



AURORA

Vulnerability Management in a Post-Pandemic World





Introduction

The global pandemic has upended the way companies operate, forcing business leaders to quickly adopt new strategies to sustain their businesses through unpredictable times. Arguably, one of the most disruptive changes that many organizations underwent was transitioning to a remote working environment as a necessary step to continue day-to-day operations, sparking increased adoption of cloud-based systems. This shift, however, was faced with significant technological and security challenges, disrupting critical business processes across many business units along the way.

Within information security, vulnerability management processes that relied on traditional (agentless) tools were proven ineffective in managing vulnerabilities across a distributed, often disconnected end-user device ecosystem. COVID-19 has accelerated an already upward trend of organizations investing heavily in cloud-based services to increase employee productivity, alleviate bandwidth usage, and quickly deliver suitable remote working tools without due regard for security unknowingly heightened their attack surface, increasing the risk of sensitive information exposure. A recent study by Sophos revealed that seventy percent (70%) of organizations that invested in popular public cloud providers reported having experienced a cyberattack at some point during 2019. According to Gartner, worldwide spending on cloud services is projected to grow 18.4% in 2021, thus it would be reasonable to assume that the number of companies that will fall victim to cyberattacks will only increase in 2021.

An often-overlooked major factor that continues to contribute to an increasingly expanded attack surface for organizations is insecurely configured Internet of Things (IoT) devices connected to employees' home networks, such as smart refrigerators, thermostats, and home security systems. Remote working arrangements without clear guidance for home network security could create opportunities for threat actors to take advantage of publicly accessible, unsecured IoTs to gain a foothold into organizations' networks. Therefore, adding requirements for securing home networks to existing corporate policies and training employees on home security hygiene practices are two approaches organizations can take to control their overall attack surface. As business leaders continue to adjust their business operations to navigate the COVID crisis, business requirements and needs will continue to change. It is therefore critical for Information security leaders to continuously evaluate their security programs and underpinning processes and procedures and make the necessary adjustments to satisfy the everchanging needs of the business during these uncertain times.

This whitepaper will explore several challenges associated with managing vulnerabilities in a post-COVID world, presenting practical solutions along the way to help organizations increase the overall effectiveness of their vulnerability management program.



Vulnerability Management Explained

Vulnerability management is the practice of timely, efficiently, and effectively remediating technical vulnerabilities on information systems, applications, equipment, and devices to preserve the confidentiality, integrity, and availability of valuable information. The main goal of vulnerability management is to reduce the likelihood of exploitation of technical vulnerabilities, thus minimizing the number of security incidents. The success of a vulnerability management program is centered around three equally important elements:

- **PEOPLE**
- **PROCESS**
- **TECHNOLOGY**

PEOPLE

Vulnerability management is a cross-functional effort requiring close collaboration from various Information Technology (IT) teams. While information security is often responsible for discovering, assessing, rating, prioritizing, and communicating vulnerabilities, information system owners across the business remain responsible for remediating those vulnerabilities within established timescales. For instance, in a traditional Information Technology organization, information security engineers or analysts are responsible for creating vulnerability scan templates or profiles, scheduling scans, ensuring that scans run successfully, analyzing the scan results, rating and prioritizing vulnerabilities, producing actionable reports, and sharing those reports with relevant information system owners. Information system owners (i.e., server or network administrators), on the other hand, are responsible for reviewing vulnerability reports and taking the necessary actions to fix the vulnerabilities following established timescales. Remediation actions can range from applying a software patch, upgrading the operating system or application, disabling or removing a system component, or making a configuration change.





Vulnerability Management Explained



PROCESS

The vulnerability management process is a series of progressive and repeatable steps to address technical vulnerabilities quickly and effectively. The process should be designed to discover known vulnerabilities on internal and external systems, scan for specific vulnerabilities (i.e., for specific CVEs), and remediate vulnerabilities per the organization's patch and configuration management processes. The process should also address external requirements that the organization must meet in order to comply with regulatory or legal mandates. For instance, PCI DSS requires companies that handle credit card information to scan their internal and external networks at least quarterly.

A typical vulnerability management process consists of six steps, including:

1. Discovering security vulnerabilities on information systems
2. Assessing discovered vulnerabilities for their applicability (i.e., false positive, true positive), the existence of exploit code in the wild, and criticality (e.g., CVSS score)
3. Rating (i.e., high, medium, low) vulnerabilities taking into account the presence of security controls that could reduce the likelihood of exploitation, thus reducing the inherent information risk
4. Prioritizing the remediation of vulnerabilities based on assigned severity
5. Communicating vulnerabilities to appropriate system owners
6. Remediating vulnerabilities, and
7. Validating the effectiveness of the remediation

While the vulnerability management process itself is often owned by Information Security (e.g., CISO or Head of Information Security), support from relevant asset owners is crucial to the success of the program.



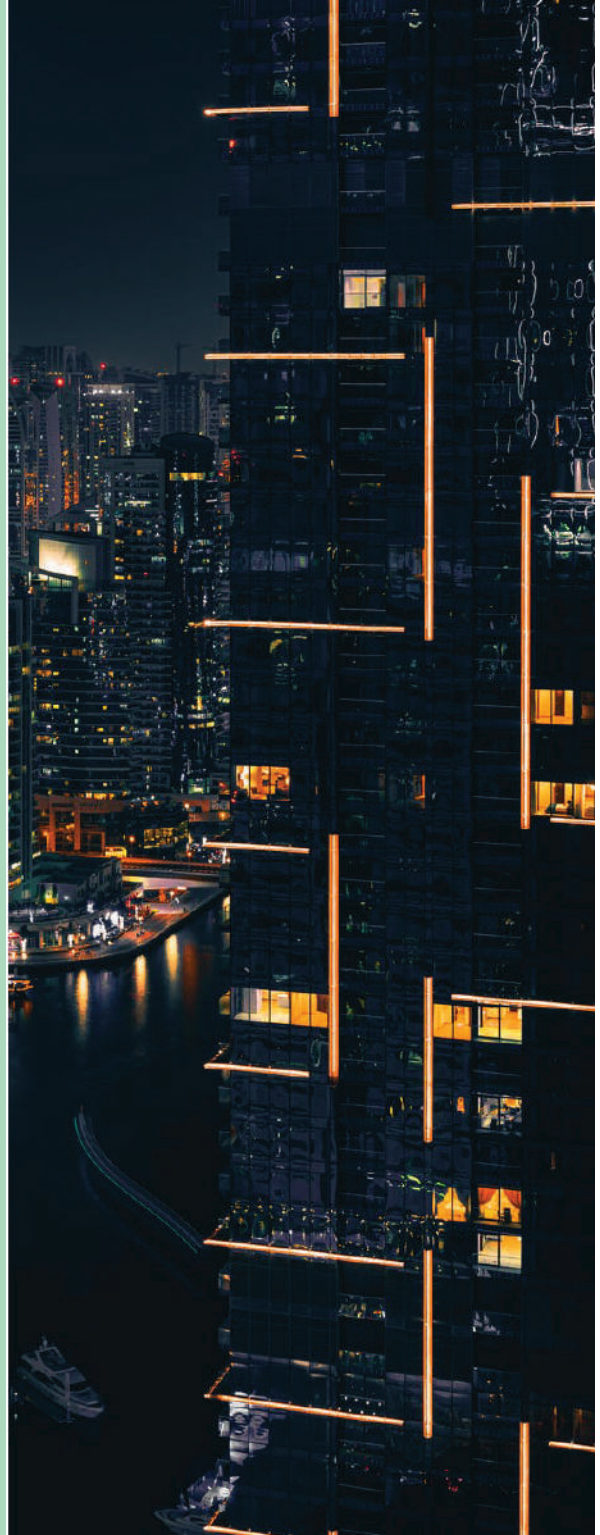
Vulnerability Management Explained

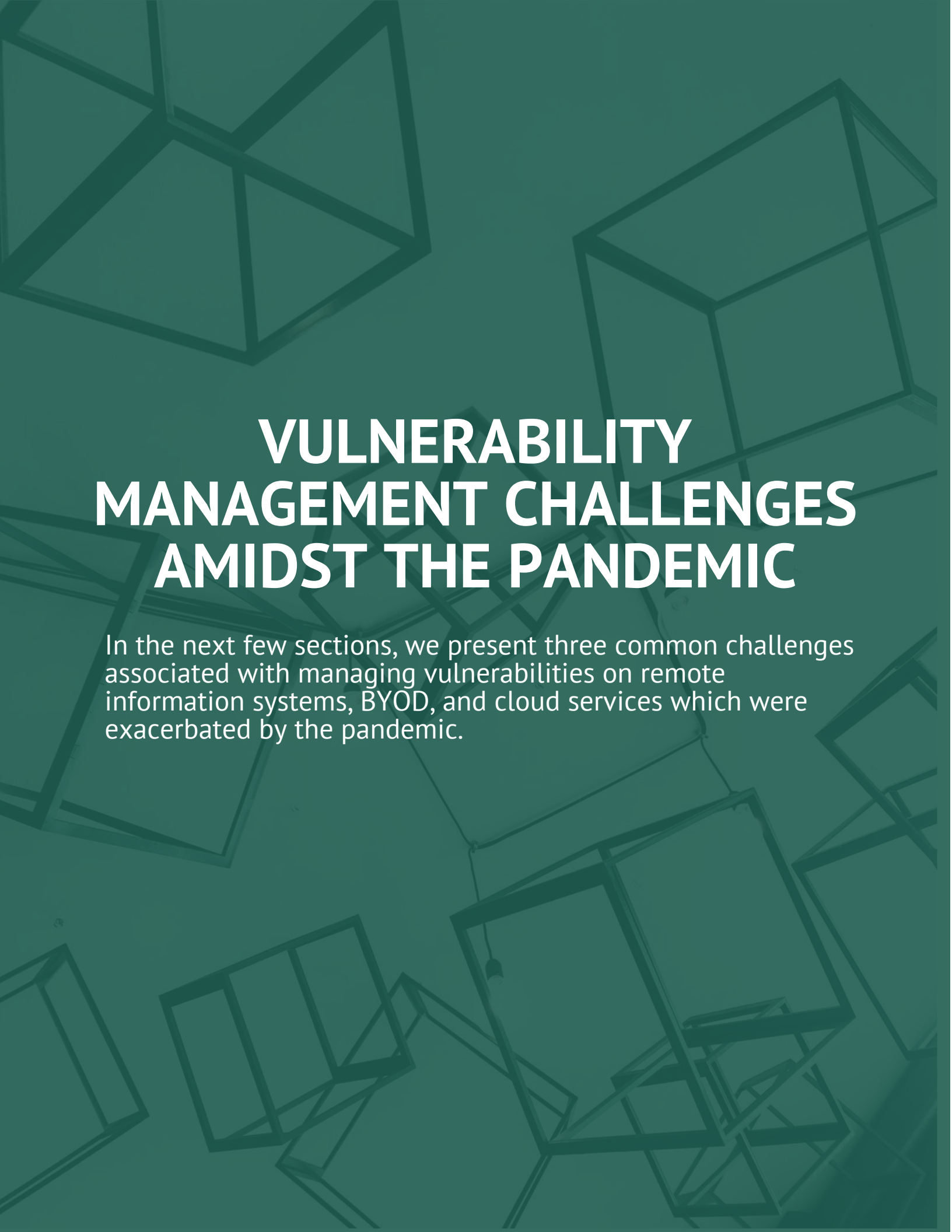
TECHNOLOGY

The technology aspect of vulnerability management consists of vulnerability scanners, port scanning tools (e.g., Nmap, Netcat, etc.), configuration management systems, patch management systems, and sources of vulnerability intelligence.

Vulnerability scanners are automated tools that check information systems (including servers and end-user devices), web applications, devices, and equipment for the presence of known vulnerabilities. Broadly speaking, vulnerability scanning tools consist of one or more scan engines responsible for performing the actual scans, and a scan console that provides visualization of the scan results. Moreover, there are two categories of vulnerability scanners: agentless and agent-based. Agentless scanners are the most common ones and are generally deployed across network segments to scan a range of IP addresses or IP networks. To increase the accuracy of results, authenticated scans are often performed where the scan engine logs into target systems using a service account. In contrast, agent-based scanning requires the installation of an agent on target systems, in particular on workstations and servers. The scan agents are managed from the scan console and scan the systems on a predefined interval, sending the scan results to a central scan console upon finishing each scan.

Ideally, organizations will use a combination of agentless and agent-based scanning technology where agents scan workstations and servers and agentless scan engines cover all other devices that do not support the installation of an agent.





VULNERABILITY MANAGEMENT CHALLENGES AMIDST THE PANDEMIC

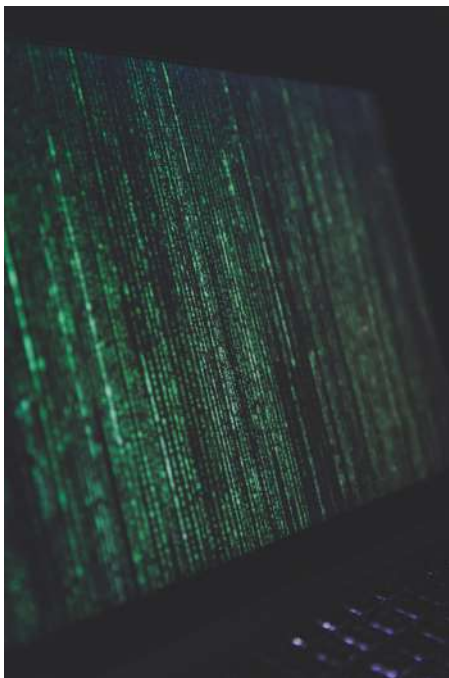
In the next few sections, we present three common challenges associated with managing vulnerabilities on remote information systems, BYOD, and cloud services which were exacerbated by the pandemic.



Challenge 1: Agentless Scanning of Remote Devices

The COVID crisis threw a curveball to information systems that relied on agentless vulnerability scanners to support their vulnerability management program, in particular concerning scanning of end-user devices remotely.

With a large percentage of the workforce now working from home, end-users rely on Virtual Private Networks (VPNs) to access internal organizational resources. When end users connect to corporate VPNs, their devices are assigned a private IP address from a pool of addresses dedicated to VPN and, as long as the scan engine (typically deployed on-premises) can reach the IP address assigned to the end-user device, a scan can be performed. Although straight forward, there are several problems associated with this approach:



1. Vulnerability scans can generate large volumes of network traffic, therefore, scanning over VPN could severely impact network performance, causing high bandwidth utilization which could lead to negative user experience and loss in end-user productivity
2. It is very common to deploy a firewall between the VPN network and any internal network segments configured to permit all inbound connections from the VPN network but deny all inbound connections from internal network segments destined to the VPN network. Since the scan engines are typically deployed within internal network segments, the firewall needs to allow the scan engine to reach the VPN network otherwise, the scan results will most likely be inaccurate and incomplete.
3. Vulnerability scans are generally scheduled to run at a specific day and time, which means that end-user devices must be connected to the VPN network during the time window in which the scan is scheduled to run.

A more practical approach is to adopt an agent-based scanning solution where scan agents are installed on all mobile devices (e.g., laptops) and devices deployed in home offices to significantly increasing the accuracy and effectiveness of the scans. For this approach to work, the scan console needs to be externally available. The reason for this is because the agents will scan the system at a predefined interval (typically from 4 to 24 hours) and send the scan results to the scan console over the Internet. Organizations should therefore consider selecting a vulnerability scanning vendor that can deliver the scan console as a Software-as-a-Service (SaaS) application.



Challenge 2: Manage Vulnerabilities on Personally Owned Devices



Another challenge brought by the pandemic is managing vulnerabilities on personally owned devices. Many organizations adopted BYOD policies amid the COVID crisis to increase workforce mobility while alleviating costs associated with licensing and hardware. However, organizations need to recognize that unless adequate safeguards are implemented to ensure that devices connecting to corporate resources are free of vulnerabilities, the organization's attack surface will be significantly enlarged, putting valuable information at risk of exposure.

One of the most significant differences between managing vulnerabilities in BYOD and corporate-owned devices is the person responsible for remediating those vulnerabilities. As we saw earlier, system owners are responsible for remediating vulnerabilities on corporate information systems, but when it comes to BYOD, the end-user (or owner of the BYOD) is responsible for ensuring that vulnerabilities are remediated on the devices that they own. In the majority of cases, the end-user will require significant assistance from IT to remediate vulnerabilities as they may not possess the technical acumen to go through the process on their own. If remediating vulnerability is a condition to gaining access to organizational information systems, then end-user productivity will drastically decrease at the same rate that costs associated with IT support will increase.

A more practical approach is to first develop a BYOD policy to establish:

1. The types of personal devices that will be permitted to connect to organizational resources
2. The types of business information and information systems end-users will be allowed to access using their personal devices
3. The conditions of access to business information and information systems (e.g., enrollment with company's MDM solution, having antivirus software is turned on, etc.)

Once the BYOD policy is defined, then technical safeguards can be implemented to containerize and protect the actual information (through the use of MDM and information rights management, for example) that end-users will access using personal devices as opposed to protecting the personal device itself. Personal devices should still be required to maintain a baseline security posture, however, remediating technical vulnerabilities should not be a condition of access to corporate resources.



Challenge 3: Managing Vulnerabilities in the Cloud

The COVID crisis drove many organizations to invest in cloud service to accelerate their migration to the cloud. Vulnerabilities in the cloud take a slightly different form than technical vulnerabilities. Whereas technical vulnerabilities are still prevalent in server-based instances deployed in the cloud, the leading cause of cloud data breaches in the past decade has been misconfigurations and mismanagement of the cloud management plane.

The cloud management plane consists of web user interfaces, web consoles, and APIs available to cloud users to build and manage their cloud environments. For instance, the cloud management plane for public IaaS providers will consist of service APIs as well as a web console, both of which are accessible over the Internet. For example, AWS' management plane consists of:

- The AWS management console, which can be accessed through a web browser over the Internet: <https://aws.amazon.com/console/>
- The AWS service APIs, which can be accessed programmatically using the AWS command-line tools or Software development kits

Similarly, the cloud management plane of a SaaS application will consist of the “administrator” tab or menu that allows the cloud user to configure the various features of the SaaS application.

Why is the cloud management plane so important?

In a traditional data center, the servers, network devices, and other infrastructure components are configured and managed through different, decentralized management interfaces accessible via internal networks or directly through a serial connection, for instance. Additionally, different roles within IT have different administrative responsibilities for managing the different parts of the infrastructure. For example, server administrators are responsible for managing all the servers, storage administrators are responsible for managing network-attached storage and storage area networks, and network administrators for managing firewalls, routers, switches, and load balancers. Therefore, for a threat actor to gain administrative access to all infrastructure components within a data center, he or she would first need to compromise several different privileged accounts, and then attempt to bypass network access controls that may exist to protect access to administrative networks and interfaces.

In the cloud, the management plane is centralized and delivered over the internet, and this is the most significant security difference between traditional data center infrastructure and cloud environments. When you sign up for a cloud service, you are provisioned with a root account that grants full administrative privileges to everything within the cloud account. If a threat actor wanted to access the cloud resources, all he or she would need to do is compromise the root account. Consequently, gaining access to the root cloud account is equivalent to gaining administrative-level access to any compute, storage, database, and network within a traditional data center.



Challenge 3: Managing Vulnerabilities in the Cloud

People, Process, and Technology

While cloud misconfigurations could be managed using the same vulnerability management process described earlier, the “people” and “technology” elements will slightly vary.

The category of tools designed to detect and manage cloud misconfigurations is called Cloud Security Posture Management (CSPM). CSPM tools can be standalone, integrated into Cloud Access Security Brokers (CASBs), or offered by the cloud provider as a native service. For example, AWS offers Security Hub as a native service to help detect misconfigurations of the AWS management plane.

As it relates to the “people” element, information security analysts or engineers tasked with managing cloud misconfigurations should possess general knowledge of cloud security and understand the various ways that cloud misconfigurations can be exploited to gain unauthorized access to or hijack organizational resources.

Organizations that have acquired cloud services in the past year should:



1. Develop security configuration benchmarks based on industry-accepted practices (e.g., CIS) for the cloud service(s)
2. Determine if the cloud provider offers CSPM as a service, acquire a third-party CSPM product, or outsource the capability to a Managed Security Service Provider
3. Incorporate cloud misconfiguration management into a vulnerability management program



Conclusion

The shift to working from home and the increased investment in and rapid adoption of cloud services have exacerbated the need to adequately manage vulnerabilities on corporate and personally owned devices as well as cloud services. As companies continue to adjust their business operations in the midst of the global pandemic, Information Security leaders should re-evaluate their security programs and take the necessary steps to continue to support and enable the achievement of business objectives during these unprecedented times. Flexibility and adaptability in the face of uncertainty are two critical success factors in information security.

If you are struggling to manage vulnerabilities in the “new normal”, Aurora is here to help. We have a team of certified experts in vulnerability management that can help you mature your existing or build a brand-new vulnerability management program to strengthen your security posture. Start your vulnerability lifecycle now, as new vulnerabilities continue to arise daily.

How can Aurora Help?

Aurora offers a portfolio of cybersecurity services to meet the diverse needs of our clients. All of our services are provided by experienced and certified security practitioners and designed to help organizations mature their existing security programs or create new ones from the ground up. With regards to vulnerability management, Aurora can help organizations conduct Vulnerability Assessments where a team of security practitioners evaluates the organization’s security posture over a period of one month to identify weaknesses in the people, process, and technology elements that underpin any security program. By the end of the engagement, Aurora would have identified:

- Gaps in existing security technology in terms of missing capabilities, disabled features, or misconfigurations
- The effectiveness of existing security technology in addressing security requirements
- Any additional security technology needed to complement or replace existing controls

Aurora also offers Vulnerability Management-as-a-service for organizations that do not have the people or technology resources needed to adequately manage vulnerabilities. Our security practitioners will guide your organization throughout the entire vulnerability management process.

Lastly, Aurora can help organizations scan their entire environment on a monthly basis, including deploying scanning tools within the environment, configuring and scheduling scans, analyzing scan results, rating and prioritizing vulnerabilities, and producing actionable remediation reports to help system owners quickly eliminate the vulnerabilities from the environment.