ALERT LOGIC®

CRITICAL WATCH® REPORT

SMB THREATSCAPE 2019

SMB THREATSCAPE 2019

Small to mid-sized businesses (SMBs) are under greater pressure than ever to address cyber threats. Cybercriminals are increasingly targeting smaller businesses in addition to larger enterprises. The principal challenge for SMBs is that they must face these threats with fewer security resources than large enterprises. Limited budgets and staff constraints are causing many organizations to make inadequate cybersecurity investment decisions that continue to put them at risk, but forward-looking SMB leaders are seeking new ways to be 'security smart' as they address cyber risks and respond to attacks.

In providing managed security services for over 4,000 organizations, Alert Logic has first-hand insights into how SMBs are being attacked and the best methods for responding and reducing their attack surface. Since the publication of our last look into the cyber security threatscape in 2018, we've observed a steady increase in attacks and changes in attack methods. Based on analysis of the 5,000 attacks per day we detected across our customer base during the period from November 2018 to April 2019, we identified threat patterns and incorporated those into better defenses for our customers. Additionally, our security researchers actively monitored emerging and evolving vulnerabilities and attack methods across the threatscape of the open internet beyond our customer base. This research has uncovered several patterns that specifically affect SMBs and so we have chosen to focus this latest **Critical Watch Report on the SMB Threatscape for 2019.**

By the numbers, this research is based on close examination of over 1.3 petabytes of security data, more than 2.8 billion IDS events, 8.2 million verified incidents, and the common vulnerabilities present in small to medium businesses. The results reveal nine key takeaways:

1. Encryption-related misconfigurations are the largest group of SMB security issues
2. In SMB AWS environments, encryption & S3 bucket configuration are a challenge
3. Weak encryption is a top SMB workload configuration concern
4. Most unpatched vulnerabilities in the SMB space are more than a year old
5. The three most popular TCP ports account for 65% of SMB port vulnerabilities
6. Unsupported Windows versions are rampant in mid-sized businesses
7. Outdated Linux kernels are present in nearly half of all SMB systems
8. Active unprotected FTP servers lurk in low-level SMB devices
9. SMB email servers are old and vulnerable

ALERT LOGIC CRITICAL WATCH ANALYSIS BY THE NUMBERS

1.3 Petabytes
of data analyzed

10.2 Trillion
log messages

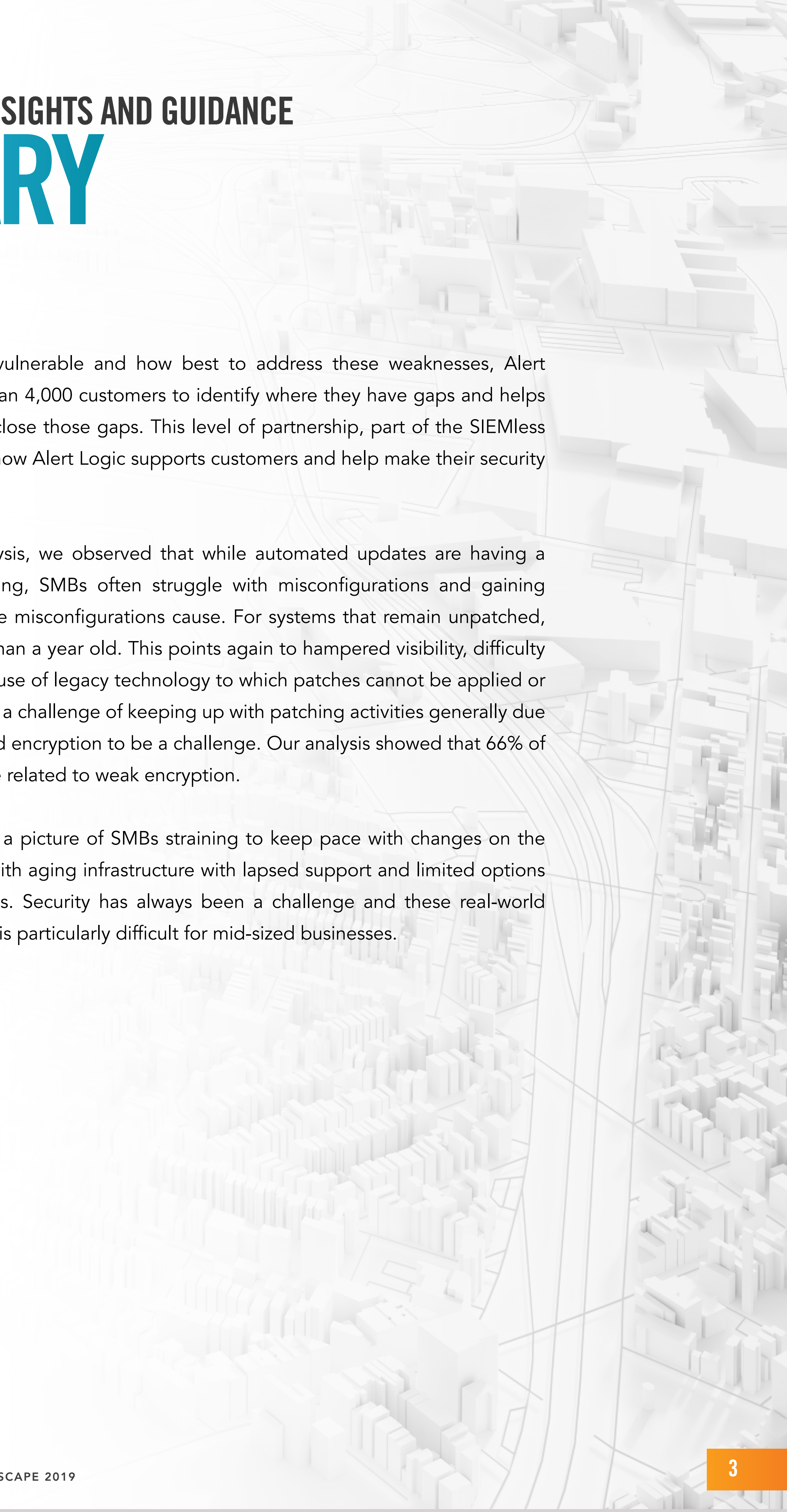
2.8 Billion
IDS events

8.2 Million
verified incidents

>4,000
customers

SMB VULNERABILITY INSIGHTS AND GUIDANCE

SUMMARY



To understand where SMBs are vulnerable and how best to address these weaknesses, Alert Logic continually scans its more than 4,000 customers to identify where they have gaps and helps organizations understand how to close those gaps. This level of partnership, part of the SIEMless Threat Management approach, is how Alert Logic supports customers and help make their security stronger every day.

In our Critical Watch Report analysis, we observed that while automated updates are having a positive impact on system patching, SMBs often struggle with misconfigurations and gaining visibility to the vulnerabilities these misconfigurations cause. For systems that remain unpatched, available patches are often more than a year old. This points again to hampered visibility, difficulty in locating vulnerabilities, and the use of legacy technology to which patches cannot be applied or are no longer provided, along with a challenge of keeping up with patching activities generally due to limited resources. SMBs also find encryption to be a challenge. Our analysis showed that 66% of workload configuration issues were related to weak encryption.

In these nine takeaways, we paint a picture of SMBs straining to keep pace with changes on the security landscape while dealing with aging infrastructure with lapsed support and limited options for security updates and bug fixes. Security has always been a challenge and these real-world observations indicate that security is particularly difficult for mid-sized businesses.

SMB VULNERABILITY INSIGHTS AND GUIDANCE

KEY TAKEAWAYS

TAKEAWAY 1

ENCRYPTION-RELATED MISCONFIGURATIONS ARE THE LARGEST GROUP OF SMB SECURITY ISSUES

Automated patching has made inroads in the fight to eliminate vulnerabilities in the SMB space. Patches are often distributed and can be done automatically across ecosystems. What remains as an issue is misconfigurations which can require remediations ranging from manual reviews to complete architectural redesigns. In our analysis, we determined that 13 encryption-related configuration issues account for 42% of all security issues found.

42%

of top SMB security issues are related to encryption

TAKEAWAY 2

FOR SMB AWS ENVIRONMENTS, ENCRYPTION ISSUES AND S3 BUCKET CONFIGURATION STILL A CHALLENGE

Amazon Web Services is a strong player in the global cloud-infrastructure industry, with a market share equivalent to that of the next four public cloud providers combined.[1] Our analysis of AWS configuration issues shows that encryption issues affect 33 percent of the SMB instances we scanned. This indicates encryption is not yet an instinctive behavior despite being a best practice and a requirement of many regulations including PCI-DSS, HIPAA, HITECH, GBLA, GDPR, NIST, SOX, and state regulations such as CA SB 1386.

In addition, while there is a significant focus on blocking inbound traffic to prevent attacks, organizations would also be well served to foil attacks by implementing basic configuration checks, preventing outbound contact to command and control servers as well as implementing measures to prevent data exfiltration. Of the SMB AWS instances we observed, more than 14 percent had significant S3 bucket configuration issues.

[1](Source: https://www.srgresearch.com/articles/fourth-quarter-growth-cloud-services-tops-banner-year-cloud-providers).

SMB VULNERABILITY INSIGHTS AND GUIDANCE

KEY TAKEAWAYS

TAKEAWAY 3

WEAK ENCRYPTION IS A TOP SMB WORKLOAD CONFIGURATION CONCERN

When we examined the top workload configuration issues, we discovered that 66 percent of the issues were related to weak encryption. Understanding and configuring encryption trade-offs within an application is difficult, and as a result, many organizations just implement the default encryption associated with an application. This presents a security challenge as many of these defaults were defined when older encryption protocols were still considered safe.

As an example, OWASP shares the perspective that these encryption protocols (below) are to be avoided[2] and yet we still see them regularly in use today:

- MD5 has recently been found less secure than previously thought. Secure applications should migrate away from this algorithm
- SHA-0 has been conclusively broken and should no longer be used for sensitive applications
- SHA-1 has been reduced in strength; SHA-256, which implements a larger key size, should be used instead
- AES is the current preferred symmetric algorithm, not DES

TAKEAWAY 4

MOST UNPATCHED VULNERABILITIES IN THE SMB SPACE ARE MORE THAN A YEAR OLD

Even though automated updates have vastly improved software patching, organizations are still having difficulty keeping pace. When examining the top 20 unpatched vulnerabilities present in the SMB space, Alert Logic found that 75 percent of them are more than a year old.

The use of open source software, a widespread and established technique for building software projects efficiently, can complicate the patch cycle. This is particularly true when the open source software is embedded. This is a challenge for organizations that leverage open source resources and libraries. To uncover and reduce the vulnerabilities left by this unpatched code, it is critical for all organizations to invest in third-party validation of the efficacy of the update process in the software development life cycle (SDLC). Regular vulnerability scanning is also a requirement.

66%

of top SMB workload configuration issues involve weak encryption

[2] (Source: https://www.owasp.org/index.php/Guide_to_Cryptography)

SMB VULNERABILITY INSIGHTS AND GUIDANCE
KEY TAKEAWAYS

TAKEAWAY 5

THE THREE MOST POPULAR TCP PORTS ACCOUNT FOR 65% OF SMB PORT VULNERABILITIES

Port scanning is done regularly by both attackers and defenders. Internal security teams, blue teams, can use regular port scanning to help identify weaknesses, firewall misconfiguration issues, and to discover unusual services running on systems.

When considering their attack surface, organizations should be aware of which ports have the most vulnerabilities—which is a factor of port popularity more than a statement on the port's relative security. In examining ports, given that these ports are the ones that are exposed to the internet it is no surprise that SSH (22/TCP), HTTPS (443/TCP) and HTTP (80/TCP) made the top three with 65 percent of the vulnerabilities. It is, however, interesting to note that the recent MS RDP BlueKeep attack targets the fourth most popular port, RDP/TCP.

As basic guidance, security across all network ports should include defense-in-depth. Ports that are not in use should be closed and organizations should install a firewall on every host as well as monitor and filter port traffic. Regular port scans and penetration testing are also best practices to help ensure there are no unchecked vulnerabilities. In addition to these steps, patch and harden any device, software, or service connected to ports to further close off avenues of attack.

Patch and harden any device, software, or service connected to the port until there are no dents in your networked assets' armor. Be proactive as new vulnerabilities appear in old and new software that attackers can reach via network ports. Lastly, be sure to change all default settings and passwords as well as running regular configuration checks.

65%

of port vulnerabilities appear on three ports: SSH (22/TCP), HTTPS (443/TCP) and HTTP (80/TCP)

SMB VULNERABILITY INSIGHTS AND GUIDANCE

KEY TAKEAWAYS

TAKEAWAY 6

UNSUPPORTED WINDOWS VERSIONS ARE RAMPANT IN MID-SIZED BUSINESSES

More than 66 percent of scanned devices are running Microsoft OS versions that will be out of support by January 2020. The current Windows Server release – 2019 – is almost undetectable while the majority of devices scanned during the period analyzed are running Windows versions that are more than 10 years old.

Additionally, there are still a non-trivial number of Windows XP and even 20-year-old Windows NT devices out there. Even if they are not exposed to the internet, these targets make lateral movement relatively easy once a host has been compromised. With the discontinuation of security updates and bug fixes for Windows Server 2008 scheduled for 2020, combined with the SMB trend of holding on to old operating systems, this security issue is likely to get much worse next year.

66%

of SMB devices run Microsoft OS versions that are expired or about to expire

SMB VULNERABILITY INSIGHTS AND GUIDANCE

KEY TAKEAWAYS

TAKEAWAY 7

OUTDATED LINUX KERNELS PRESENT IN NEARLY HALF OF ALL SMB SYSTEMS

Kernels are the heart of an operating system. They manage everything including hardware, memory, applications, and even user privileges. Kernel vulnerabilities are discovered quite frequently, and fixes are only released for supported versions. In a 2017 article, ComputerWorld described these outdated Linux kernels as the working dead.

50%

the approximate amount of SMB Linux kernels that are among the 'working dead'

Many deployed application systems mask the underlying OS distribution flavor making it difficult to determine which kernel version is being run, however about half the systems we identified are still running a version 2.6 kernel, which has been out of support for more than 3 years. There are at least 69 known vulnerabilities for this kernel level, with many of them relatively easy to exploit and with 24 of the Common Vulnerabilities and Exposures (CVEs) scoring 7 or above on the severity scale.

TAKEAWAY 8

ACTIVE UNPROTECTED FTP SERVERS LURK IN LOW-LEVEL SMB DEVICES

The nearly 50-year-old file transfer protocol (FTP) is really showing its age from a security standpoint and yet we continue to find FTP servers in SMB environments. With a lack of built-in strong authentication and non-repudiation functionality, FTP is seriously flawed. Yet, of all the FTP servers found, very few were using SFTP for increased security. In our vulnerability scanning, we found a disturbing number of FTP servers active on printers, cameras and uninterruptable power supplies—estimated to be as much as one-third of all the FTP servers we found.

Hackers continue to use these innocent-looking devices to store and distribute malware. As a precaution, organizations should shut down unnecessary FTP servers and access, especially on devices that are not commonly monitored such as printers and power supplies.

SMB VULNERABILITY INSIGHTS AND GUIDANCE

KEY TAKEAWAYS

TAKEAWAY 9

SMB EMAIL SERVERS ARE OLD AND VULNERABLE

Modern businesses are fueled by email and mid-sized businesses are no exception. Without email, business communication grinds to a halt. This is why we were surprised to see that almost a third of the top email servers detected were running on Exchange 2000, which has been unsupported for almost 10 years (since July 2010). Despite being the life blood of organizations, SMBs are running the risk of email failures resulting from newly identified vulnerabilities for which patches will not be made available.

>30%

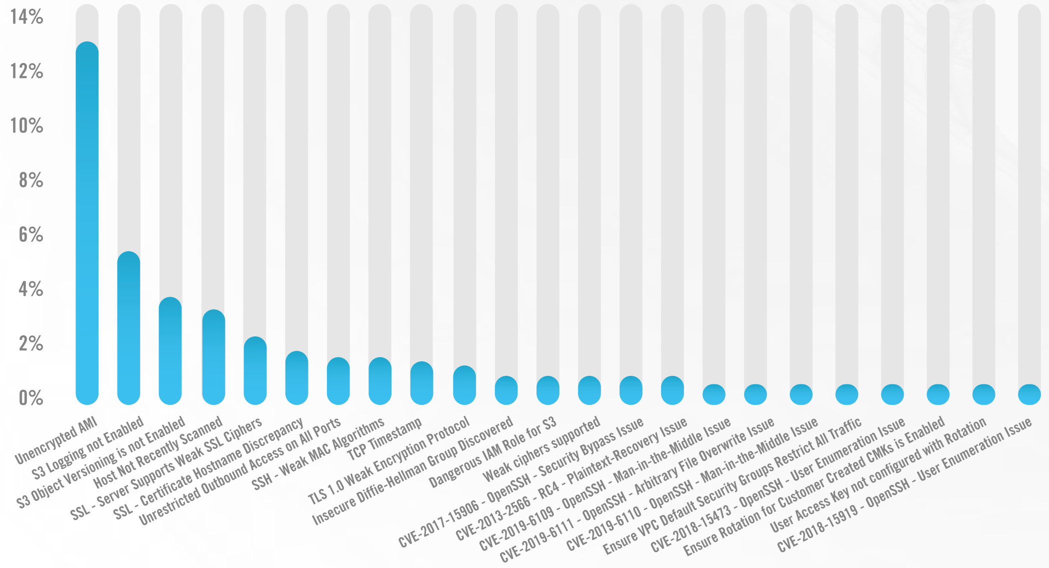
of SMB email servers operate on unsupported software

SMB VULNERABILITY INSIGHTS AND GUIDANCE

THE DATA

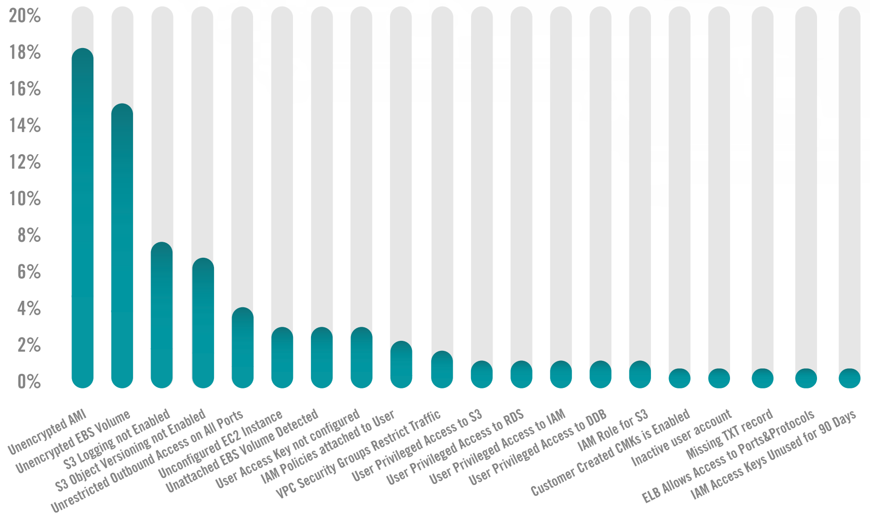
Top Security Issues for SMBs

TABLE 1



Top AWS SMB Configuration Issues

TABLE 2

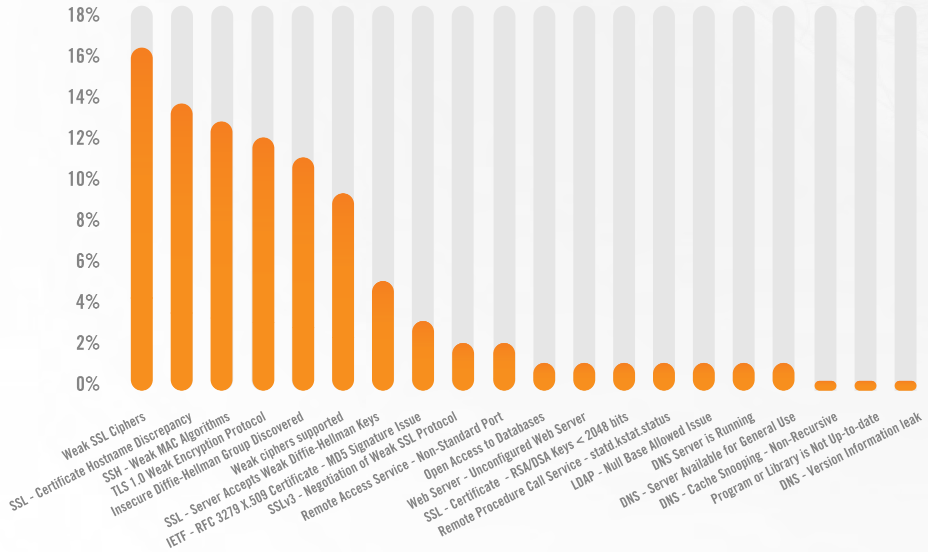


SMB VULNERABILITY INSIGHTS AND GUIDANCE

THE DATA

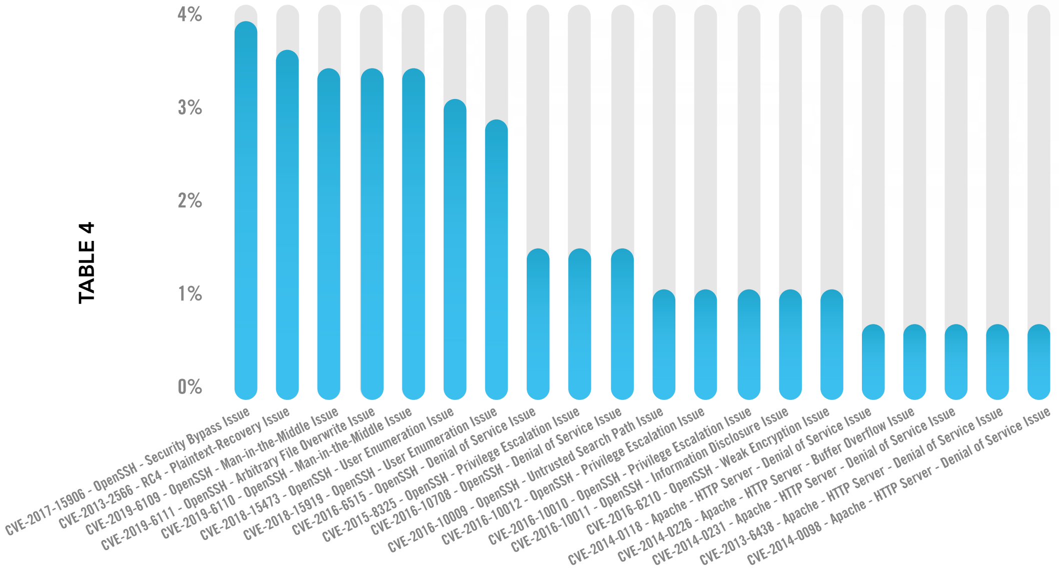
Top SMB Workload Configuration Issues

TABLE 3



Top Missing Patches

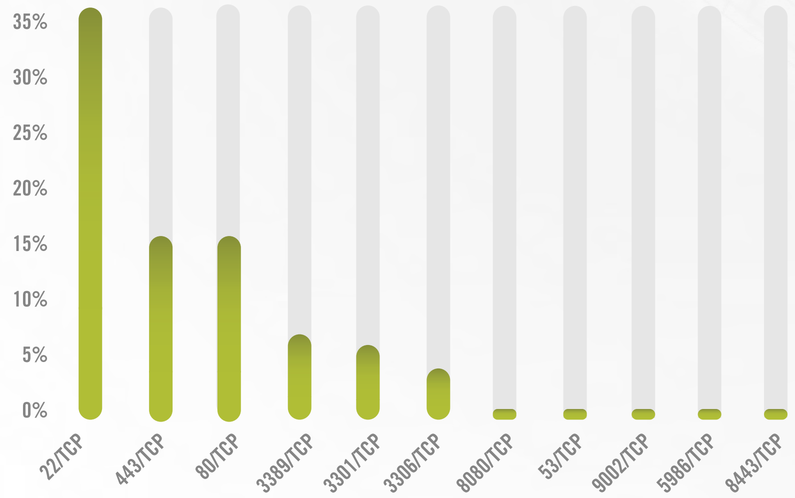
TABLE 4



THE DATA

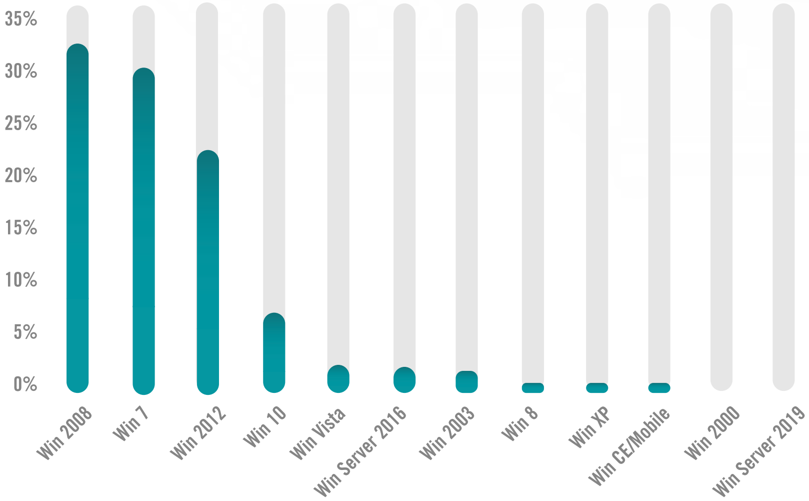
Top Vulnerable Ports

TABLE 5



Windows OS Distribution in SMBs

TABLE 6

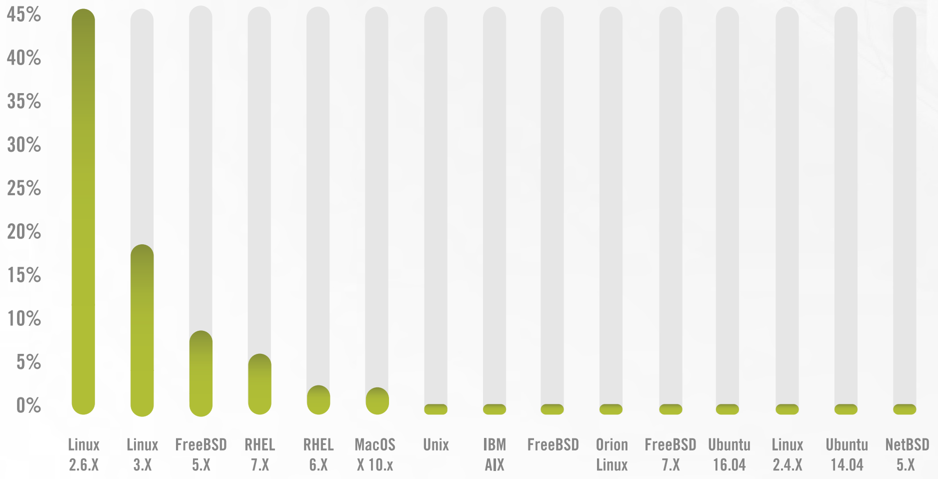


SMB VULNERABILITY INSIGHTS AND GUIDANCE

THE DATA

SMB Linux/Unix OS Distribution

TABLE 7



SMB FTP Server Distribution

TABLE 8

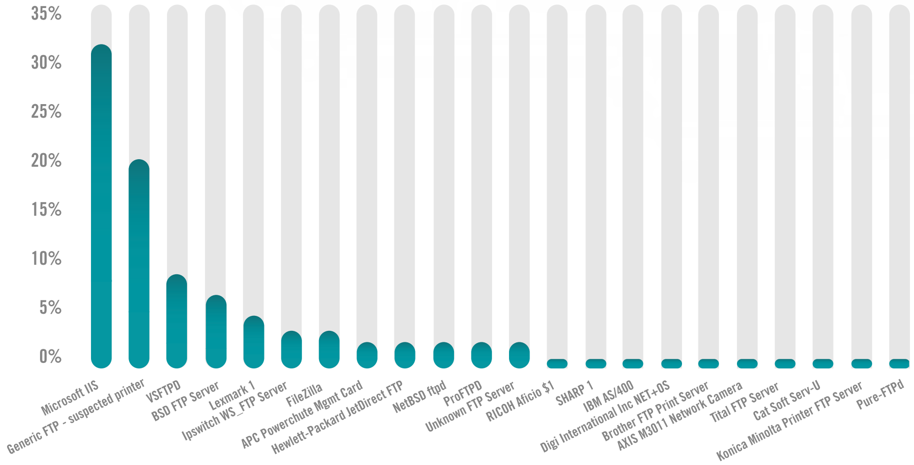
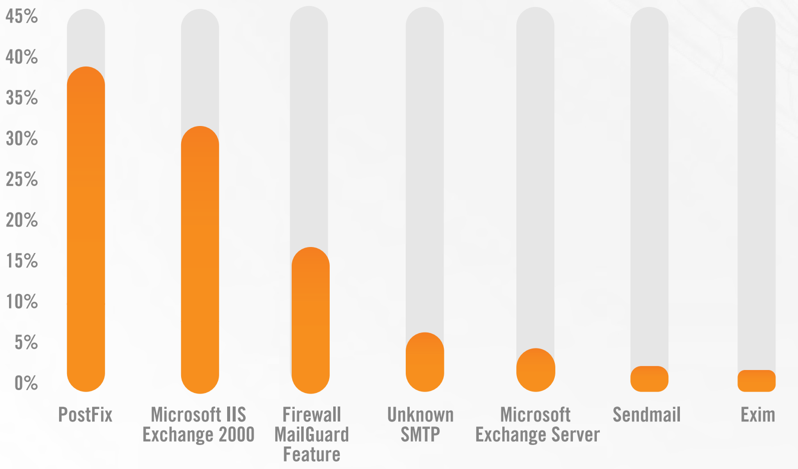
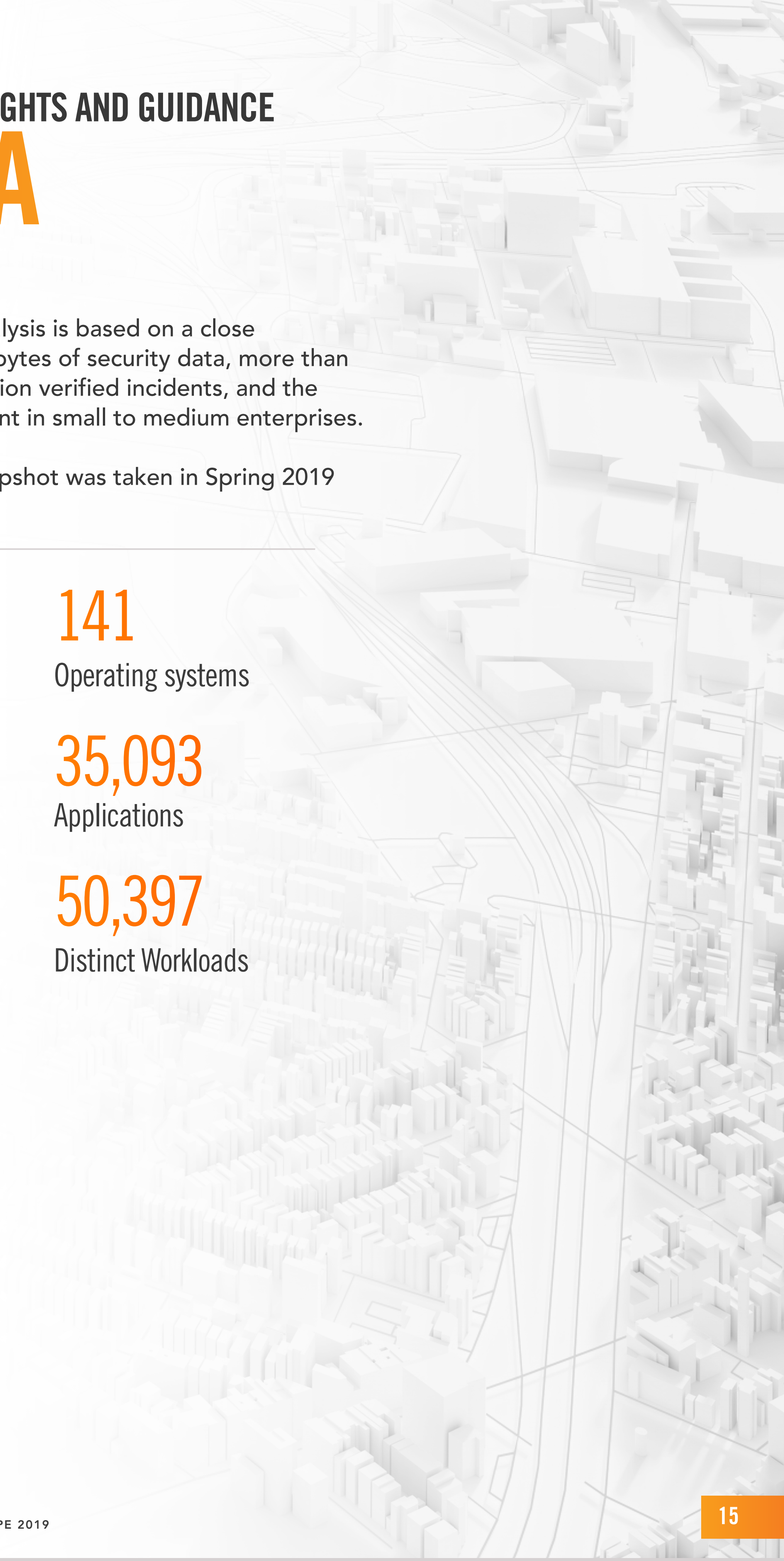


TABLE 9

SMB Email Server Distribution





SMB VULNERABILITY INSIGHTS AND GUIDANCE

THE DATA

Alert Logic Critical Watch analysis is based on a close examination of over 1.3 petabytes of security data, more than 2.8 billion IDS events, 8.2 million verified incidents, and the common vulnerabilities present in small to medium enterprises.

Our ‘key takeaways’ data snapshot was taken in Spring 2019 and respresents:

762
Unique customers

141
Operating systems

1457
AWS environments

35,093
Applications

2786
VPCs

50,397
Distinct Workloads

3,412,170
Individual vulnerabilities

ALERT LOGIC®

SIEMLESS THREAT MANAGEMENT

alertlogic.com