technologies, including laptops, mobile phones, tablets, fitness trackers or smart home gadgets like voice assistants, that are managed outside of the IT department.

With extensive insights provided by 2,650 IT professionals across the United States (US), United Kingdom (UK), Germany, Spain, the Netherlands and the United Arab Emirates (UAE), this report investigates the extent to which shadow IoT devices pose a security risk to networks.

This report also provides practical recommendations on how companies can best manage the threat posed by shadow IoT devices.

The Challenge

According to recent research[1] from Strategy Analytics, the number of devices connected to the Internet reached 22 billion worldwide at the end of 2018. It is predicted that almost 40 billion devices will be connected by 2025 and 50 billion by 2030. Though some industries may see a decline in device adoption, the majority of sectors will see consistent growth. This includes the enterprise segment, which is already considered to be the leading sector when it comes to using IoT devices.

Our research shows that the majority of enterprise organizations (78 percent) had more than 1,000 connected devices on their corporate networks in 2019. This number is in line with results from the year prior. In the 2018 Infoblox report, "What Is Lurking on Your Network," over three-quarters of organizations reported having more than 1,000 business devices, such as laptops or tablets supplied or managed by the company, connected to the enterprise network on a typical day.

More than a quarter (28 percent) of respondents reported having 1,000 to 2,000 devices connected, while almost half (48 percent) of organizations have between 2,000 and 10,000. These numbers vary across regions. Over a third of respondents in Spain (34 percent) have 1,000 – 2,000 connected devices on their corporate network. This is compared to only 24 percent in Germany who said the same. In the Netherlands, the prevalence of connected devices is more common than in other parts of the world. Thirty-one percent of Dutch enterprises have between 5,001 and 10,000 connected devices on their corporate network at a time, while fewer than one in seven in the US (13 percent) claim the same.

In addition to devices deployed by the IT team, organizations across the world reported personal devices—such as personal laptops, Kindles, mobile phones and fitness trackers—connecting to their networks. Overall, almost half (48 percent) of all enterprises believe they

1. https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where

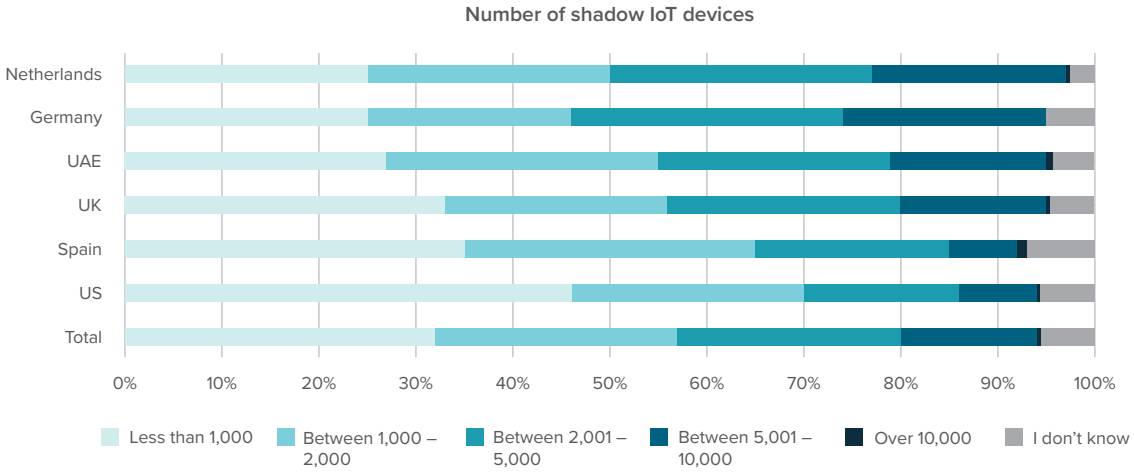


Figure 1: Number of shadow IoT devices connected in each country

have between 1,000 and 5,000 personal IoT devices connected to the network at a time; 14 percent believe that number to be 5,001 or more.

Businesses in the US (46 percent), Spain (35 percent) and the UK (33 percent) all believe that there are less than 1,000 non-business related IoT devices connected to their enterprise networks. That number increases across the other regions as 29 percent of IT leaders in the UAE claim to see between 1,000 and 2,000 such devices, while 27 percent of those in the Netherlands see between 2,001 and 5,000 of them.

The Threat

Over the past 12 months, only 20 percent of IT leaders claimed to have not discovered any shadow IoT devices—such as unauthorized wireless access points—connected to their infrastructure. Unfortunately, this isn't the case for all organizations. Almost half (46 percent) of IT leaders have discovered up to 20 shadow IoT devices on their networks over the past year, and worryingly, more than a quarter (29 percent) of organizations saw more than 20, while some saw as many as 50.

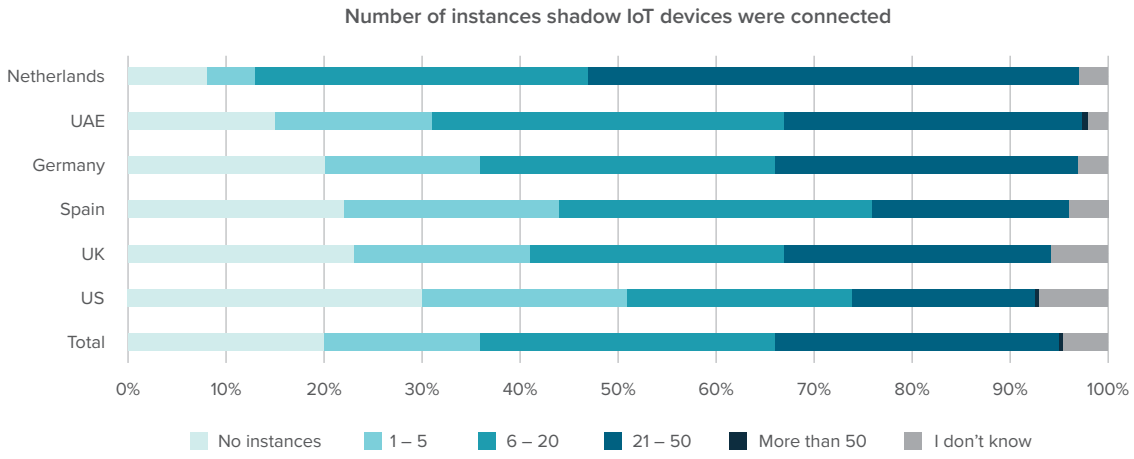


Figure 2: Number of instances shadow IoT devices were connected in each country

Almost a quarter (23 percent) of UK organizations saw zero shadow IoT devices connected to their network, though the majority (43 percent) saw up to 20, and 28 percent saw as many as 50. In the Netherlands, the case was almost the opposite. As a whole, only 8 percent of all Dutch IT leaders did not come across shadow IoT devices on their network, while 40 percent saw up to 20, and half (50 percent) saw up to 50.

While the numbers vary across regions, these practices open up enterprise networks to significant risk of malware and other types of cyberattack. In early 2019, a large-scale botnet attack targeted an online streaming application by using more than 400,000 connected devices over 13 days. Researchers at Imperva noted[2] that the DDoS attack associated with this attack mirrored much of the activity seen in the infamous Mirai botnet, producing almost 300,000 requests per minute.

In April 2019, a similar situation arose involving unnamed Microsoft customers.[3] The attack targeted three specific IoT devices—a printer, a VoIP phone, and a video decoder—using them to gain access to corporate networks. This particular attack was traced to the STRONTIUM hacking group, which security researchers have strongly linked to Russia's GRU military intelligence agency. According to Microsoft, one in five notifications of STRONTIUM activity was tied to attacks against non-governmental organizations, think tanks or politically affiliated organizations around the world. The other 80 percent have largely targeted organizations across sectors, including the military, IT, government, education and engineering fields.

Though these are just two instances of IoT vulnerabilities, they are a prime example of what can go wrong when unsecured devices gain access to networks. So, with billions of new connected devices slated to appear over the next few years, where do we go from here?

Confidence Is Inconsistent

The good news is that most organizations are taking the risk very seriously and as a result have put policies in place to safeguard against external threats. Eighty-nine percent of organizations have a security policy in place for personal IoT devices connected to their network. This figure is slightly higher in the Netherlands, where 93 percent say they do, and lower in the US, where only 86 percent do. Organizations with a turnover (annual revenue) of under $132,000 have the lowest prevalence of security policies in place, and 41 percent reported not having a personal IoT security policy at all. That number drops significantly as the turnover figure increases.

Of those organizations with policies in place, almost all (99 percent) find them effective, with nearly half of respondents (47 percent) considering them very effective. That said, the levels of confidence range significantly across regions. Nearly three in five IT leaders in the Netherlands (58 percent) feel their security policy for personal IoT devices is very effective compared to just over a third of respondents in Spain (34 percent). Sixty-two percent of those in Spain feel their security policy for personal IoT devices is mostly effective, compared to just 37 percent in the Netherlands.

2. https://www.bankinfosecurity.com/massive-botnet-attack-used-more-than-400000-iot-devices-a-12841

3. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

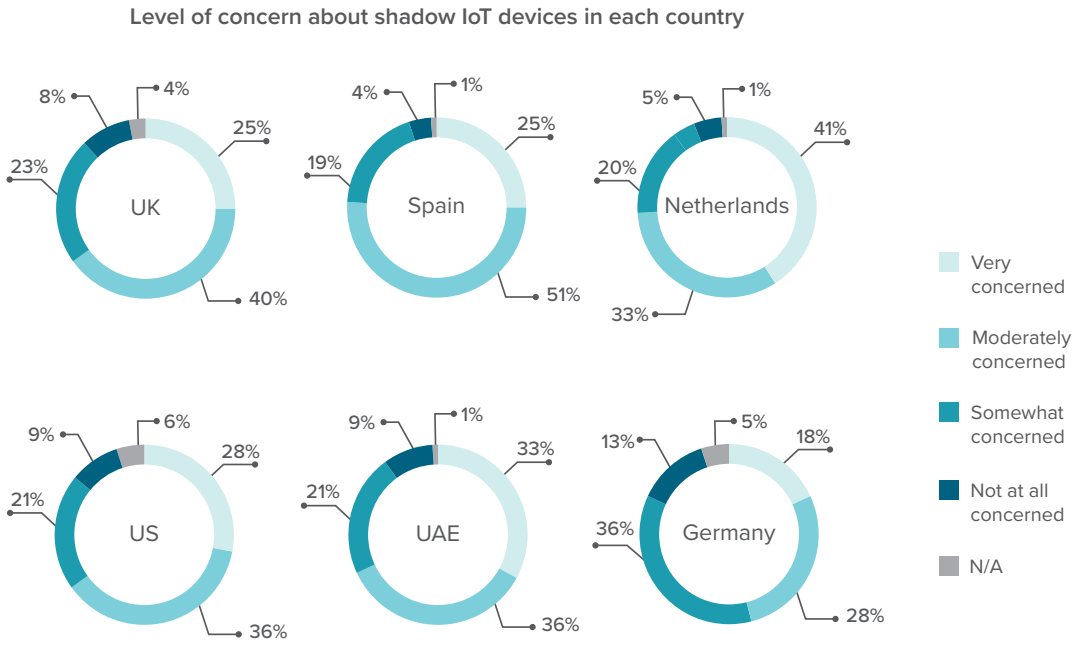


Figure 3: Level of concern about shadow IoT devices in each country

Despite feeling confident in their security, 89 percent of IT leaders remain concerned about shadow IoT devices lurking on remote or branch locations of the business. But that concern isn't equal globally: 41 percent of those in the Netherlands say they are very concerned about this challenge, while only 18 percent of those in Germany say the same.

Managing the New Network Perimeter at Scale

As business becomes more global and organizations look to reach beyond their borders, the number of branch offices and remote locations continues to increase. This proliferation of outlying work sites has serious security implications, as local offices can often be slower to implement important safety considerations than their headquarter counterparts. According to this research, only a quarter (28 percent) of local offices mirror the security solutions seen at their central headquarters. This number varies from country to country, with those in the UAE reporting 34 percent and those in the Netherlands well under the global average at 24 percent.

Managed network security services can help lower costs, improve organizational agility and improve security standards across locations. Luckily, nearly all respondents across all regions (89 percent) agree and have a company-wide security policy across all branch offices.

As it stands, 28 percent of IT leaders say they have a basic policy enforcement that includes a firewall and virus endpoint, but do not deploy any advance detection or enforcement at branch or remote offices. Twenty-seven percent of IT professionals say they tunnel all branch traffic back to their central network, while 14 percent say their branch offices only have infrastructure for workstations so they are considered "untrusted zones."

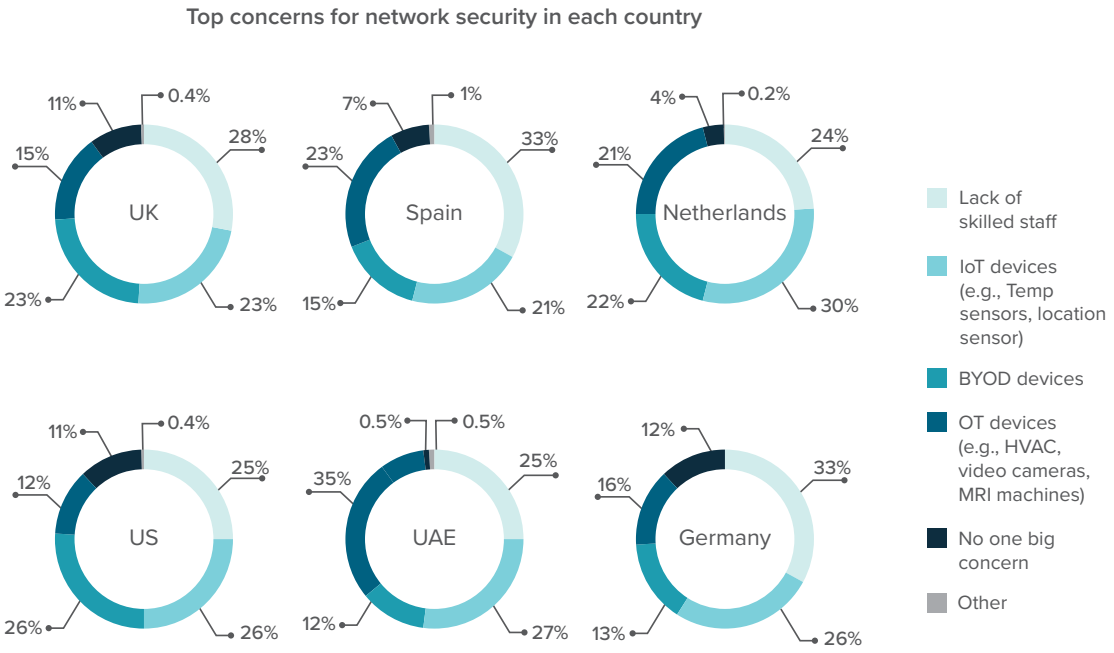


Figure 4: Top concerns for network security in each country

Managing Growing Concerns

Though threats often come from external sources, the leading cause of concern when it comes to network security is a lack of skilled staff (28 percent). This is closely followed by IoT devices (25 percent), BYOD devices (19 percent) and OT devices (19 percent). The focus of this concern varies from region to region. In the US, BYOD devices are considered a leading concern (26 percent), while only 12 percent of organizations in the UAE felt the same.

To combat shadow IoT attacks, most organizations plan to upgrade their overall security solutions. Over the next two to three years, 72 percent of businesses plan to deploy cloud-based functions (e.g., CASB, UEBA, Proxy), and 52 percent plan to implement on-premises devices (e.g., NGFW, IDS/IPS, DPI, DLP). In the UAE, plans to incorporate cloud-based functions soared past the global average, with 81 percent planning to do so by 2023 at the latest.

Despite these concerns, not all regions plan to integrate new network security solutions. Leaders in the UAE and Netherlands plan to make significant changes, while 13 percent of UK and 12 percent of US organizations still do not plan to deploy any network security solutions in the near future.

Conclusions and Recommendations

Around the world, awareness of the risk has grown significantly, yet IoT devices remain an open portal for cybercriminals looking to attack a network. It's clear that businesses are prioritizing safety, but they are still bogged down by a lack of skilled staff and the increasing number of shadow devices connecting to their infrastructure. Because of this, network and security professionals must actively manage the threat introduced by shadow devices.

How Can IT Teams Prioritize to Defend Their Networks?

Understand the Changing Ecosystem

The number of breaches is quickly growing. In 2019, the number of attacks rose 54 percent from the year prior according to a report by Risk Based Security.[4] Because the risk ecosystem is changing at such a rapid pace, organizations must change their security habits to match. While it can be easy to go down one security path, IT managers must stop and consider the wider changing needs of the business. Rethinking the approach to network security will ensure organizations are always one step ahead of cyberthreats.

Rethink Core Network Infrastructure

As enterprises continue to expand into branch offices and support their organizations with SaaS and cloud-based applications, they must prioritize implementing defenses and evolving DDI infrastructure to provide an optimal end-user experience. They must evaluate their network architecture to address visibility, reliability and management challenges of remote locations. But this won't happen on its own—organisations must implement the right tools to enable this transition.

Secure DNS

Many Internet communications rely on DNS, yet this traffic is often unsecured. This can leave organizations with various vulnerabilities that can be exploited for data exfiltration and the spread of malware. When secured, DNS can act as an organization's first line of defense by providing essential context and visibility, alerting IT admins of any network irregularities, reporting on what devices are joining and leaving the network and helping resolve problems faster. With thousands of devices joining the network daily, IT leaders must consider investing in DNS security solutions so they can identify and block malicious activity.

4. https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com