A SANS Survey

# SANS Vulnerability Management Survey 2020

Written by **David Hazar**

November 2020

*Sponsored by:*

**Anomali**

Analyst Program

# Executive Summary

Vulnerability management is nothing new. In fact, it was one of the first IT security functions deployed by many organizations. Companies have been tracking vulnerabilities in their systems and third-party software since the late 1990s by adding them to the Common Vulnerabilities and Exposures (CVE) database maintained by MITRE. They have also had the ability to automatically identify vulnerabilities in their systems, software and even custom-developed applications by leveraging automated technology for around the same amount of time.

However, vulnerability *identification* does not equal vulnerability *management*. Although identification might satisfy compliance requirements for a time, eventually companies must progress from identifying vulnerabilities to remediating those vulnerabilities. That is where many organizations struggle. Large enterprises are often crippled by massive backlogs, numbering in the seven- to eight-figure range. This is obviously unacceptable, but it's what is making progress so difficult to achieve.

Fixing vulnerabilities is difficult for a number of reasons:

- We don't budget for it—and we don't have extra time or resources.
- Operational teams are already overworked.
- It never ends—even if we remediate everything, new vulnerabilities are constantly being discovered, and reports come in at different times and in different formats, depending on the tools or teams being leveraged for identification.
- It's a business expectation, but not a business requirement; therefore, the effort is not always recognized and rewarded.
- Security is accountable—but is not responsible—for much of the work.

In order to succeed with vulnerability management, it takes a coordinated effort among security, IT (both systems and software development) and the business operations groups. Organizations must also identify, acknowledge and track the roadblocks and the technical debt within the organization that are preventing timely remediation of vulnerabilities. It is not uncommon to find that well over 50% of outstanding vulnerabilities cannot be remediated due to issues that are extremely challenging to overcome and cannot be resolved with current operational budgets and resources.

In the 2020 Vulnerability Management Survey, we looked at the following:

- **Automated discovery techniques across a variety of asset types**
    - More than 70% of respondents' organizations are using automation to discover vulnerabilities.
    - Automated discovery for custom applications is lagging behind other asset types, with only 40% of respondents including this asset type in their vulnerability management (VM) program and only 42% of those performing automated identification.

- **Maturity of remediation techniques across a variety of asset types**
  - Most organizations rank themselves as very mature or mature at patching for the operating system and other server software or middleware. Still, many organizations struggle with non-business client-side third-party software, non-standard asset types (ICS/IoT/embedded), mobile endpoints and business partner environments.
  - Approximately 80% of organizations consider themselves very mature or mature at managing configurations for more common asset types (e.g., operating systems, third-party software, network devices), but ICS/IoT/embedded assets are lagging behind, as are mobile endpoints and business partner environments.
- **Vulnerability prioritization techniques**
  - Almost 82% of respondents' organizations are prioritizing vulnerabilities. While nearly 78% are using CVSS severity, more than 66% are including asset value and 73% consider exploitability to go beyond severity and follow a more risk-based approach to prioritization.
- **Remediation deadlines/timelines**
  - Of those respondents' organizations prioritizing vulnerabilities, 75% are using risk level and remediation timelines to focus remediation efforts.
  - Just over 42% of organizations have tailored their remediation timelines based on asset type.
- **Roles and responsibilities for VM tasks**
  - Security is responsible for the overall vulnerability management for 74% of respondents.
  - IT takes the lead for infrastructure vulnerability discovery and patch and configuration management, at 46%.

We did not focus on manual identification techniques including penetration testing, red teaming, bug bounties, and other options in this survey.

Some of the key findings and takeaways from the survey include:

- An increase in both cloud and container infrastructure VM requirements and capabilities over levels reported in 2019[1]
- A disconnect in the understanding of the cloud shared responsibility model for infrastructure-as-a-service (IaaS), with nearly 22% of respondents claiming the cloud provider is responsible for vulnerability management
- Lack of involvement of audit, risk and compliance in traditional VM (2% for infrastructure, 2% for custom-developed applications) but slightly more involvement when it comes to the cloud (4%) and third-party or open source software (8%)
- Ignoring of application security and application vulnerability management (only 40% include in VM program) or relying solely on manual identification techniques (only 42% of those that include it use automation)
- The prioritization of vulnerabilities based on either severity or risk by most organizations
- Lack of confidence by many organizations in the maturity of their patch and configuration management capabilities, especially for certain asset types

[1] "SANS Vulnerability Management Survey," April 2019, www.sans.org/reading-room/whitepapers/analyst/vulnerability-management-survey-38900 [Registration required.]

## Survey Demographics

Because we conducted a similar vulnerability management survey in 2019,[2] we also analyzed some of the changes to determine what progress has been made and identify some of the year-over-year differences.

Similar to last year, the majority of respondents came from organizations headquartered in North America, followed by Europe and Asia. The survey results show a global presence—at least one-third of the respondents' organizations have operations in the United States, Europe and Asia, and close to a quarter maintain operations in Canada and Australia/New Zealand. The industries largely mirrored 2019 with financial services, government, IT consulting, healthcare and education providing the greatest participation. Cloud services made some gains, which is not surprising, but some of that could have come from some telecommunications companies rebranding themselves as cloud services. There was also a good mix of small versus medium-to-large organizations, with an almost 50/50 split between those with less than 5,000 employees and those with more than 5,000 (see Figure 1).

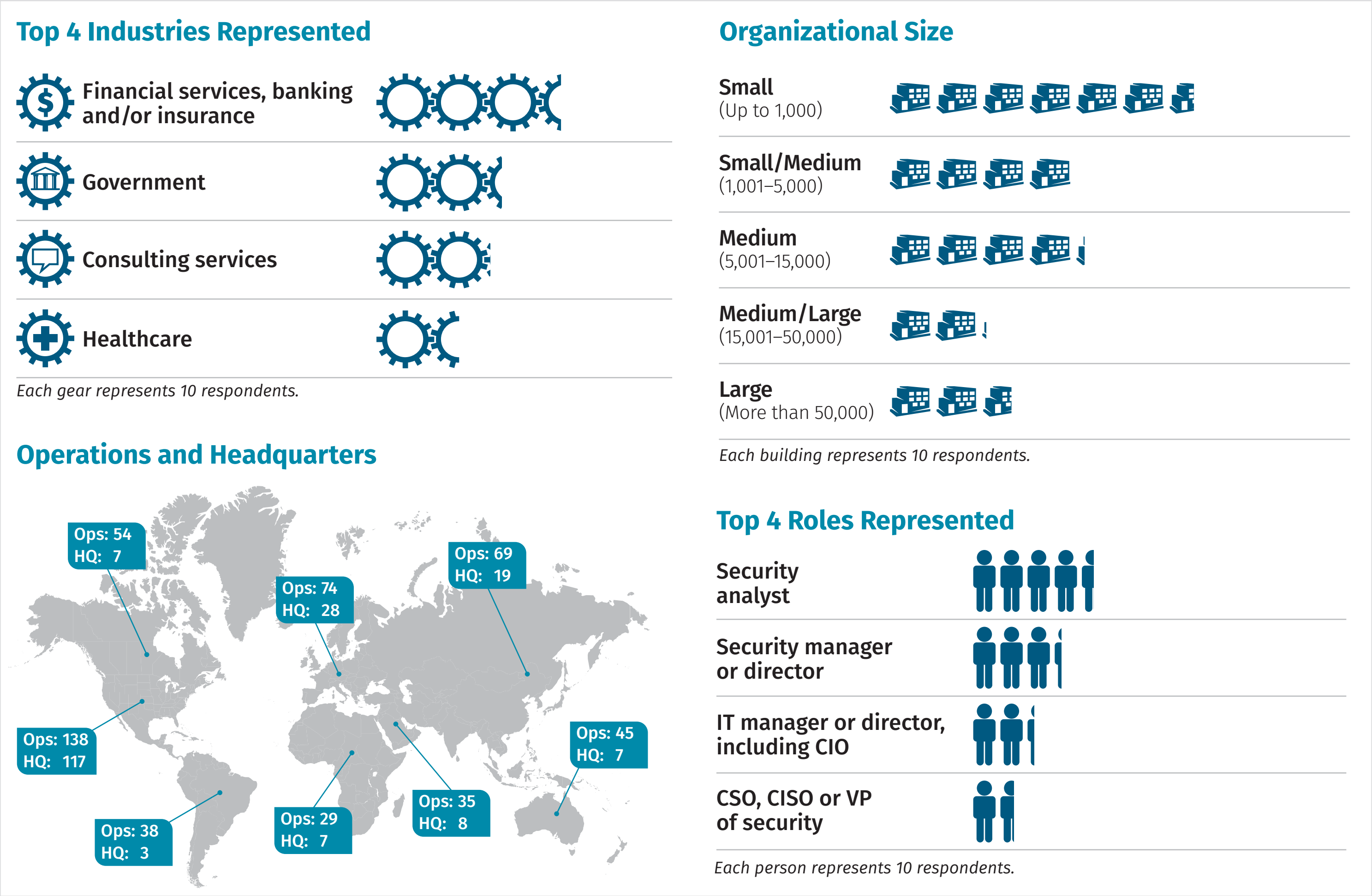


*Figure 1. Key Demographic Information*

[2] "SANS Vulnerability Management Survey," April 2019, www.sans.org/reading-room/whitepapers/analyst/vulnerability-management-survey-38900 [Registration required.]

# Setting the Stage

It was promising to see that the percentage of respondents' organizations that have formal programs managed either internally (61%) or through a third party (2%) is up more than eight percentage points from last year. The majority of those that do not have a formal program are still informally managing their vulnerabilities (24%) in some fashion, while others have plans to formalize a program in the next 12 months (11%). See Figure 2.

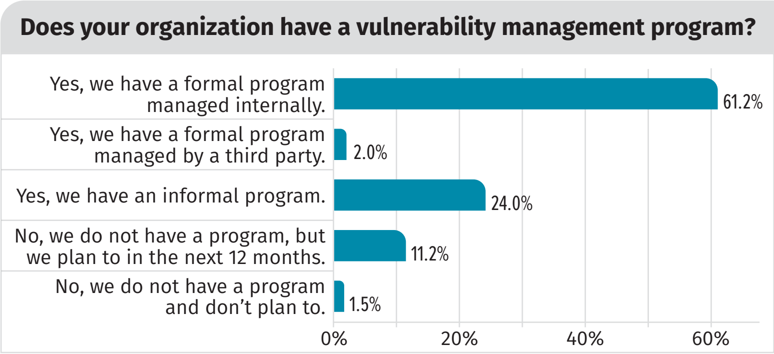


*Figure 2. Formal vs. Informal Programs*

These results indicate that 87% of organizations at least have some processes in place to identify or manage their vulnerabilities. As expected, the larger the organization, the more likely it is to have a formal program (see Table 1). The industries most likely to have a formal program are financial services and government.

**Formal vs. Informal Vulnerability Management Programs by Organization Size**

| | Total | <100 | 101–500 | 501–1,000 | 1,001–2,000 | 2,001–5,000 | 5,001–10,000 | 10,001–15,000 | 15,001–50,000 | 50,001–100,000 | >100,000 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Total count** | **197** | **26** | **26** | **14** | **15** | **25** | **25** | **17** | **21** | **13** | **15** |
| Yes, we have a formal program managed internally. | 121 | 9 | 15 | 6 | 8 | 11 | 13 | 12 | 18 | 13 | 15 |
| Yes, we have a formal program managed by a third party. | 4 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| Yes, we have an informal program. | 47 | 8 | 8 | 6 | 6 | 8 | 4 | 4 | 3 | 0 | 0 |
| No, we do not have a program, but we plan to in the next 12 months. | 22 | 7 | 2 | 2 | 0 | 5 | 6 | 0 | 0 | 0 | 0 |
| No, we do not have a program and don't plan to. | 3 | 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

*Table 1. Formal vs. Informal Programs by Size*

We asked respondents to identify the specific types of assets that were included in their vulnerability management program. Options included traditional infrastructure, cloud IaaS, custom applications, cloud SaaS, third-party/open source applications, container infrastructure, cloud platform-as-a-service (PaaS) and IoT/embedded/ICS. Not surprisingly, infrastructure is still the main focus, with on-premises infrastructure being included by nearly all the organizations and cloud IaaS coming in second. See Figure 3.

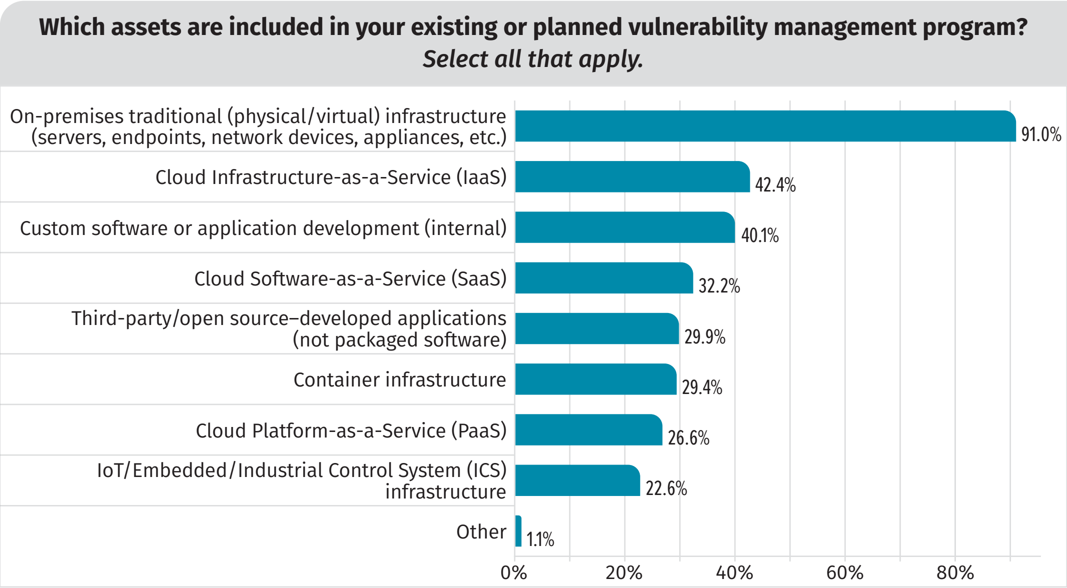


*Figure 3. Vulnerability Management Program Assets*

Reviewing the 2020 results against those from 2019, it appears that the biggest increases to the assets in the formal VM program were in the cloud and container infrastructure categories. Intuitively, these additions make sense because more companies are moving to the cloud. Containers are continuing to gain traction with the addition of more robust orchestration and operational tooling and more mature security offerings in the space as well.

## Responsibility for Vulnerability Management Programs

Information security is still the most common group within organizations assigned responsibility for overall vulnerability management (74%), but respondents indicated that a lot of responsibility is placed on IT organizations for remediation activities such as patch (67%) and configuration management (69%), as illustrated in Figure 4. It is interesting that a higher number of respondents in manufacturing and retail indicated that the overall vulnerability management was more of an IT responsibility. Audit, risk, compliance and third parties are not heavily involved in vulnerability management these days but are more involved in the processes associated with cloud assets and third-party or open source software. Most likely this involvement stems from heavier involvement in the procurement process and additional focus on the cloud due to its ever increasing popularity and complexity.

Although 71% of respondents' organizations perform automated vulnerability discovery for their asset types, that does not ensure that all assets in a given category are subject to automated scanning. In fact, only 94% of the organizations include traditional infrastructure as part of their program while still using automation in some capacity for vulnerability discovery across other asset types. Some organizations reported even lower percentages for other asset types, with some types closer to 50%.

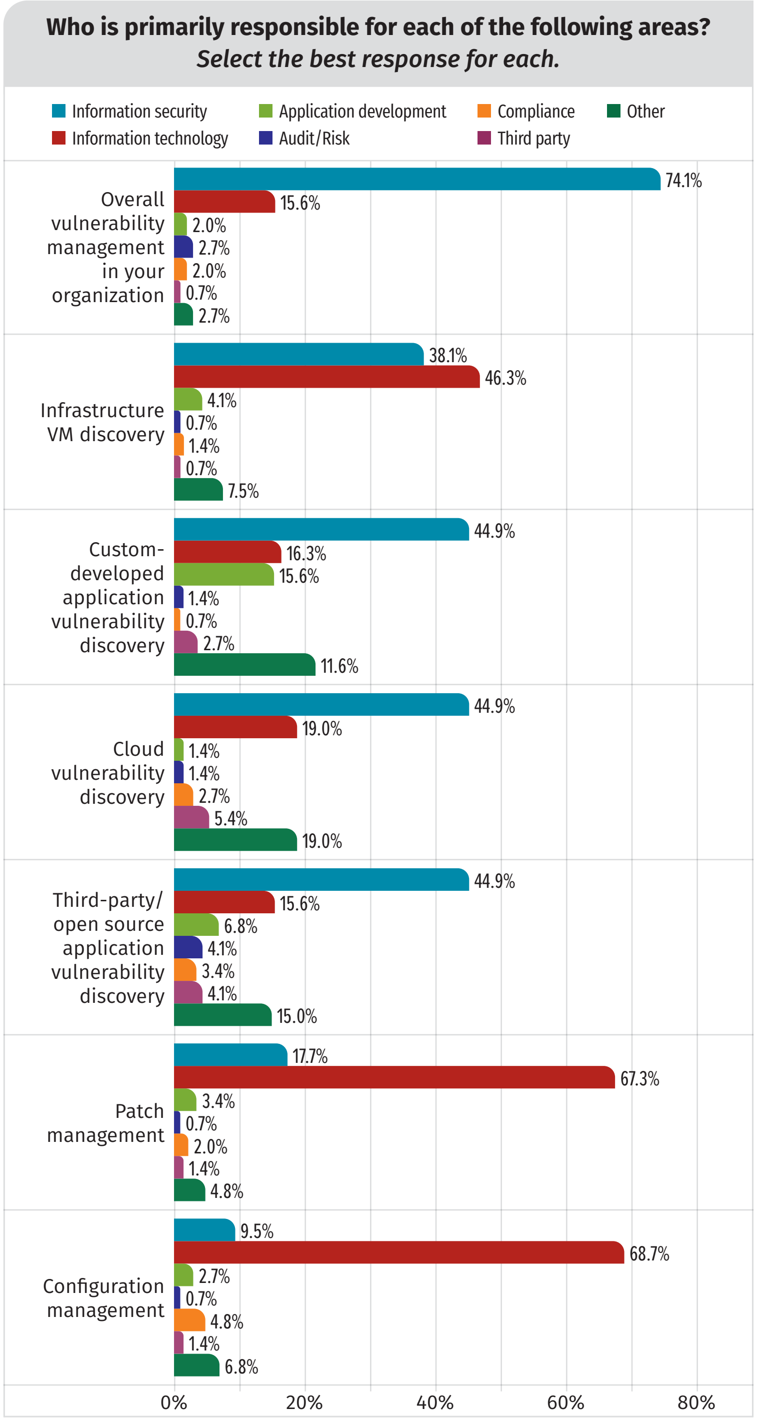


*Figure 4. Primary Responsibility*

Newer types of assets lend themselves to higher levels of automation from the start. While cloud IaaS assets are included by only 42% of the respondents using automation, around 88% of respondents are using automated scanning for these assets. See Figure 5.

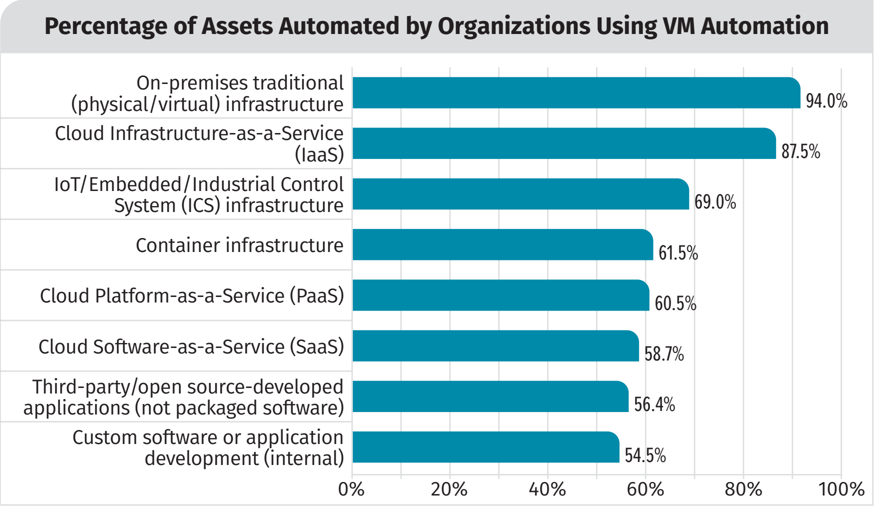


*Figure 5. Automated Discovery by Asset Type*

The higher numbers for IoT/embedded/ICS systems might be due to the fact that many organizations are using their traditional infrastructure scanning technologies in this space. Although the lower percentages for some of these asset types is somewhat surprising, it is important to recognize that organizations could still be using manual forms of identification and relying on patch and configuration management tools to notify them of outdated software or insecure configurations.

## Identification

While identification is only a part of the overall vulnerability management effort and not a solution to the problem, it is still an important mechanism to quantify the risk associated with vulnerabilities present in organizational environments. Moreover, it provides data to help security personnel understand their organization-specific challenges and roadblocks, as well as garner support to make meaningful change. Let's take a deeper look at how respondents reported their organizations are identifying vulnerabilities.

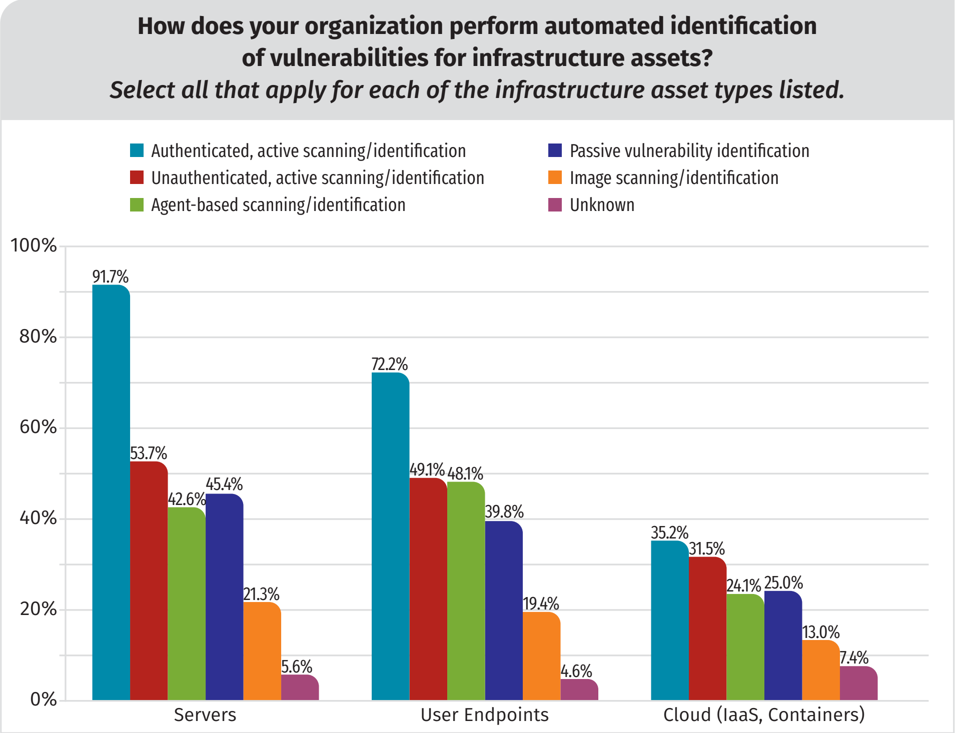


*Figure 6. Methods of Automated Vulnerability Identification*

Organizations performing automated identification are using a variety of techniques. While authenticated scanning is by far the most utilized technique for servers and end user devices, there is good traction across other scan types as well. Currently, the least utilized methodology is image scanning, but that will most likely continue to grow as more organizations move to the cloud and implement containerized infrastructures, which will allow for more immutable approaches to architecture and design. See Figure 6.

We were surprised to find that there weren’t higher percentages of agent-based scanning for end user and cloud infrastructures. With the transition to a primarily remote workforce for many companies—and with cloud providers offering free or native agent scanning capabilities—adoption should be more widespread. However, these changes to operating models and capabilities may be too recent. We may have to wait for future survey results to see the impact. Nearly 50% of organizations are using agents in some capacity, so the number is not insignificant, but it wouldn’t be surprising if the numbers were much higher for end user and cloud assets in subsequent surveys. Image scanning is another technique that was lower than expected for cloud assets. This may indicate that organizations have taken a more “lift-and-shift” approach to their cloud migrations.

An *immutable infrastructure* is one in which no changes are made to a server, container or operational environment once it is deployed. If changes are required, a new one infrastructure is deployed with the changes included and the old server, container or operational environment is destroyed.

For organizations that are automatically identifying vulnerabilities in their custom-developed applications—which is only about 19% of the respondents—static application security testing is the most common technique leveraged. The number of these respondents performing software composition analysis was only 21%, which seems disproportionately low. The number of unknown answers, at slightly more than 34%, is also surprising and might reflect that application vulnerability management or application security is sometimes handled by a different group than the one that handles infrastructure vulnerability management. See Figure 7.

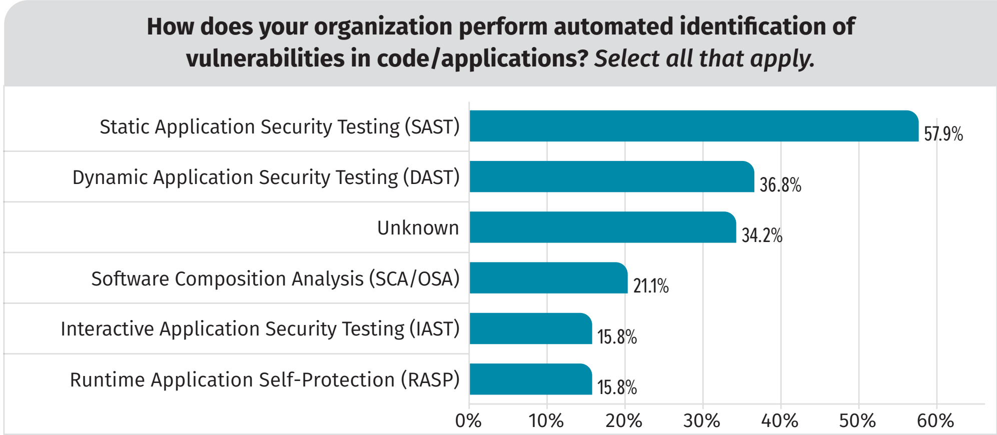

**How does your organization perform automated identification of vulnerabilities in code/applications?** ***Select all that apply.***

*Figure 7. Automated Vulnerability Identification in Code/Applications*

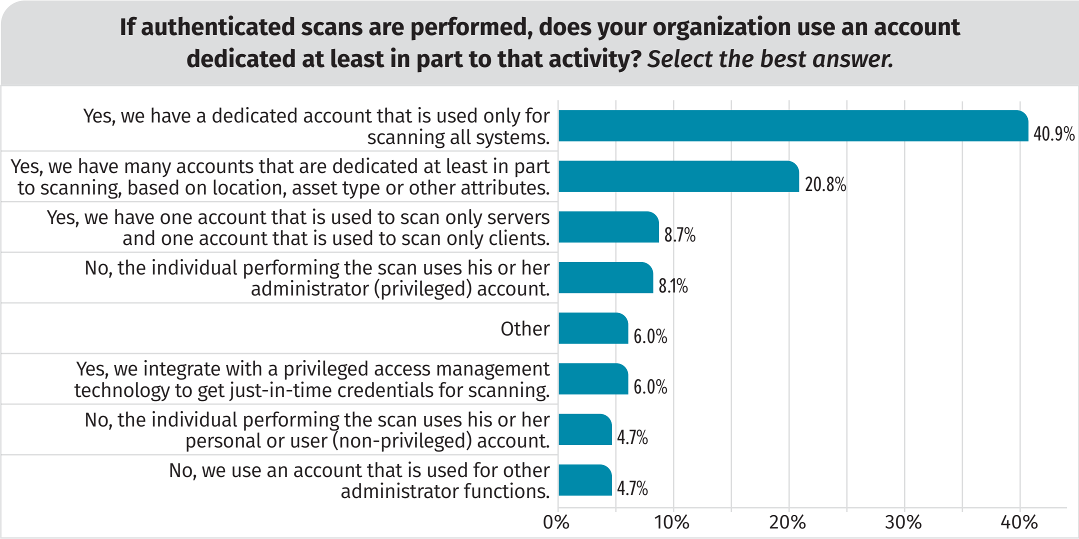
As increasingly more development frameworks provide standard or third-party frameworks for common tasks, much less code is written in-house. For example, some estimate that more than 90%[3] of code in **Node.js** applications is actually written by third parties. A 2017 survey conducted by npm found that, while 97% of the developers responding to the survey use open source software, 77% of those were concerned about the security of these libraries.[4] It will be interesting to see if there is an increase in the percentage of organizations leveraging software component or dependency analysis moving forward.

The other interesting statistic related to applications is that about 16% of these respondents leverage Runtime Application Self-Protection (RASP). There has been quite a bit of buzz about this newer assessment and defense technology. Perhaps the benefit of being able to potentially protect against unknown risks in applications is overriding the performance and stability concerns some have had with coupling the RASP technology to the application runtime.

[3,4] “Attitudes to security in the JavaScript community,” https://medium.com/npm-inc/security-in-the-js-community-4bac032e553b

Not surprisingly, most organizations (76%) are relying on updates from tool vendors to support the latest vulnerability signatures. A smaller percentage leverage free or public use updates or custom signatures. Depending on the asset category, between 37% and 69% of organizations scan with all the available/applicable rules enabled. The bulk of the remaining respondents either use customized rules for scanning or are unsure of their process.

Of those utilizing authenticated scanning, almost 77% of scanning takes place with an account dedicated, at least in part, to scanning, and 41% use a single dedicated account (see Figure 8). For infrastructure scanning, IT teams are responsible for managing and running the identification infrastructure more often than security, but for custom applications, cloud and third-party or open source infrastructures, the opposite is true.



**If authenticated scans are performed, does your organization use an account dedicated at least in part to that activity?** ***Select the best answer.***

*Figure 8. Authenticated Scan Account Types*

## Analysis and Communication

Almost 82% of respondents have some way to rate their vulnerabilities based on risk, and another 10% are investigating ways to do so. Of those prioritizing their vulnerabilities, 76% of respondents know that their organization is leveraging risk ratings or other prioritization factors for remediation. This is not surprising, given all of the discussion surrounding vulnerability prioritization these days. There seems to be an entire secondary market for technology to help organizations gauge the risk associated with each of their vulnerabilities and prioritize them accordingly.

Respondents' organizations use a variety of factors to assess and assign risk to each vulnerability, with the Common Vulnerability Scoring System (CVSS) severity (78%), exploitability (73%), and the importance of the asset to the business (66%) garnering the top responses. These are definitely useful attributes that should be used to prioritize vulnerabilities, but for the vulnerabilities that cannot easily be remediated in the organization, focusing on the most common solutions or remediation actions (21%) might be more useful (see Figure 9 on the next page).

Prioritization is no doubt an important part of vulnerability management. However, many times it ignores some fundamental issues in the organization that prevent teams from resolving large groups of vulnerabilities. In many situations, there is some roadblock to remediation, such as some legacy piece of software or hardware being leveraged by an existing business process. Other times, it could be applications that are no longer adequately supported by the business. Organizations must first identify and acknowledge all the blockers, then prioritize what's left.

Let's look at an example of how looking at common solutions or remediation actions can provide more insight into vulnerabilities that organizations are struggling to remediate. There are many CVE entries or vulnerabilities associated with Adobe Flash and the Java Runtime. However, sometimes these vulnerabilities are not fixed by updating Adobe Flash or the Java Runtime on the system. Figure 10 is a mockup of what a report might look like when it is grouped by remediation action or solution.

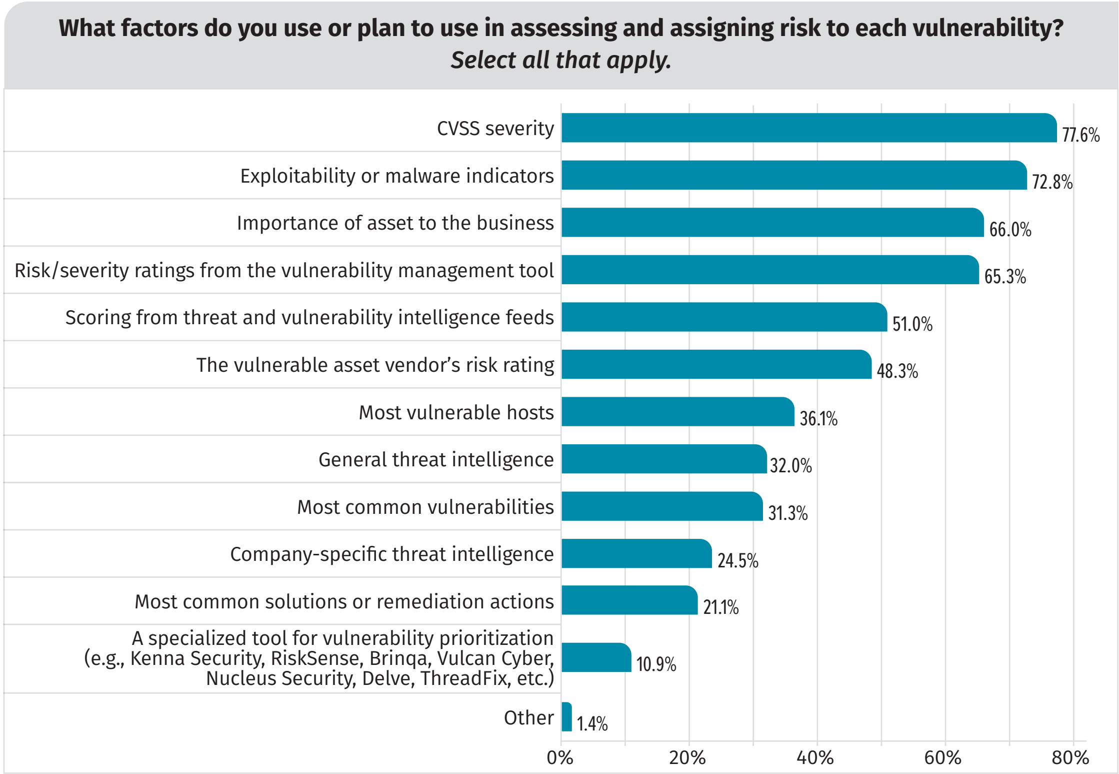


*Figure 9. Assessing and Assigning Risk Factors*

Based on this data, it would be easy to assume that the organization is struggling to update Flash. In reality, Flash might not be the cause of these vulnerabilities—at least not directly. After some conversations with the systems administrators and engineers, you might determine that the real culprit is Google Chrome. Due to specific business requirements, the organization might be running and supporting an old version of Google Chrome. Google Chrome bundles Adobe Flash, and for every reported Google Chrome vulnerability there might be two or three vulnerabilities associated with the bundled version of Adobe Flash. While the report initially led us down the wrong path, it typically doesn't take long to get to the root cause.

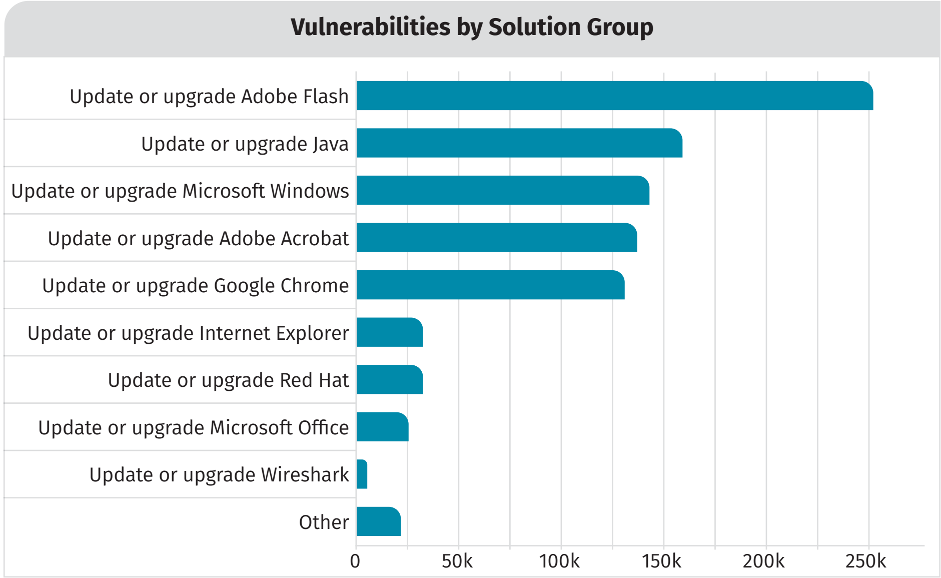


*Figure 10. Remediation Action/ Solution Report Example*

We have seen this scenario play out with numerous organizations with a variety of software packages. The solution is not always easy and straightforward. These situations usually require special projects, or at least increased focus, effort and funding. Once these more systemic issues or roadblocks are identified, the risk needs to be escalated to the right level. Too often, security and IT are aware of the problem but have not shared it elsewhere. Prioritization works only for the vulnerabilities that don't have these issues or exceptions.

When looking at remediation deadlines within organizations, 42% of organizations have deadlines that differ by asset type, whereas 36% have the same deadlines and 22% don't know if differentiated deadlines exist. See Figure 11.

Organizations might need to treat custom application vulnerabilities differently than infrastructure vulnerabilities because, for infrastructure vulnerabilities, security teams are not responsible for creating the patch, configuration guidance or workaround. Except for zero-day vulnerabilities, patch or configuration guidance is already available. For custom applications, teams must create, test and deploy the fix. There may even be a case for different treatment timelines based on the development or engineering team's release cycle. If they are developing and releasing changes daily or weekly, the timelines can be much shorter than if they release changes monthly, quarterly or semi-annually. Whatever timelines your organization sets, they should always be based on what is achievable for each asset type.

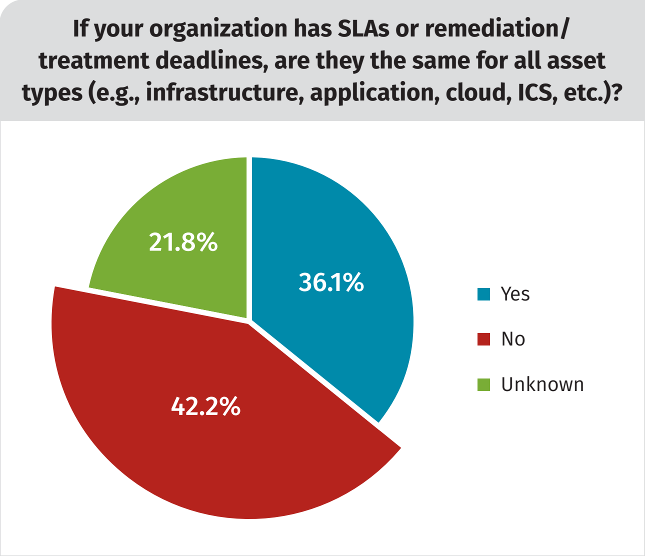


*Figure 11. Remediation/ Treatment Deadlines by Asset*

Organizations use a variety of reporting approaches. It is encouraging that 50% are creating targeted or owner/platform-based reports or dashboards. This can be extremely effective as long as organizations exclude vulnerabilities they cannot currently remediate, although they can still include them in program-level reports. Meetings or conference calls serve as the communication vehicle for vulnerability data for 43% of the respondents' organizations, with 41% creating tickets for groups of vulnerabilities that can be assigned to the responsible party, 40% having general vulnerability dashboards and reports, and 39% emailing reports to the responsible party. See Figure 12.

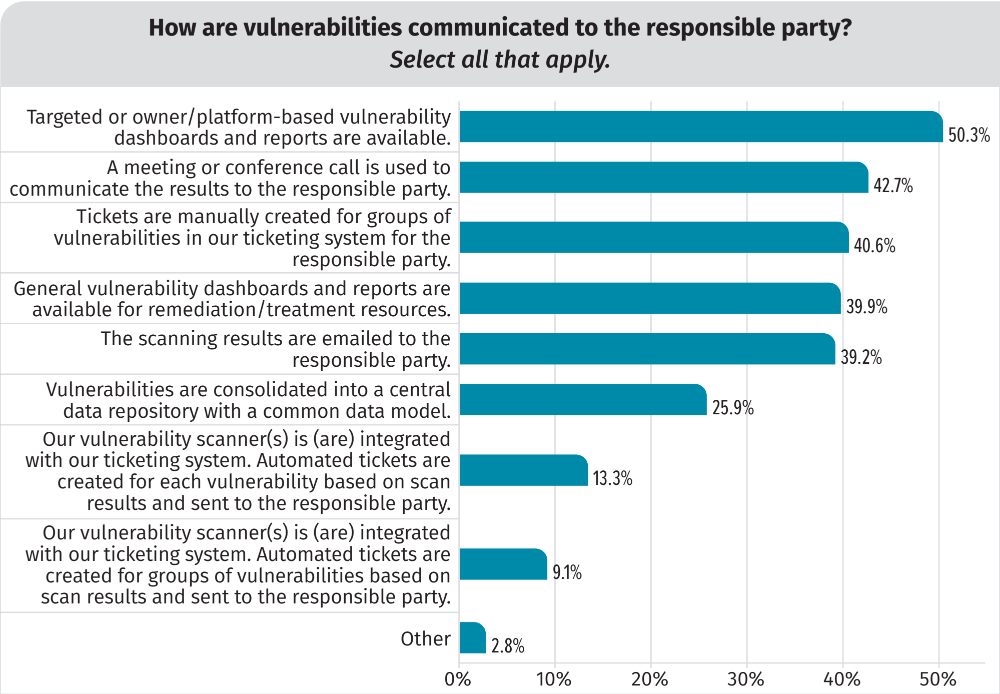


*Figure 12. Vulnerability Reporting Methods*

Analysis and communication can have a huge impact on the effectiveness of the vulnerability management program and the willingness of remediation teams to engage. This is a huge differentiator between organizations that are making good progress and those that continue to struggle. If organizations can reduce the amount of work for these teams by analyzing the data coming from the identification tools and ensuring the teams get credit for the work they are performing—even though it may not be one of their primary responsibilities—it helps improve buy-in and encourages participation.

## Remediation

The ultimate goal of identification, analysis and communication is to drive remediation and reduce the number of vulnerabilities in the organization, which decreases risk. Patch management and configuration management are two key high-level categories of remediation activity. Survey respondents appear to struggle with both as related to non-server assets (IoT, ICS, mobile) and business partners. See Figures 13 and 14 for how respondents consider the maturity of their processes.

Even though respondents were most comfortable with the maturity of patching operating systems, only 50% of respondents overall were confident enough to say their organization was "Very Mature" for patch management and 60% for configuration management.

The maturity estimations for both patch and configuration management lead us to believe that there is still room for improvement at most organizations. We also predict that IoT and other non-server assets will continue to be a struggle for many organizations until better technology exists to support these assets or more resources are directed toward efforts to replace outdated, unsupported or legacy equipment.

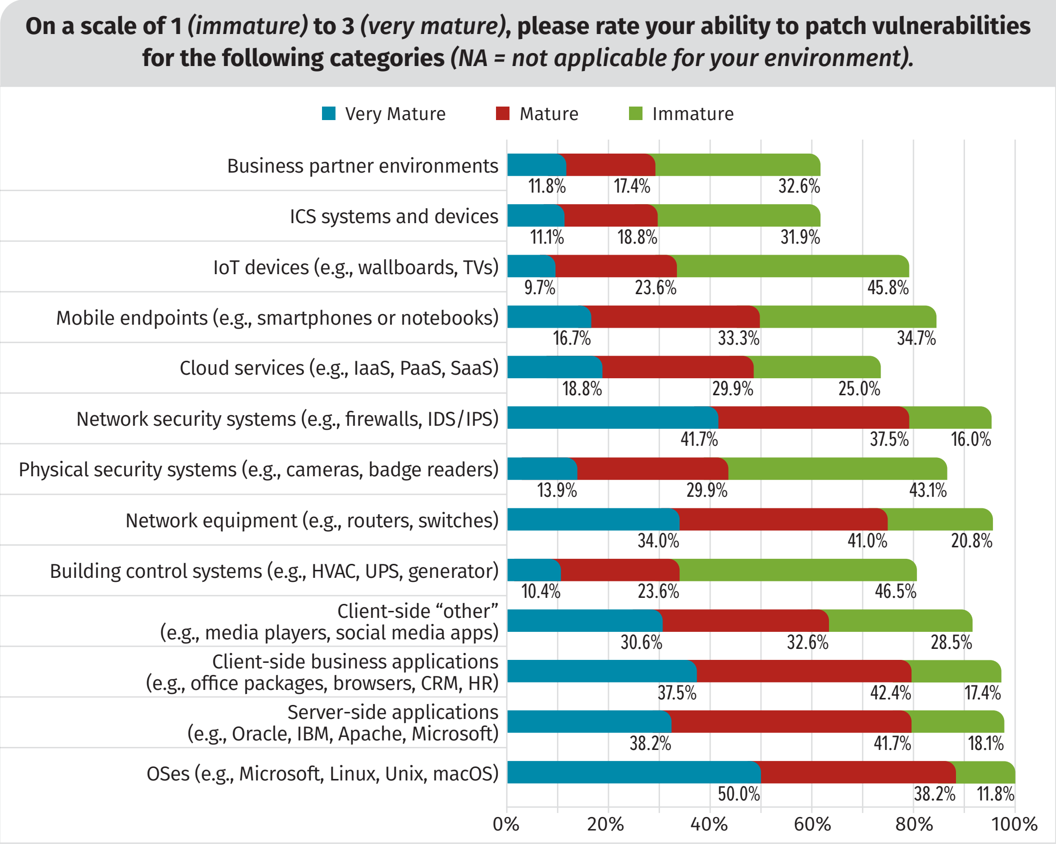

**On a scale of 1 *(immature)* to 3 *(very mature)*, please rate your ability to patch vulnerabilities for the following categories *(NA = not applicable for your environment).***

*Figure 13. Patching Maturity*

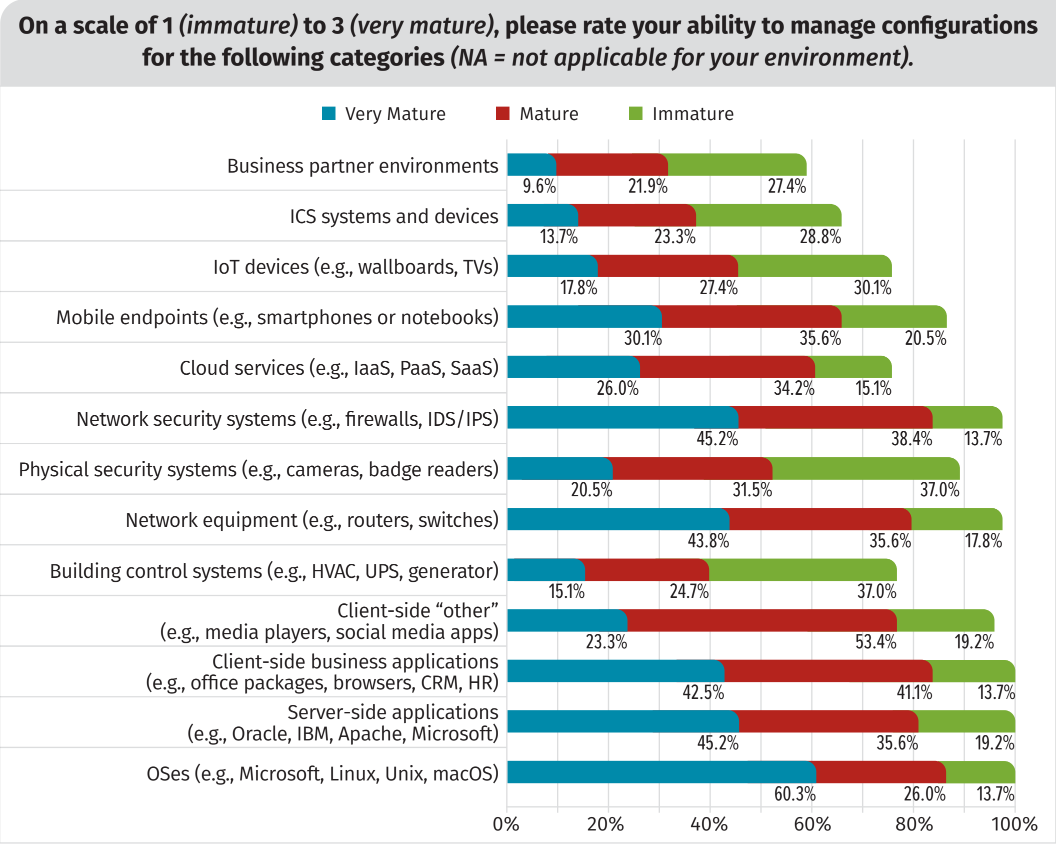

**On a scale of 1 *(immature)* to 3 *(very mature)*, please rate your ability to manage configurations for the following categories *(NA = not applicable for your environment).***

*Figure 14. Configuration Management Maturity*

## Vulnerability Management in the Cloud

Vulnerability management in the cloud, like most things cloud, is constantly evolving. It is a little disconcerting that almost 22% of the respondents do not know what is being done to identify vulnerabilities in their cloud IaaS infrastructure or believe the cloud provider is responsible. While it might be somewhat true that the provider is responsible for cloud PaaS and SaaS, it is definitely not the case for IaaS. The cloud provider is responsible only for physical security, hardware security, the security of the virtualization platform and all the related software-defined components and services provided to the customer. The customer is responsible for everything from the operating system on up and for the configuration of some of the related software-defined components and services.

Only about 18% of respondents automatically scan for vulnerabilities or misconfigurations in their cloud PaaS environments, whereas only 22% do so in cloud SaaS environments. This could be due, in part, to the semantics of using the term *automated vulnerability scanning* to describe this scanning activity as opposed to cloud security scanning or automated identification of cloud misconfigurations. Nonetheless, it is important for organizations to take advantage of the options available for assessing these types of assets. Sure, there are plenty of commercial vendors that offer cloud security solutions, but there are also many cloud-native options and even free and open source capabilities available (e.g., Cloud Custodian, CloudMapper, Cartography, various CIS Benchmark scanning tools).

The lack of awareness regarding what is being done to identify vulnerabilities in the cloud and low scan rates for PaaS and SaaS highlight a problem with the cloud and cloud security in general. The shared responsibility model can lead to confusion about roles and responsibilities—and this confusion can lead to gaps. However, when properly understood, the shared responsibility model can offload much of the VM problem to the cloud provider, allowing organizations to focus on the remaining assets that they might not yet feel comfortable running in the cloud.

To help others better understand the shared responsibility model, think about different types of living arrangements. Traditional non-cloud operating environments are like owning a home. The owner is responsible for everything. Cloud IaaS can be likened to owning a townhome or condo in a gated community with guards. The exterior and physical security are mostly taken care of. The owner must still lock the front door, but there is someone helping keep some of the bad stuff out and maintaining everything outside the home. However, all interior maintenance is still the owner's responsibility. With IaaS, organizations still must patch, configure and fix the operating systems, software and applications running on the virtual infrastructure provided and maintained by the cloud provider.

If organizations want even less responsibility, they can choose cloud PaaS. This is like renting an apartment. Renters can hang some things on the wall, furnish it, buy groceries and so on, but the renter is not responsible for the structure itself. Finally, cloud SaaS is like paying for a hotel suite: Almost everything is provided—the guest can customize it a bit, but there are typically quite a few restrictions. This model doesn't quite free the guest from responsibility. A guest is still accountable for who he or she lets into the suite (**`AuthN`**/**`AuthZ`**) and for securing any valuables (data) they bring with them.

There are a variety of different depictions and explanations of the shared responsibility model out there, but they are not granular enough to answer all questions and remove all doubt. If there is ever a doubt about who is responsible, it is best to reach out to the provider and ask for clarification. This can help avoid any gaps in coverage.

Another interesting trend in the cloud not completely supported by the survey results is the move toward agent-based identification. Amazon Web Services (AWS) offers its cloud-native, agent-based scanning technology called Amazon Inspector, and Microsoft Azure offers the Qualys Cloud Agent for free with standard Azure virtual machines and higher if you have Azure Defender enabled. Due to the more ephemeral nature of resources in the cloud, we envision agent usage for cloud IaaS increasing in the next few years. However, these gains could be offset by a shift toward containers or other immutable infrastructure design patterns and PaaS offerings.

## Vulnerability Management for Non-Traditional Infrastructure

Although not all the assets included in this category are new, the reality is that VM programs have historically been more focused on or successful with traditional server and client systems with non-embedded operating systems. As new asset types have emerged and threats have increased for other asset types, more types of assets are being included in the program.

As mentioned in the section on remediation, many organizations struggle to patch and configure non-traditional systems. In many cases, vulnerability identification can also be (or may become) a struggle. More traditional identification techniques such as active scanning or agent-based scanning might not be as effective for these types of assets. There may also be concerns about stability for industrial control systems and older embedded systems that prevent organizations from performing active scanning. This is why passive scanning was added to the list of identification capabilities surveyed this year. We think these asset types and an uptick in IPv6 utilization (due in part to IoT) are big contributing factors to the adoption of passive scanning. See Figures 15 and 16 on the next page.

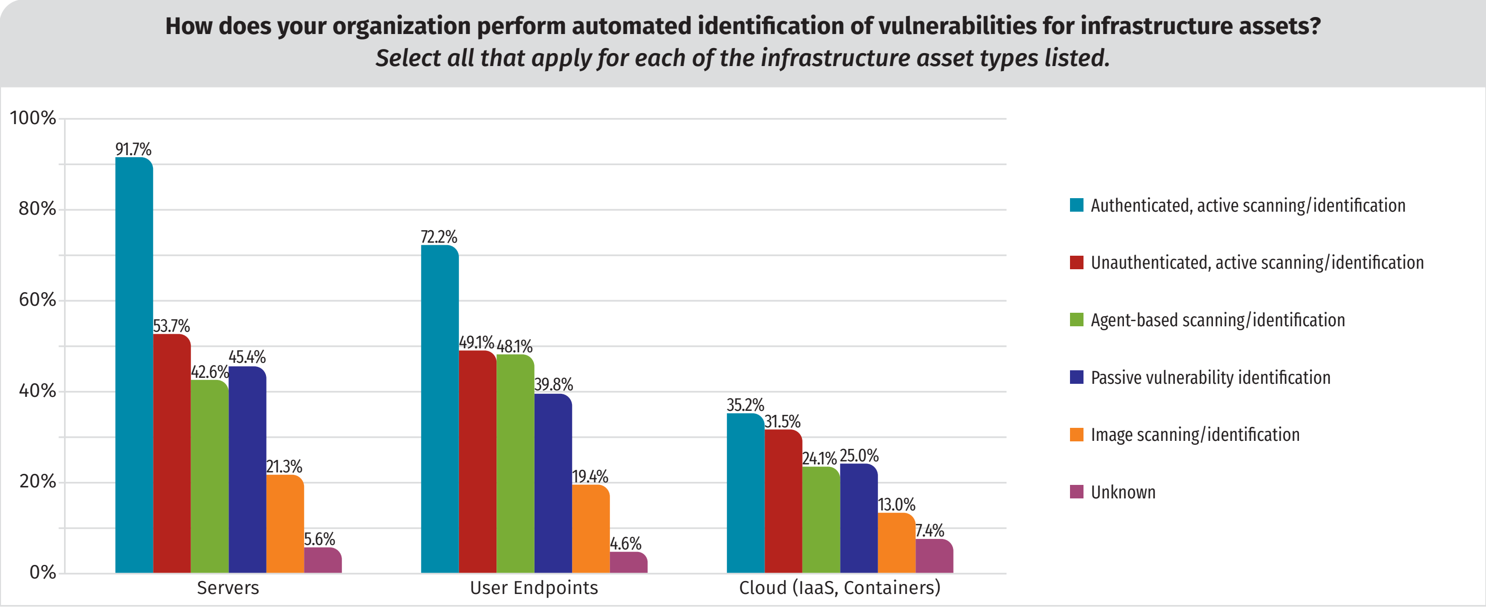

**How does your organization perform automated identification of vulnerabilities for infrastructure assets?** *Select all that apply for each of the infrastructure asset types listed.*

*Figure 15. Performing Automated Vulnerability Identification for Infrastructure Assets*

Another difficulty with IoT/embedded/ICS assets is that remediation is more dependent on vendor updates, which are not always offered and/or may not be backward-compatible with the use case. In addition to ensuring these devices are set to be updated when updates are available, organizations must practice better asset life-cycle management and work more closely with vendors to understand when products will reach the end of support or end of life. That way, they can better plan for replacements, if available, and start evaluating risk and compensating controls if they are not available.

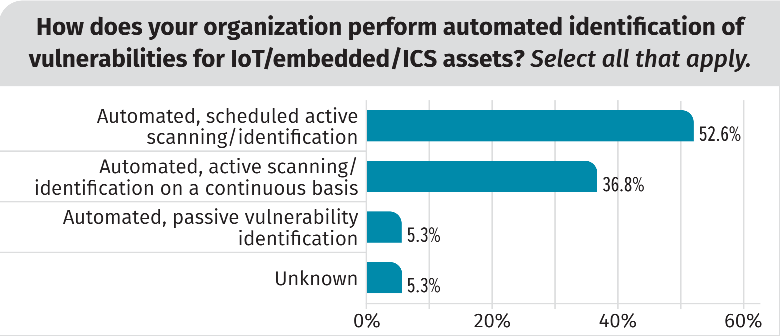

**How does your organization perform automated identification of vulnerabilities for IoT/embedded/ICS assets?** ***Select all that apply.***

*Figure 16. Performing Automated Vulnerability Identification for IoT/Embedded/ICS Assets*

## Vulnerability Management for Applications

For custom-developed applications, vulnerability management can be a struggle. Potentially contributing to the problem is the fact that many security organizations are much more familiar with infrastructure engineering and systems management than they are with secure coding and application development. Combine this with the fact that only 40% of respondents include custom software and applications as part of their VM program, less than 55% perform automated scanning, and the most common automated scanning technology is static application security testing (which frequently results in a false-positive rate of greater than 50%), and some of the reasons for this struggle become quite evident. Review Figure 4 (pg. 6) and see Figure 17.

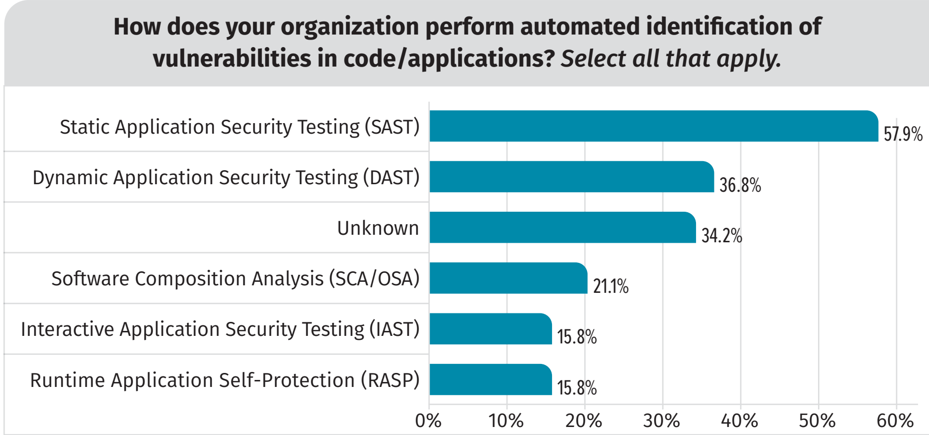

**How does your organization perform automated identification of vulnerabilities in code/applications?** ***Select all that apply.***

*Figure 17. Automated Identification of Vulnerabilities in Code/Applications*

Application teams typically have large backlogs of features that the business or customers are anxiously awaiting. This also makes it harder to squeeze in work to remediate vulnerabilities when they are not critical or high risk, or when there is a chance that they might not be exploitable. Any additional analysis or customized reporting and communication that fits better into the way these teams develop and release software can be a huge help in getting them to engage and reduce pushback.

## Summary and Final Recommendations

Most organizations are following best practices when it comes to the identification of vulnerabilities. We foresee a much greater percentage of agent-based identification being leveraged for end users due to the increase in the remote workforce. We also see a continued shift away from traditional, active scanning outside of on-premises data centers. This will most likely be replaced with a combination of agent-based scanning, passive scanning and image scanning.

While the number of respondents emailing scanning results has gone down from 52% in 2019 to 39% in 2020, some of the largest gains—in terms of improving vulnerability management within organizations—can come from more robust analysis, reporting and communication. Focusing on root-cause analysis and prioritizing the vulnerabilities that are not currently blocked can help accelerate remediation and help the business understand where additional support is required. See Figure 18.

The end goal for all this effort is to enable organizations to effectively and efficiently remediate vulnerabilities. For most larger organizations, lack of automated patch and configuration management technologies is not the issue. By analyzing the data, vulnerability management teams can help identify any gaps that might need to be addressed in order to support these efforts. For example, if 70% of outstanding vulnerabilities are due to third-party software, either the remediation teams do not have the right technology to deal with updates to third-party software or there are business requirements within the organization that prevent the teams from updating to non-vulnerable versions. While security might not be directly responsible for the remediation of these vulnerabilities, anything security can do to help identify and remove impediments will make remediation that much easier for IT organizations.

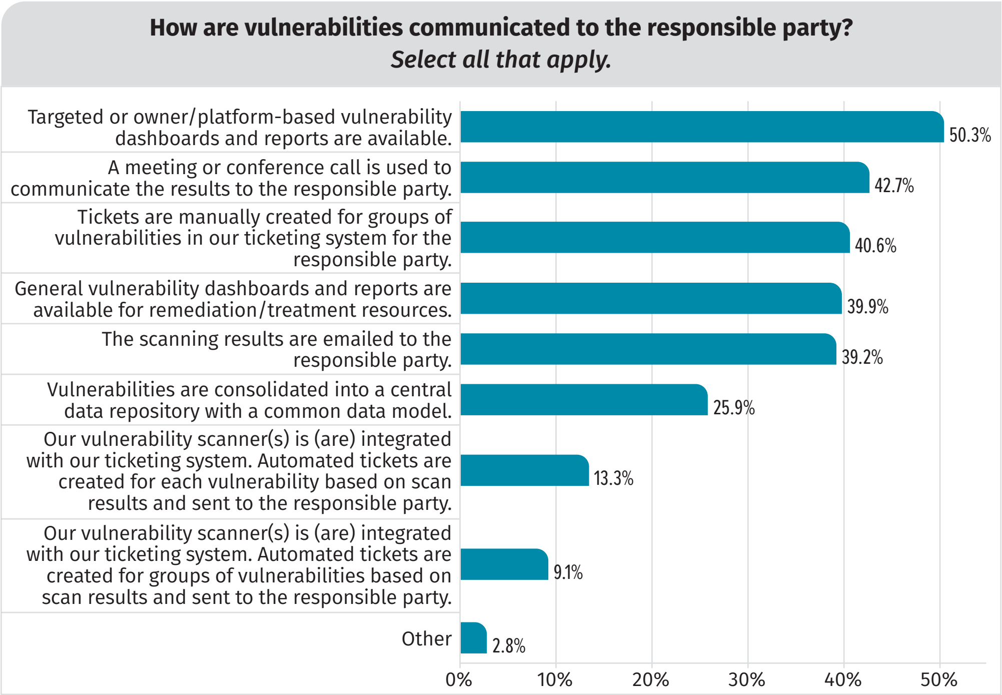


*Figure 18. Vulnerability Reporting Methods*

## About the Author

**David Hazar** is a SANS analyst, instructor and co-author of SANS MGT516: Managing Security Vulnerabilities: Enterprise and Cloud. He is also an instructor for SANS SEC540: Cloud Security and DevOps Automation. A security consultant based in Salt Lake City, Utah, David focuses on vulnerability management, application security, cloud security and DevOps. David has 20+ years of broad, deep technical experience gained from a wide variety of IT functions held throughout his career, including: developer, server admin, network admin, domain admin, telephony admin, database admin/developer, security engineer, risk manager and AppSec engineer. He holds the CISSP, GWAPT, GWEB, GMOB, GCIA, GCIH, GCUX, GCWN, GSSP-.NET and GSTRT certifications.

## Sponsor

**SANS would like to thank this survey's sponsor:**

ANOMALI®