Navigating the New Distributed Enterprise

Também disponível em português
www.isaca.org/currentissue

The early days of the COVID-19 pandemic were like a seismic jolt for IT and security managers. Almost overnight, governments and other entities instituted lockdowns to try to curb the spread of the virus—and IT suddenly had to support a new distributed workforce.

Three years later, COVID-19 is still circulating, although the incidence of cases is much reduced.[1] However, the remote work trend remains strong, due at least in part to employee demand.[2] Now that a hybrid or distributed workforce has become the new normal, it is imperative to ensure that digital trust, security and integrity of users, devices and assets are top of mind, no matter where they physically reside.

Taking Control of Assets

The days of tightly controlled onsite networks, data centers and user endpoints are gone. It is now common for servers, applications and other assets to be housed or owned separately—and at least somewhat outside the strict control of enterprise IT. Given this migration and the pervasiveness of shadow IT among users or departments outside the IT domain,[3] it is vital to implement asset discovery as part of an asset management process.

Asset discovery is a foundational exercise to identify all assets that connect to the enterprise network and determine the importance and criticality of each one. The process must be continuous, automated and augmented by manual updates when needed. A wide variety of asset discovery tools are available, ranging from freeware to licensed enterprise-class software and services.[4]

A Risk-Based Approach

Having an accurate asset inventory sets the stage for IT to identify the critical resources that need to be protected against malicious acts or inadvertent misuse. Depending on the environment and staff resources, a risk-based approach might be required to protect assets that are either high in value or have evidenced a high level of risk in terms of behaviors. The latter might include assets with high numbers of abnormalities, general indicators of compromise (IoCs), or other factors that render them especially vulnerable to attacks. Making this determination is often beyond the scope of asset management systems, as is deciphering the interconnections between assets. For these use cases, an extended detection and response (XDR) system can be beneficial due to its ability to gather and contextualize data from many sources, providing in-depth visibility and mapping.

Endpoint Exigencies

In a distributed or hybrid workforce, special considerations are required for client, mobile and bring-your-own-device (BYOD) equipment. Of primary importance is whether access to the network and resources will be restricted to enterprise-owned devices or permitted for user-owned endpoints as well. Device restriction, usually based on device

TIMOTHY LIU

Is the cofounder and chief technology officer of Hillstone Networks, a leading provider of infrastructure protection solutions. He has more than 25 years of experience in the technology and security industries, working with Fortune 500 enterprises and data centers to proactively defend against cyberattacks on a global level.

Fully supporting the distributed workforce also requires a foundational shift from IP address-based network access control to identity-based NAC.

operating system (OS) or media access control (MAC) address, is often possible via perimeter security solutions. For example, next-generation firewalls allow IT to exert tight control over which devices may access the network and its assets.

For all endpoints, regardless of ownership or physical location, health checking is critical to ensure device integrity and digital trust. Typically, this is performed by an endpoint agent such as a Secure Sockets Layer Virtual Private Network (SSL VPN) client, which can support multiple device operating systems (OSs) and check for OS versions, antivirus protection and other conditions.

Yet another consideration is the potential for loss or theft of an enterprise-owned or personal endpoint that can expose sensitive enterprise information. Device tracking, the ability to wipe enterprise data upon session end or other criteria, encryption and multifactor authentication (MFA) are important.

From IP-Based to ID-Based Network Access Control

Fully supporting the distributed workforce also requires a foundational shift from Internet Protocol (IP) address-based network access control to identity-based network access control (NAC). IP-based NAC, using active directory or similar mechanisms, has long been used to support on-premises devices. This approach amplifies security by allowing only devices connected to specific networks (IP addresses) to access an enterprise's sensitive data and resources.

However, in distributed environments, a centralized NAC can become a single point of failure. For example, unreliable network connections can result in spotty network access approvals for remote users. Further, remote and distributed workers are often far more mobile than their office-dwelling counterparts. A remote worker might log in via a public WiFi hotspot, a poorly secured home network, a shared mobile phone network or some other access point—rendering an IP-based NAC scheme difficult or impossible to enforce.

As a result, many enterprises are turning to cloud-based Identity as a Service (IDaaS) as an alternative.[5] IDaaS is a hosted distributed identity and access management (IAM)[6] service with NAC incorporated as a component. The IDaaS model offers the scalability, elasticity and agility of the cloud, reduced overhead for management and capital expenditures, plus broad geographic distribution and, in many cases, easier integration with other cloud resources, such as Software as a Service (SaaS).

IDaaS can also offer advanced secure access services such as adaptive MFA, single sign-on across network- and cloud-based enterprise resources, and even self-service portals that allow users to request access and update their information. However, IDaaS is not without drawbacks or risk. The provider may limit the permissions included in an IDaaS offering, and breaches are a real possibility, as evidenced by the recent Okta ransomware attack.[7]

Cloud Considerations

With both traditional NAC and cloud-based IAM, cloud implementation in general has become an important—almost intrinsic—part of supporting the distributed workforce. Ninety-four percent of all enterprises now use cloud services, and 48 percent of enterprises store classified and other important information in the cloud.[8]

Although localization of network-based applications and resources traditionally worked well for onsite employees, the new distributed workforce model requires that resources be available for remote and mobile workers as well. IT managers will increasingly need to facilitate the movement of in-house applications (apps) to the cloud, including hybrid and public cloud architectures, to better support workers regardless of location.

However, the security considerations—and by extension, digital trust issues—for users accessing apps and data stores in the public cloud are quite different from those associated with locally hosted resources. For example, cloud providers often operate on a shared security responsibility model that makes the provider liable for securing the infrastructure but assigns the client with responsibility for the security and integrity of its own hosted data and applications.

In addition, cloud-native applications and their variants continue to gain momentum for the extreme flexibility, adaptability and utility they offer.[9] These apps exist solely in the cloud and require additional considerations with regard to cybersecurity and digital trust.

There are many point security products available for cloud elements; however, they typically provide a relatively narrow window into potential threats, especially if the cloud infrastructure is especially large or encompasses multiple cloud providers. Thus, many organizations are investigating cloud workload protection platforms (CWPPs), which can span multicloud environments, containers, microservices, cloud-native apps, virtual machines (VMs) and other resources.

Unlike disparate and disjointed point security products, CWPPs are designed to span the entire cloud stack—from DevOps through image management and runtime. At the DevOps stage, CWPPs can provide code analysis and image encapsulation and scanning to help ensure the integrity and security of code and packaging. Image management encompasses further image scanning to protect against faults and threats and user access control to protect the image warehouse.

At runtime, the defenses are usually divided into two primary categories: platform layer security and runtime security. The former typically includes security for the architecture, network, host, kernel and Docker daemon; compliance baselining; access control; and security management and encryption. The container runtime security usually spans L7 and container isolation, threat detection, vulnerability scanning and process management.

CWPP Capabilities

Although CWPP technology is relatively young, it normally includes standout capabilities that are especially pertinent to multicloud and container environments. For example, container architectures are typically not attached to IP addresses but migrate and change on the fly as needed. As a result, CWPP container asset management needs to interface with the container orchestration system, such as Kubernetes, to synchronize the attributes of various assets.

This capability also plays into asset traffic visualization, a critical component of cybersecurity. Certain orchestration systems lack the ability to segment containers or groups to prevent illegal or malicious access. By accessing the orchestration component's traffic mechanism, CWPP can detect and display traffic between containers, external networks and other assets. This allows admins to quickly visualize container asset interactions, control them and spot any illegal access attempts.

Accurate visualization also allows a CWPP to enforce microsegmentation of cloud workloads to prevent the rapid spread of malware between assets and reduce illegal accesses. Most orchestration systems provide some type of mechanism for this function, but they are typically labor intensive and lack logging capabilities. CWPP, in contrast, offers microsegmentation via a graphical user interface (GUI) for easy visualization and control with just a few clicks, and full logging for forensics.

Although CWPP technology is relatively young, it normally includes standout capabilities that are especially pertinent to multicloud and container environments.

Establishing Digital Trust

No conversation about digital trust would be complete without addressing the challenges of securing access for employees and others, regardless of their physical location. When the COVID-19 pandemic and its associated lockdowns first hit, most IT teams turned to a technology that was already in place for secure remote access: Secure Sockets Layer virtual private network (SSL VPN).

However, deploying SSL VPN at scale to support hundreds or thousands of dispersed workers quickly brought certain limitations and other issues into sharp focus. For example, enterprise-class SSL VPNs are usually licensed on a per-user or per-capacity basis. Expanding to support additional remote users can quickly become expensive in terms of licenses, additional hardware costs and IT staff time to manage user permissions and devices.

In addition, some VPNs will authenticate users just once—upon session initiation—and then grant access for all assets and resources for which the user is authorized. Security risk can thus arise if user credentials are stolen by a hacker or if the user device itself is hacked. Finally, SSL VPNs have exhibited multiple vulnerabilities over the years, to the extent that the US National Security Agency (NSA) issued a cybersecurity advisory in 2019.[10]

LOOKING FOR MORE?

- Read *Zero Trust: How to Beat Adversaries at Their Own Game. www.isaca.org/zero-trust*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

These are among the key reasons many organizations are turning to zero-trust network access (ZTNA), which dictates, in short, never trust, always verify. Precursors to the current definition have circulated among researchers since the mid-1990s, but it was formally codified in US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 *Zero Trust Architecture* in 2020.[11] The zero-trust model eliminates implicit trust of users and devices while granting only the minimum privileges possible. Authentication is continuous so that if any change to user or device security posture is detected, access rights can be revoked.

Importantly, ZTNA breaks from the traditional network-centric focus to embrace a user-to-application model. This allows devices and users to be assessed comprehensively for identity, posture and context of access requests. It also expands security beyond the network perimeter to encompass any and all resources connected to the network—whether they are cloud-based, remote, virtual or any other permutation.

Perhaps even more important, ZTNA does not require a complete (and expensive) replacement of current remote access security infrastructures. Rather, it can coincide with existing SSL VPN architectures, augmenting and expanding security services while gradually being deployed to serve other users and groups directly.

ZTNA does not require a complete (and expensive) replacement of current remote access security infrastructures.

Conclusion

For many enterprises, work routines changed dramatically in the opening days of the COVID-19 pandemic, and it is doubtful they will change back. Thus, establishing a state of digital trust in the new distributed workforce is unlikely to be a one-and-done process. Instead, it is far more likely to be an incremental process that layers new techniques and technologies onto existing infrastructures allowing them to evolve to a new, higher level of digital trust and security overall. Further, the collective experiences of IT and security teams in supporting the distributed enterprise will likely point to new models for establishing digital trust.

Endnotes

1 World Health Organization (WHO), "WHO Coronavirus (COVID-19) Dashboard," *https://covid19.who.int/*

2 Remoters, "Remote Work Trends to Look for in 2023," *https://remoters.net/remote-work-trends-future-insights/*

3 Walters, M.; "Four Practical Steps to Eliminate Shadow IT Permanently," *Forbes*, 25 February 2022, *https://www.forbes.com/sites/forbestechcouncil/2022/02/25/four-practical-steps-to-eliminate-shadow-it-permanently/*

4 Creamer, L.; "The Best IT Asset Management Software," *PC Magazine*, 13 July 2019, *https://www.pcmag.com/picks/the-best-it-asset-management-software*

5 Hughes, C.; "IDaaS Explained: How It Compares to IAM," *CSO*, 23 May 2022, *https://www.csoonline.com/article/3660554/idaas-explained-how-it-compares-to-iam.html*

6 National Institute for Standards and Technology (NIST), "Identity and Access Management," USA, *https://www.nist.gov/identity-access-management*

7 Carey, S.; "LAPSUS$ Ransomware Group Claims Okta Breach," *CSO*, 22 March 2022, *https://www.csoonline.com/article/3654273/lapsus-ransomware-group-claims-okta-breach.html*

8 Sumina, V.; "Twenty-Six Cloud Computing Statistics, Facts and Trends for 2023," Cloudwards, 7 June 2022, *https://www.cloudwards.net/cloud-computing-statistics/*

9 Mia-Platform Team; "Top Four Cloud Native Trends in 2022 Shaping the Future of Business," Cloud Native Computing Foundation, 5 January 2022, *https://www.cncf.io/blog/2022/01/05/top-4-cloud-native-trends-in-2022-shaping-the-future-of-business/*

10 National Security Agency, "Mitigating Recent VPN Vulnerabilities," USA, October 2019, *https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF*

11 Rose, S.; O. Borchert; S. Mitchell; S. Connelly; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 *Zero Trust Architecture*, USA, 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf*