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 Outdated Linux kernels are present in nearly half of all SMB systems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.

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).

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)

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)

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

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

THREAT INTELLIGENCE BRIEF:

THE ECONOMICS OF CYBERCRIME

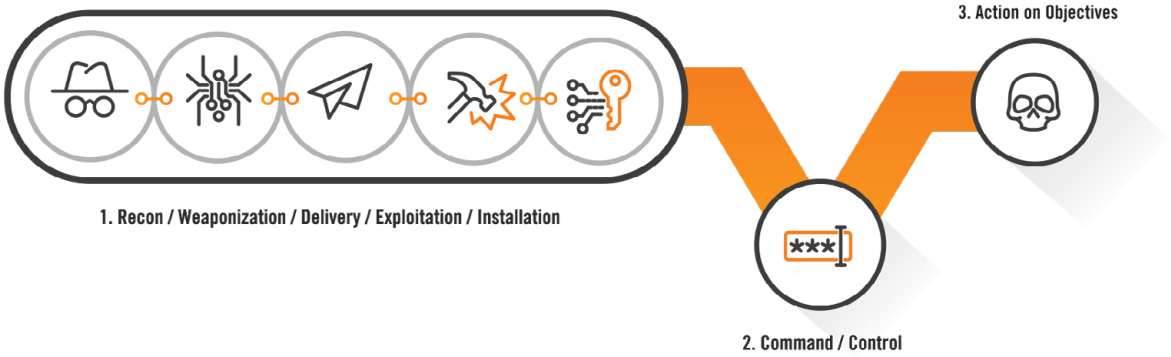
Organizations of all sizes are struggling with a 'perfect storm' in cybercrime, In recent years, cyber attack methods have evolved aggressively to become more targeted, more sophisticated, and more frequent. With new highly scalable attacks targeting any vulnerable company and with their very low cost of delivery, attacks don't need a high success rate to make money. New techniques and attacks against smaller and less protected targets create multiple opportunities for fast profit.

For the criminals, attacks couldn't get much simpler. Exploit kits, packaged attacks and Ransomware-as-a-Service (RaaS) are removing historic technical barriers, allowing a widening group of criminals to build, launch, and profit from their own campaigns. With the commoditization of attacks and how rapidly they evolve, it is clear that cyber crime has become big business, albeit a nefarious one, with all the considerations of a business including risk-reward trade-offs and hard calculations about how much money these attacks can earn.

One of the trends we observed in 2019 was a shift in criminal tactics and payload delivery that followed the lines of market externalities. At the end of 2018, for example, it looked like cryptojacking — in which malware hijacks a computer's resources to mine cryptocurrency like Monero or Bitcoin — looked to be the new cryptocrime of choice. Unfortunately for the attackers, cryptocurrencies hit a major downturn, taking with them the profitability model that had inspired the attacks. As a result, the 2019 attack landscape has shifted yet again to ransomware, a popular attack in which attackers commonly encrypt a system's files and demand money for the key, experienced a resurgence, targeting businesses, individuals and municipal government entities, most recently the city of Baltimore.

In addition, to the return of ransomware, Alert Logic has seen continued proliferation of the so-called dropper attacks which we highlighted in our 2018 report. These attacks modified the kill chain with a innovation in payload delivery:

THE NEW CYBER KILL CHAIN®



THREAT INTELLIGENCE BRIEF:

THE ECONOMICS OF CYBERCRIME

These threats and others pose significant risks to small and medium business (SMBs), which are clearly in the crosshairs of cyber attackers and are often ill-equipped to deal with the full and constantly shifting range of attacks. Inc Magazine reported on the devastating effects of these attacks on small businesses, with 60% closing within 6 months of a successful breach.

PERFECT STORMS

"Monetization strategies change over time," said Jack Danahy, Senior Vice President, Security, for information security company Alert Logic, but "there's there will always be a way to monetize a successful cyber attack."

Whether a criminal operation's "crime of choice" at any given moment involves credit card thefts, weaponized adware, or mining cryptocurrency, they are all motivated by, and relate to, the execution of a perfect crime.

There are three elements that define a perfect crime, and they are all part of the perfect storm that is fueling the growth in cybercrime, Danahy said. They are profit, simplicity of execution, and anonymity. The first consideration, of course, is whether a scheme will pay off; the more the better. With regard to simplicity, criminals like crimes that are straightforward: complexity invites mistakes and disruption. Finally, criminals don't want to be caught: The more difficult it is to associate the criminal and the crime, the more likely they'll choose that option. Commoditized and automated cybercrimes like ransomware hit on all of these criteria.

PROFITABILITY: Exact numbers can be hard to pin down, but estimates on the costs from ransomware range from $8 billion globally in 2018 to $75 billion a year from small and mid-size U.S. businesses. Another estimate, looking at cybercrime overall, projects that the total costs will hit $6 trillion by 2021. However, costs are measured, cybercrime is the fastest growing criminal activity, not least because it is so lucrative.

SIMPLICITY: Ransomware is also a very simple attack, because attacks can be conducted from a computer anywhere in the world, and because the criminals don't even have to know how to write their own attacks; they just need to go shopping for them on the Dark Web. The devastating WannaCry campaign of 2017 was built on two packages (EternalBlue and DoublePulsar) that were reportedly developed by the US National Security Agency but then leaked publicly by the hacker group The Shadow Brokers. The complexity of the underlying technology was hidden by the development of a campaign that automated the discovery, exploitation, and ultimate compromise, of targeted systems.

ANONYMITY: The payouts for these crimes are made in pseudo-anonymous cryptocurrencies, and are delivered across a range of geographies and timezones, and this obfuscated payment is then combined with the use of ephemeral aliases, spoofed servers, and variable international law. As a result, the criminals experience near total anonymity, and are seldom identified, pursued, or prosecuted.

As recent history has shown, however, the dominance of ransomware or any specific method of cybercrime is not a steady state. Monetization of cybercrime has historically shifted regularly and will shift again, maybe turning back to cryptojacking, some other historic tactic, or some new criminal innovation. As that evolution continues, existing campaigns and tactics will remain, no matter what the next trend brings. We see that that the distributed denial-of-service attacks from the 1990's are still around, as are spyware, credential and credit card theft, and many other exploits. A successful cybersecurity strategy must continue to defend against this range of threats while also keeping current with the new.

THE SMB CHALLENGE

When defending networks, devices, and data against this changing landscape, organizations require a balanced approach that will effectively prevent attacks from succeeding but that will also quickly detect any signs that an attack has managed to infect a system. Given the rapid lateral spread of modern campaigns and the techniques they use to remove evidence of their arrival, detection and mitigation can only be assured with continuous monitoring by trained security analysts. Most organizations do not have the resources or infrastructure to support this kind of 24/7 visibility, and small and medium businesss (SMBs) are particularly exposed. In this environment, managed security monitoring, detection, and response is the most effective option.

"Criminals have gone so far as to create, and then rent out, attack infrastructure like exploit kits and ransomware as a service."

-Jack Danahy, SVP, Security, Alert Logic

SMBs are at a disadvantage when it comes to implementing a comprehensive cybersecurity strategy. These common attack campaigns do not differentiate between small and large organizations, they simply target network address ranges or available email addresses. As a result, the SMB is facing the same threats as much larger organizations without the substantial budget and cybersecurity staffing. They are also more dynamic, with many SMBs adding new systems, technologies, and employees in a less regimented, more organic process, leading to additional vulnerability and complexity. As a result, criminals have found SMBs to be an attractive set of targets.

We can see the results. While data breaches involving large businesses get public attention because of the volume of compromised information involved, Verizon's 2019 DBIR found that 43 percent of all breaches involved small businesses, more than the number of victims in the public sector, healthcare and financial industries combined.

THREAT INTELLIGENCE BRIEF:
THE ECONOMICS OF CYBERCRIME

A BETTER WAY

A service such as Alert Logic's, takes a holistic approach to threat detection and mitigation, scanning for the full range of threats at all stages of the attack lifecycle. In addition to identifying exploits as they attempt to compromise systems, Alert Logic also identifies malware and attackers that have already taken up shop. This is a critical benefit, since dwell time (the amount of time a successful compromise continues to operate prior to detection) continues to be a critical problem. According to recent estimates, dwell time remains high, at 78 days. It is common for organizations to go months before they realize they've been hacked, while most attacks succeed and begin exfiltrating data in minutes.

By watching for anomalous user behavior, data exfiltration, and other signs, Alert Logic analysts can identify previously infected systems.

Alert Logic also identifies unpatched system vulnerabilities, another all-too-common entry point for successful hacks. According to DarkReading, 60% of data breaches over the past two years began with an exploit of an unpatched system. In the case of 2017's WannaCry campaign, 200,000 systems were compromised using a vulnerability for which a patch was released almost two months before the attack began. The recent Microsoft BlueKeep patch has available since mid-May, but over 1 million internet-connected computers remain visibly unpatched.

A managed service such as Alert Logic raises the visibility of these vulnerabilities to reduce the likelihood of these common compromises. The service identifies organization assets and scans them for known vulnerabilities, providing prioritized recommendations for remediation based on vulnerability severity and likely impact. Applying patches remains an organizational responsibility, but the existence of this to-do list with clear priorities provides the guidance and visibility to reduce patch latency and decrease the window of vulnerability.

Alert Logic also identifies unpatched system vulnerabilities, another all-too-common entry point for successful hacks. According to DarkReading, 60% of data breaches over the past two years began with an exploit of an unpatched system. In the case of 2017's WannaCry campaign, 200,000 systems were compromised using a vulnerability for which a patch was released almost two months before the attack began. The recent Microsoft BlueKeep patch has available since mid-May, but over 1 million internet-connected computers remain visibly unpatched.

A managed service such as Alert Logic raises the visibility of these vulnerabilities to reduce the likelihood of these common compromises. The service identifies organization assets and scans them for known vulnerabilities, providing prioritized recommendations for remediation based on vulnerability severity and likely impact. Applying patches remains an organizational responsibility, but the existence of this to-do list with clear priorities provides the guidance and visibility to reduce patch latency and decrease the window of vulnerability.

THREAT INTELLIGENCE BRIEF:

CURATION AND THE OPEN SOURCE PROBLEM

Open-source threat intelligence sounds like a sweet deal for many organizations. It can add much needed attack data information to organizations that would otherwise be flying blind. It costs less than investing in proprietary intelligence feeds, and lets organizations avoid being locked in to a particular vendor. And tapping into shared resources can bring more talent — and eyeballs — into the fold, improving reliability and providing an increased measure of security through transparency.

It's an approach that appeals to small and medium businesss (SMBs) that may not have the resources to invest in major development projects but are still looking for the shortest distance to growth and profitability. Businesses have adopted open source threat intelligence as a component of their security programs because it provides them with vital attack information they couldn't otherwise afford.

But no single approach is perfect, and an overreliance on open threat intelligence has its downsides, several of which can crop up when it comes to implementing a security strategy that is both comprehensive enough and supple enough to handle a constantly shifting cyber threat landscape. SMBs face the same threats as large corporations and government agencies but, in the same vein as their budgetary disadvantage when acquiring and making use of attack data, they may not have the means on their own to effectively deal with a cybersecurity challenge that is getting bigger all the time. An outside service capable of dealing with the full spectrum of cyber threats could be the key to keeping a business safe.

> *"One of the biggest problems with relying on open source threat intelligence exclusively, is that there is no specific context that relates to your business. That can make the problem of responding to threats harder."*
>
> *-Jonny Milliken, Threat Intelligence, Alert Logic*

DROWNING IN DATA

For starters, cybersecurity monitoring in any circumstance generates reams of data from multiple sources. "So in the end what you get is a lot of data but not really information," said Jonny Milliken, Threat Intelligence Manager for cybersecurity provider Alert Logic. The trick is analyzing that data for pertinent information that an organization can then act on. "And this is more difficult with open source perspectives because then you also

THREAT INTELLIGENCE BRIEF:
CURATION AND THE OPEN SOURCE PROBLEM

need to have somebody to identify which of that data is even relevant to the organization," Milliken said.

The data must be curated — analyzed in relation to other applicable inputs — so that serious threats can be separated out from the mountain of noise, false positives and activity that looks suspicious but are actually benign. Open source threat intelligence complicates the challenge because, unlike a paid third-party service that has cyber personnel on the other end of the phone, the open source development community isn't set up for a quick response. "There's nobody there to help curate the data for you," Milliken said.

That can leave small and medium businesss (SMBs) and similar organizations, which may be short on cybersecurity budgets and manpower, in difficult straits. "They can't find the staff to hire. And even when they do find staff, they can't retain them," he said. "Then you've got a real problem just in terms of being able to take that open source data and turn it into something that you can do something with. Extracting actionable data from a sea of information is an enormous job. Everything has to be placed into context. And when it comes to threat intelligence, context is everything."

The lack of context in analyzing a suspected attack can lead to confusion in how, and whether, to respond. "The other challenge with open source threat intelligence, is that relying on that as your information source for attack data—you're going to lose time," which is a critical factor in mitigating the effects of an attack, he said. Members of an open source community might offer ad hoc advice on an attack, but it won't be contextualized to your business. You'll need to add that level of detail. "All of that effort takes time away from your response. Failing to act quickly in an efficient and informed way leaves you more vulnerable to the effects of that attack because your mitigation and remediation steps can't be performed it as quickly as they should."

Other factors can further complicate the challenge. Automation through machine learning and other technologies, which have accelerated the pace of the cybersecurity battles, can help significantly with analyzing and responding to attacks, but it also comes with caveats. "Analysis and automation can allow good things to scale, but it also allows problems to scale. So if you have bad data, then automation will allow you to just generate more bad information based on greater amounts of bad data" Milliken said. "It is important, as in all things, just to make sure that you understand the problem and that you're addressing it appropriately for that business. Then automation allows that good stuff to scale. But if you do it badly then automation can lead you down a bad path."

THREAT INTELLIGENCE BRIEF:
CURATION AND THE OPEN SOURCE PROBLEM

EXTRACTING VALUE FROM DATA

In terms of providing comprehensive cybersecurity, these factors only add to what is, by any measure, and overwhelmingly big job. A service that provides a holistic approach can survey cyber activity in context, with internal intelligence analysts acquiring data, analyzing it in relation to data from all of its other customers as well as curated open source data, validating its usefulness, and recommending courses of action. Essentially, it turns data into information and information into action. A customer need focus only on the last part, rather than all of the factors that went into a recommendation.

"And in the end, that's all really customers really want," Milliken said. "They don't really want lakes of log data or even disparate bits of potentially valuable information." They want to know if a breach has occurred and what they should do about it. Or, perhaps, that a breach hasn't occurred, but someone is keeping an eye out for the next one, so they won't find out about it when the FBI tells them six months later. "And that's where Alert Logic is able to help," he said.

The company has a lot of data to draw on. Alert Logic logs over 2.8 billion intrusion detection system (IDS) events annually. "So that is 2.8 billion potentially malicious activities that we have assessed in our systems through a combination of our analytics engine, our machine learning algorithms, and expert analysts and threat hunters, in order to identify the needles in this giant haystack we have created," he said. A large store of IDS signatures and other data provides a perspective that a small organization couldn't create with the tools it has at hand, and increases the likelihood of detecting, deterring and responding to a greater variety of attacks.

"One of the largest challenges Alert Logic solves for our customers is the ability to accelerate their threat response."

-Jonny Milliken,
Threat Intelligence, Alert Logic

THE COMMUNITY DEFENSE ADVANTAGE

An advantage of a holistic approach is the community defense effect which is an old idea in economics, business and, increasingly, health care that applies neatly to cybersecurity. The community defense effect posits that the value of a product or service increases as more people use it, because the biggest benefits

THREAT INTELLIGENCE BRIEF:

CURATION AND THE OPEN SOURCE PROBLEM

of the network lie in having a vast number of users. The classic example is the telephone — as more people connected to a telephone service, they each had more people they could talk to. As a result, there was more value in having a phone. It's also taken hold in many other areas, including social media, where the appeal of something like Facebook and Twitter depends on the rest of the world being on Facebook and Twitter.

In cybersecurity, the community defense effect payoff comes in the form of a feedback loop that includes data from multiple customers. Using this resource of more than 4,000 customers, our security researchers can quickly identify active threats, understand which threats pose the biggest danger, and how best to mount an active response. With that kind of threat intelligence, an attack can be identified early and prevented across the network, before it can take hold of any customer's network, essentially inoculating the entire community of customers against that attack. The community defenses' one-for-all-and-all-for-one approach also helps with threat hunting, an emerging proactive security practice that aims to identify new exploits before they strike.

Threat hunting is "basically, looking for attacks that aren't known," Milliken said. Antivirus and other tools are good at fending off known attacks, but the snake that bites you is always the one you didn't see—that is, zero days attacks that exploit previously unknown vulnerabilities. Machine learning and analytics tools have enhanced threat hunting, allowing it to look for suspicious, not just unusual, behavior, which enables pre-emptive mitigation.

"It's sort of analogous to the herd effect in terms of bio immune response," Milliken said. Identifying attacks before they hit can, in terms of threat detection, inoculate large swathes of customers. "We can take the knowledge and the visibility and the data across all customers and use that to protect every other customer. And that is not a thing that customers can do by themselves." Alert Logic draws on the wealth of data from its customers to help the rest of its customers. Being part of a herd provides better protection that being on your own.

"Antivirus and other tools are good at fending off known attacks, but the snake that bites you is always the one you didn't see—that is, attacks that exploit previously unknown vulnerabilities."

-Jonny Milliken, Threat Intelligence, Alert Logic

THREAT INTELLIGENCE BRIEF:
CURATION AND THE OPEN SOURCE PROBLEM

MANAGING RISK

There's no such thing as a perfect, unhackable system, so a big component of effective security is managing risk. Risk is composed on three basic elements: The threat, the vulnerability, and whether the threat is actually attacking that vulnerability. "If an attacker is not attempting it well then your risk is pretty much zero," Milliken said. No one wants to have vulnerabilities, but if no one is attacking a particular weakness, it can't be breached. "So from our perspective, once we've helped our customers reduce their attack surface and eliminate as many vulnerabilities as they can, the bit that we would focus on is what is the actual threat," he said. "Let's get the data to analyze that and cover the things that you're being currently hit with right now. In the end that's how we stop attackers in their tracks. And we do it in a way that a customer simply cannot replicate on their own."

A lot goes into identifying those actual threats. Along with monitoring and analysis, Alert Logic also has a reverse engineering team that works to identify the existence of vulnerabilities before they are loose in the world. "Our goal is to eventually work out such a large scope of the different potential malicious things that an attacker could do that no matter what you think it is that the attacker does you'll have that data in our dataset," and ready for a quick response, he said."

> ***"The benefit that a curated threat intelligence resource brings is relevant information tailored to your business environment. So you, as a customer, get insight into what you are being hit with right now and how to stop that specific threat or attack. We do that in a way that a customer simply cannot replicate on their own."***
>
> ***-Jonny Milliken,***
> ***Threat Intelligence, Alert Logic***

Sometimes analysts will "war room" a serious threat, such as the recent Microsoft remote code execution vulnerability (CVE-2019-0708), which threatens a large swath of the Internet and, therefore, the customer base. But for the most part, new attacks are handled routinely. Thousands of new attacks are released weekly, and getting a handle on their severity is just part of the job. Alert Logic's follow the sun model means that our analysts work around the clock, checking with each other across seven time zones, and checking with security operations centers and other teams to hasten a response.

THREAT INTELLIGENCE BRIEF:
CURATION AND THE OPEN SOURCE PROBLEM

CONCLUSION

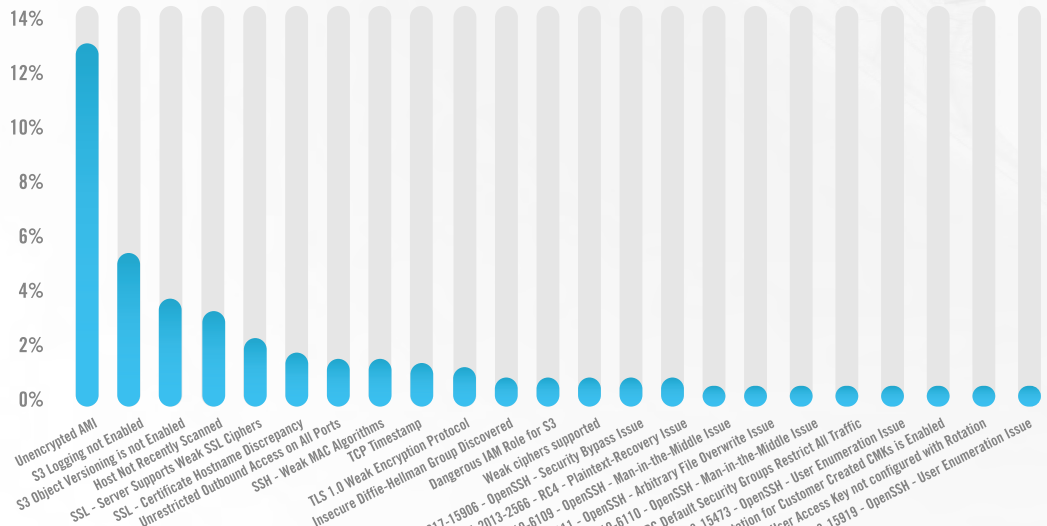
A lot goes into a cyber defense strategy, but ultimately, it's a results-driven operation. You either survive an attack or you don't. All of the considerable action that takes place behind the scenes is essential to securing the network, but to SMBs and similar organizations, what matters in the final outcome.

Small and medium businesses are at a disadvantage in defending themselves against a vast cyber battlefield where attackers are generating ever-more sophisticated attacks against an ever-growing attack surface, including mobile, Internet of Things and other connected devices. To help keep their systems from being compromised, and to mitigate successful attacks as quickly as possible, they need a holistic cybersecurity approach with the capacity to monitor systems, identify even brand-new threat, locate existing, unpatched vulnerabilities and turn all that information into action. The bottom line is that their bottom lines depend on it.

THE DATA

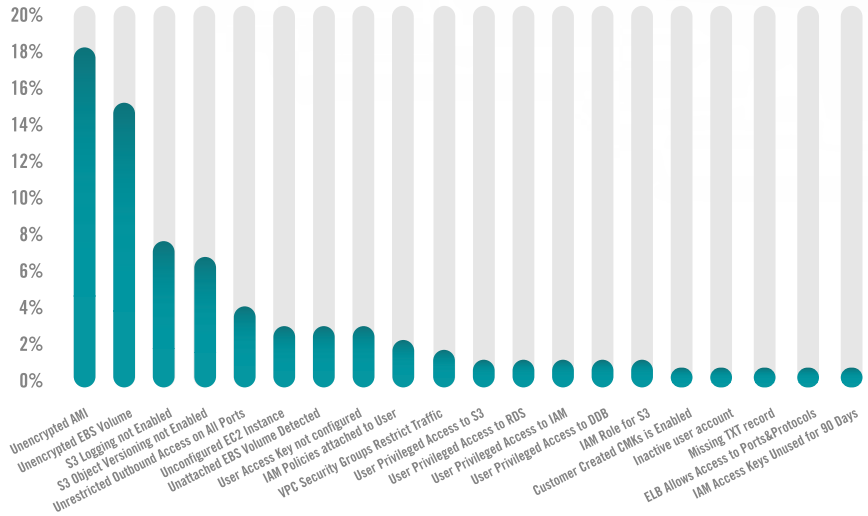
Top Security Issues for SMBs

TABLE 1



Top AWS SMB Configuration Issues

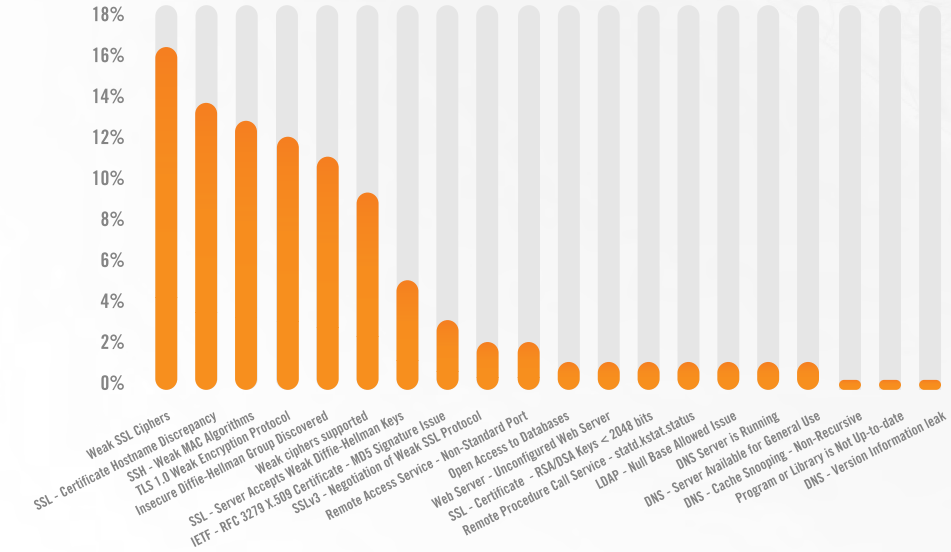
TABLE 2



THE DATA

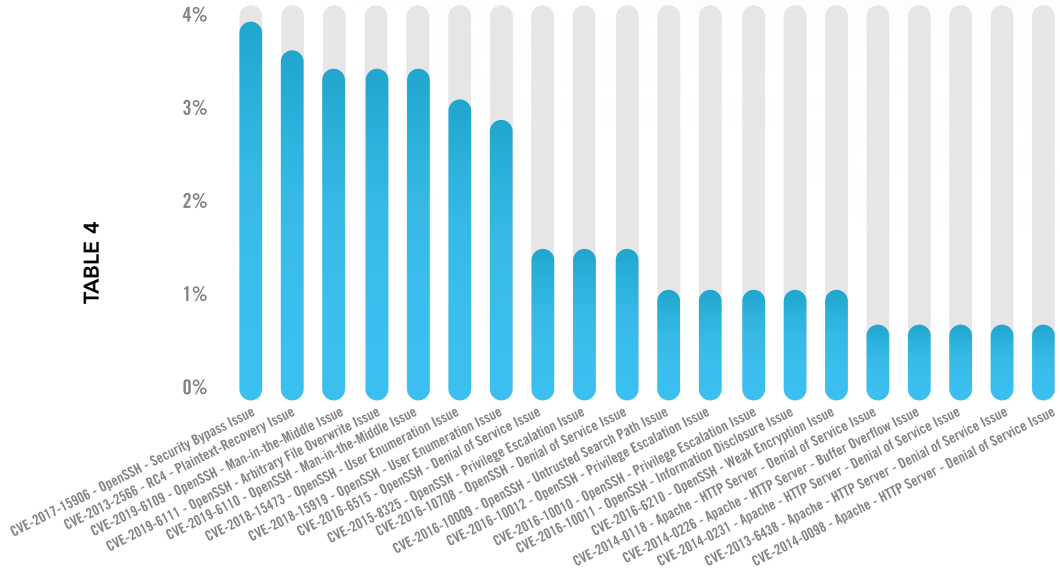
Top SMB Workload Configuration Issues

TABLE 3



Top Missing Patches

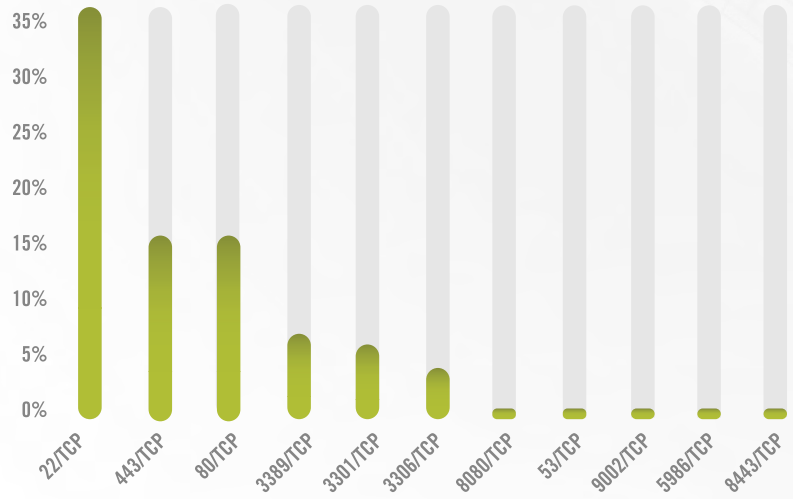
TABLE 4



THE DATA

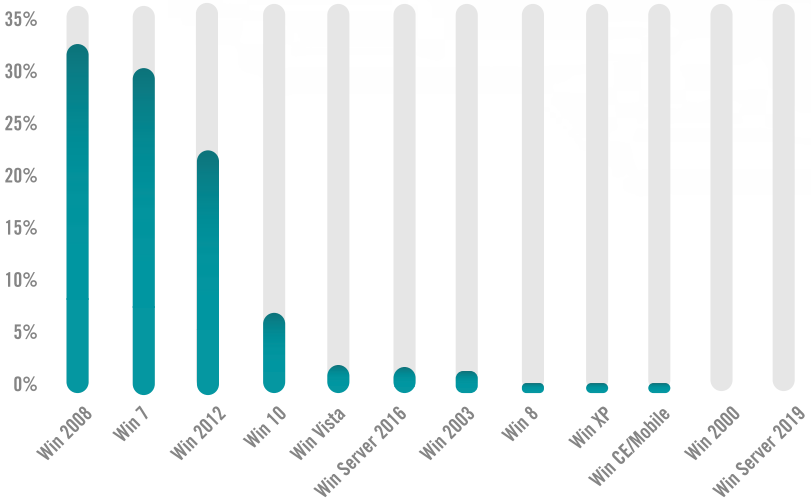
Top Vulnerable Ports

TABLE 5



Windows OS Distribution in SMBs

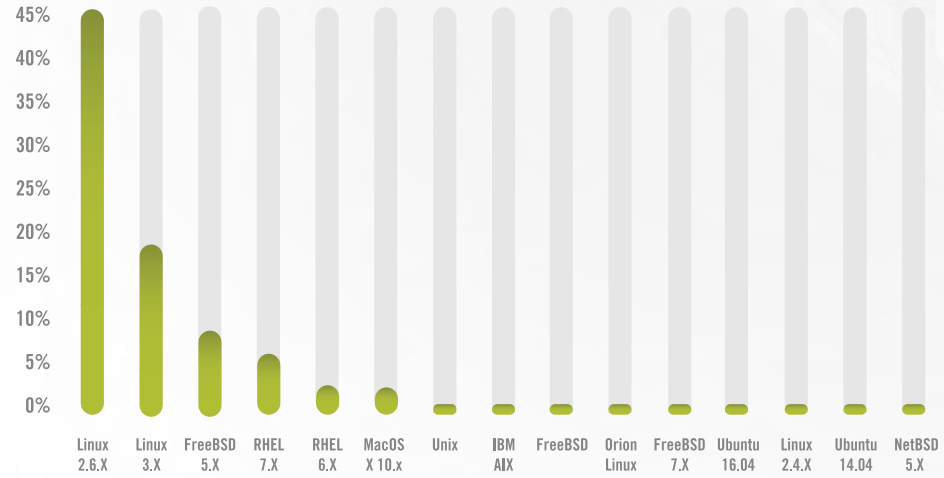
TABLE 6



THE DATA

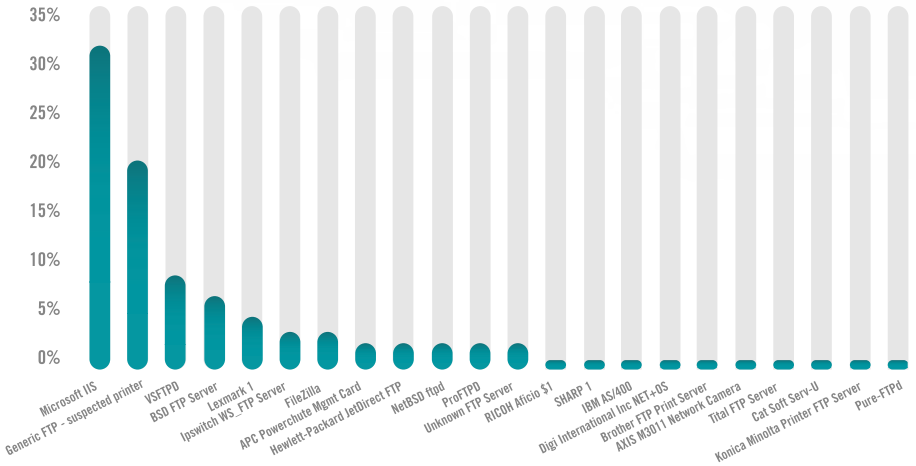
SMB Linux/Unix OS Distribution

TABLE 7



SMB FTP Server Distribution

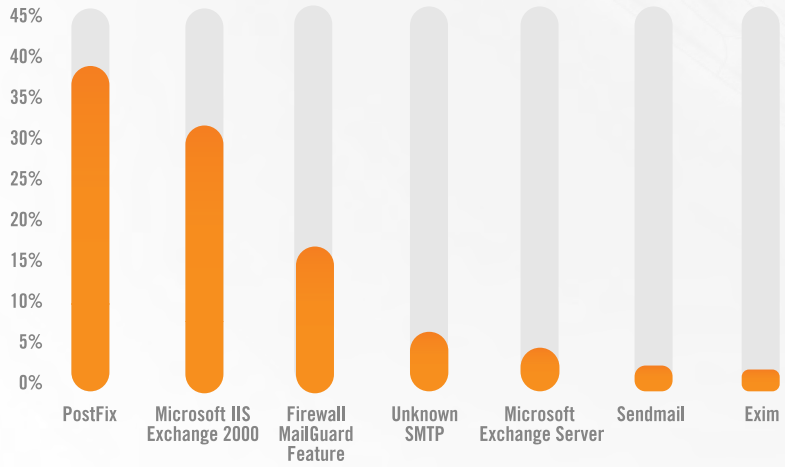
TABLE 8



THE DATA

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