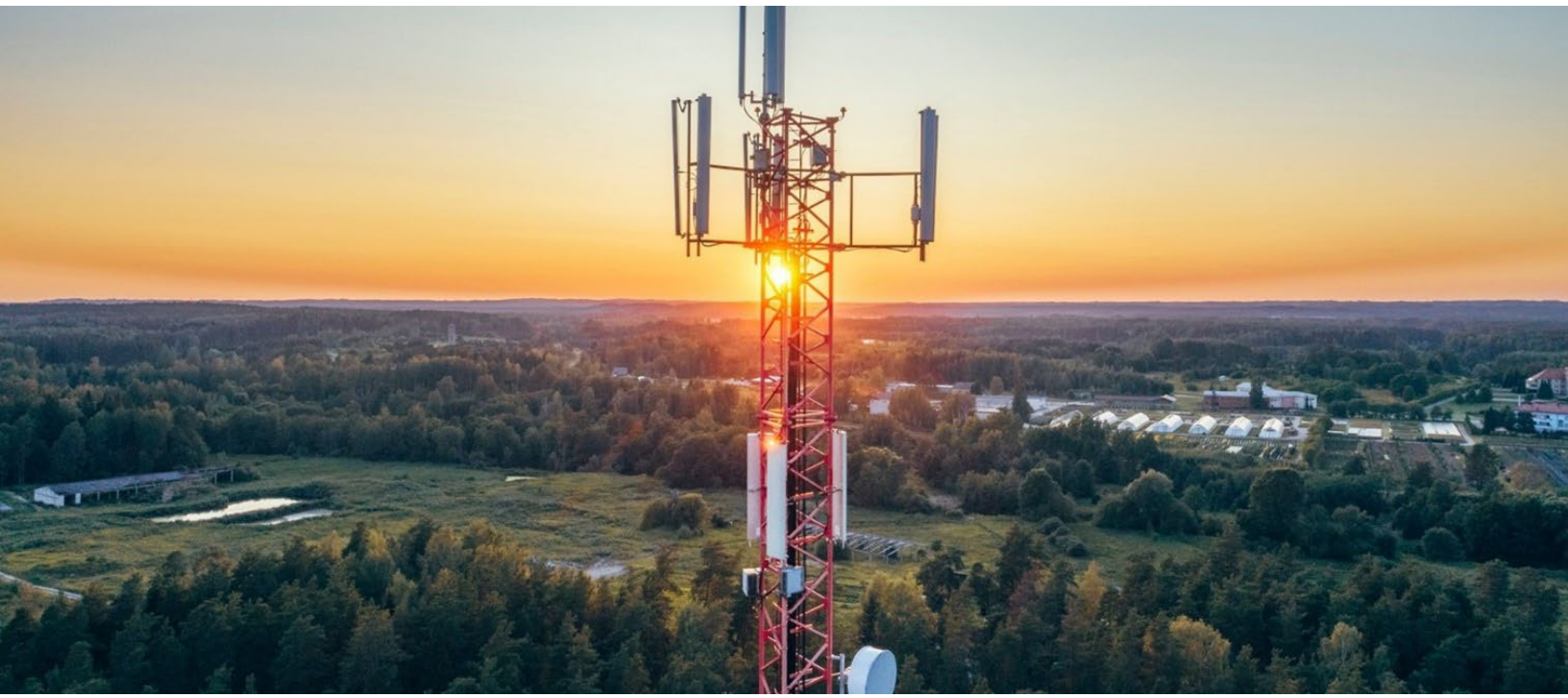
TLP:CLEAR

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

certnz

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



MODERN APPROACHES TO NETWORK ACCESS SECURITY

Publication: June 18, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. Federal Bureau of Investigation
New Zealand's Government Communications Security Bureau
New Zealand's Computer Emergency Response Team
Canadian Centre for Cyber Security

Table of Contents

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) has frequently identified virtual private network (VPN) solutions that have been involved in many recent high-profile incidents, both with cyber criminals and nation-state actors. CISA has discovered over 22 Known Exploited Vulnerabilities (KEVs) related to VPN compromise, leading to broad access to victim networks. These incidents and associated vulnerabilities are prompting some to consider replacing their legacy VPN solutions with modern network access solutions. The shift of more services into the cloud also points to the value of Secure Access Service Edge (SASE) instead of a traditional security stack located in an on-premises data center. While some VPN solutions are inherently more secure than others—and not always the cause of major cyber incidents—current hybrid networks require adopting modern network access security solutions to help organizations protect corporate resources. Moreover, these network access solutions provide opportunities to integrate granular access control not inherent to traditional VPN approaches. CISA encourages a careful analysis of how your security needs have changed in light of increased use of cloud services and leveraging any technology updates to progress in your Zero Trust journey.

Organizations that embrace these newer practices will reach an overall outcome closer to zero trust (ZT) principles.

This report provides an overview of modern approaches to network access security for executive leaders, network defenders of critical infrastructure, and government organizations. The report is specifically intended for organizations wanting to shift from traditional broad remote access deployments and move toward more robust and fine-grained security solutions (i.e., Secure Service Edge [SSE] and Secure Access Service Edge [SASE]). By using risk-based access control policies to deliver decisions through policy decision engines, these solutions integrate security and access control, strengthening an organization's usability and security through adaptive policies. This report provides best practices for users and organizations transitioning from traditional architectures to the cloud and furnishes primarily cloud-based solutions that can support hybrid and on-premises deployments in pursuit of zero trust goals.

This report outlines protections for IT and operational technology (OT) networks across a spectrum of network sensitivities and worst-case consequences of compromise. CISA, the Federal Bureau of Investigation (FBI), New Zealand's Government Communications Security Bureau (GCSB), New Zealand's Computer Emergency Response Team (CERT-NZ), and the Canadian Centre for Cyber Security (CCCS) (hereafter referred to as the authoring organizations) urge business owners—regardless of size—to review this report to better understand the vulnerabilities, threats, and practices associated with traditional remote access and VPN deployment, along with the inherent business risk posed to an organization's network by remote access misconfiguration. The authoring organizations are releasing this report to provide leaders with guidance to help prioritize the protection of organizations' remote computing environment security while operating under the fundamental principles of least privilege.

REMOTE ACCESS AND VPN LIMITATIONS

An enterprise remote access VPN allows users to access the corporate/business network through a private and encrypted tunnel. VPNs provide ease of access for employees to servers, company applications, and external data. Despite this, once a user establishes a connection over a VPN to access resources on the internal enterprise network, the organization may be susceptible to compromise through various VPN limitations—including vulnerabilities inherent to the network's design (e.g., IP address and Domain Name System [DNS] spoofing), the complexity of implementation, a misconfiguration, or even a vulnerability in the VPN solution.

Aside from general VPN and remote access risks, third parties connecting into an organization's network may also pose risks due to compromised devices on the network and poor cyber hygiene practices. Without strict network segmentation and adherence to the principles of least privilege and zero trust, organizations who provide remote access to third party vendors introduce additional risks to their environment. Although some VPNs can be configured to enforce granular firewall policies to provide limited levels of access to company resources, not all VPN providers offer this as an option. Many VPN solutions are software based, meaning the risk of cyber threat actors exploiting software vulnerabilities can become detrimental to business operations. As such, business owners should consider hardware-enforced solutions in addition.

IMPACT

Vulnerabilities in VPN systems can lead to substantial impacts to organizations if exploited by threat actors because they may enable easy access across a large enterprise network after successful exploitation of the device. CISA documented multiple such vulnerabilities over the past six months:

- CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893 in affecting Ivanti Connect Secure (ICS) and Ivanti Policy Secure gateways. Multiple sources observed the Internet-facing ICS VPN appliance fell victim to compromise when an attacker exploited configuration data to reverse tunnel from the ICS VPN appliance.[1] Then, the attacker modified a JavaScript file used by the Web SSL VPN component of the device to compromise credentials and move from system to system.[1] Memory and disk forensics were used during forensic analysis, combined with the Integrity Checker Tool, to identify malicious files on the compromised Ivanti Connect Secure VPN appliance.[2] However, this tool and patching failed to detect the compromise due to threat actors going virtually undetected, circumventing factory reset, and gaining root-level-access.[2]
- CVE-2023-4966 (Citrix Bleed) affecting Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances. This vulnerability allowed threat actors to bypass password requirements and multifactor authentication (MFA), leading to successful hijacking of legitimate user sessions on Citrix NetScaler web applications. Through hijacking legitimate user sessions, threat actors acquired elevated permissions to harvest credentials, move laterally, and access data and resources.[3] Lockbit 3.0 affiliates exploited this vulnerability in ransomware attacks.[3]

Aside from exploiting vulnerabilities, threat actors can gain access to all services within an organization's network if they use a compromised device or account and connect through VPN services. The most

significant risks to critical infrastructure entities are those that use a VPN tied to identity management and Active Directory. As noted in joint advisory, PRC [People's Republic of China] State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Volt Typhoon, a PRC state-sponsored cyber group that targets U.S. critical infrastructure, uses VPN sessions to securely connect to victim environments with administrative credentials. This allows Volt Typhoon actors to move laterally, obtain domain credentials for the network, and blend in with regular traffic, significantly reducing their risk of detection.

SOLUTIONS

Current modern solutions—Zero trust, SSE, and SASE--provide remote access to applications and services based on a granular access control policy. This type of policy rejects access to users who are not explicitly authenticated and authorized for a particular application or service. See the sections below for details. Organizations can leverage a more secure approach to network access by implementing ZT principles and continuously monitoring user activity, thereby promoting data security in transit. By not exposing internal applications to unnecessary risk, the organization can reduce the overall threat of compromise—further securing data at rest. The effectiveness of any proposed modern security solution greatly depends on how the organization's network and infrastructure is postured. Adhering to ZT principles to any degree will enhance your organization's ability to secure information, keeping it safe from threats and data loss. Current modern solutions—ZT architecture, SSE, and SASE—adhere to ZT principles and provide remote access to applications and services based on a granular access control policy.

Note: Organizations may differ from others and each solution has unique planning, architecture, or adaptation needs. Organizations should assess their needs and security posture and make an informed decision based on comprehensive analysis and before selecting a solution.

ZERO TRUST

ZT, defined by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-207, is designed to prevent unauthorized access to data and services coupled with granular access control enforcement. ZT is a collection of concepts and ideas that aid organizations with enforcing accurate per request access decisions based on the principles of least privilege in information systems and services. ZT operates under the assumption that no user or asset should implicitly be trusted, requiring each user, device, and application to continually reauthenticate and reauthorize throughout the transaction.

In order to develop zero trust strategies and implementation plans, organizations should adopt CISA's Zero Trust Maturity Model (ZTMM). The ZTMM presents a gradient of implementation across five distinct pillars, where advancement in maturity can be made over time. The model also presents ways in which various CISA cybersecurity programs support ZT solutions.

Note: CISA and the authoring organizations encourage all organizations to review the policies, procedures, and publications of zero trust as defined by their parent cybersecurity center when developing a plan of action and implementation.

For more information on zero trust and the Zero Trust Maturity Model, these CISA's Zero Trust Maturity Model.

SECURE SERVICE EDGE

SSE is a collection of cloud security capabilities that enable safe browsing, more secure software as a service (SaaS) application, and an easy approach to validating users accessing network data. Moreover, SSE is a comprehensive approach to network security, combining networking, security practices and policies, and services to a single platform. This approach allows organizations to ensure application security and access to data regardless of a user's device or location. SSE security capabilities consist of Zero Trust Network Access, Cloud secure Web Gateway, Cloud Access Security Broker, and Firewall-as-a-Service.[4]

Zero Trust Network Access

Zero Trust Network Access (ZTNA) is an IT security solution designed to provide more secure remote access to an organization's applications, data, and services by operating on strictly defined access control policies. These policies adhere to zero trust principles and facilitate security during remote access by implementing zero trust access control methodologies and granting access on a least privilege basis. Through ZTNA, organizations can restrict the tools available to potential attackers who gain access to compromised remote devices or services. This is achieved using an access broker security agent, which verifies user identity, access requirements, and zero trust policy rules. Security brokers can also monitor connections, including device security posture and client geolocation, and enforce MFA. Users undergo periodic reauthentication during each session to ensure security and identification. The authentication process restarts entirely if users seek access to additional applications.

Cloud Secure Web Gateway

Cloud Secure Web Gateway (SWG) is a security solution that protects users and devices from web-based threats and enforces security policies within the network. The SWG acts as a URL filter between users and the internet. SWG is a detection method for malicious or unauthorized content, web access controls, Secure Sockets Layer/Transport Layer Security (SSL/TLS) decryption for encrypted traffic analysis, application control, user authentication, and reporting analytics.

Cloud Access Security Broker

Cloud Access Security Broker (CASB) is a cloud security solution that can help organizations manage data across multiple software as a service application, as well as when data is in transit to cloud environments. A CASB can also help organizations enforce security policies, governance and compliance, detect and mitigate cloud threats, and enable an organizations' capability in ensuring effective protection of data across multiple locations.

Firewall-as-a-Service

Firewall as a Service (FWaaS) is a cloud-based security solution that enables organizations to monitor and aggregate traffic from multiple sources, such as data centers, offices, and cloud infrastructures. FWaaS operates similarly to a traditional firewall by inspecting and filtering network traffic, enforcing policies, and protecting against cyber threats. With the integration of FWaaS, organizations have the capability to

centrally manage through a cloud-based dashboard—promoting scalability, flexibility, and simplified administration.

SECURE ACCESS SERVICE EDGE

While SSE operates by converging security functions into a single cloud service, Secure Access Service Edge (SASE) is a cloud architecture that combines network and security as a service capability, including software-defined wide area networking (SD-WAN), SWG, CASB, next-generation firewall (NGFW), and ZTNA.[5] Cloud service providers (CSPs) can provide organizations with networking and security as a service in lieu of implementing security solutions on premises or being directed to data centers. This allows network administrators to have visibility of all ports and protocols and applications provided by the CSP or the organization. The SASE model offers a secure management interface, reduces complexity, and deploys security appliances that foster robust and more secure policies.

Software-Defined Wide Area Networking

SD-WAN is an offered solution/technology that simplifies the management and operation of wide area networks (WANs). In traditional WAN setups, network management is closely tied to hardware, such as routers and switches. With SD-WAN, organizations possess the ability to abstract the network infrastructure, enabling centralized control and management through software. Key features of SD-WAN are:

- Centralized control,
- Security integration, and
- Visibility and analytics.

Next Generation Firewall

NGFW is a network security device that performs traditional firewall security features while possessing protection capabilities against threats and vulnerabilities. Along with packet filtering and stateful inspection, NGFW provides the following:

- The ability to allow more granular control over network traffic by identifying and controlling applications, as well as monitoring ports and protocols;
- Built-in intrusion prevention systems (IPSs) designed to detect and block anomalies on company networks;
- Advanced threat protection and integrated threat intelligence feeds to enhance mitigation against targeted attacks; and
- Content filtering that inspects and filters web content (including URL and content-based filtering) to enforce ZT policies, detect malicious websites, and prevent exfiltration of data.

In a SASE architecture, enterprise traffic can be routed to cloud-based services in several ways depending on the provider. SD-WAN is considered one of the most effective ways to route traffic based on the organization's specific requirements. SD-WAN offers dynamic path selection, centralized management, and security integration. SASE solutions provide organizations with greater control over users by classifying the traffic at the application layer and throughout the network and by limiting what access is given, what data

users can obtain, and which applications can be used while operating in an enterprise environment. SASE also improves continuous monitoring by using one platform (instead of handling monitoring and reporting across multiple consoles). This enables efficient incident response and reduces complexity by streamlining networking and security. By condensing platforms and eliminating manually intensive point security solutions, SASE can help reduce logistical challenges associated with dispatching, installing, and updating network and security devices.[5]

SASE provides easier security, better user experience, management interface security, fast deployment, and reduced cost.

Hardware-Enforced Network Segmentation

Hardware-enforced network segmentation is used in networks where cyber operations pose credible threats to public safety, national security, and critical functions. More specifically, this practice adds a layer of hardware protection to a defense-in-depth security posture, addressing the pervasive risk of known and unknown vulnerabilities in software-based security solutions. Hardware-enforced network segmentation uses unidirectional technologies, such as unidirectional gateway or data diodes (NIST SP800-82 revision 3).

Examples of remote access using hardware-enforced network segmentation include:

- Unidirectional remote screen view transmits real-time screen images through unidirectional hardware to remote service technicians. Those technicians can then provide on-site personnel with real-time advice to diagnose and correct complex problems.
- Remote access systems, with unidirectional hardware controls channels for keystrokes and mouse movements, are independent of unidirectional monitoring channels for screen images and provide stronger protections than software-only systems.[6]

In both cases, time-limited hardware switches that enable temporary bidirectional remote access may be appropriate to deploy in parallel with unidirectional solutions and in series with software-based remote access security solutions. These time-limited switches provide personnel at protected sites with physical control over how long software-based remote access is enabled.

BEST PRACTICES

SASE, SSE, and hardware-enforced network segmentation provide organizations the potential to replace traditional VPNs and security features and foster policies that offer a zero trust approach to modern security implementation. The authoring organizations encourage all entities to carefully assess your security posture and perform a risk analysis before implementing any/all solutions to determine if these approaches fit your organization.

In addition to implementing ZT, SASE, SSE, and hardware-enforced solutions, the authoring organizations strongly encourage entities to apply the best practices listed below. These best practices align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and NIST. The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement.

Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline practices.

- **Implement a centralized management solution.** Having centralized management allows system administrators the ability to control remote access to applications and servers, manage privileged access, and simplify network control. Without the ability to deploy, monitor, and manage through one centralized point, the cost associated with technical support, troubleshooting VPN connections, and support of the VPN client increases. The ability to monitor and manage your VPN environment is critical to modern network defenses due to the underlying issue that no VPN can guarantee absolute security. Additionally, if a data breach occurs due to user error or third-party vendors, an organization cannot readily prove the origin of the issue without the aforementioned centralized access to data identifying the user, application, and/or connection.[7]
- **Implement network segmentation**. All connections to OT networks are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality [CPG 2.F]. Boundaries should be unidirectional for the most consequential systems, communications, and remote access systems at consequence. See joint advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems for more information.
- **Implement Security Orchestration, Automation, and Response (SOAR)** by implementing an automated response to certain security events.
- **Develop, maintain, update, and regularly drill IT and OT cybersecurity incident response plans** for both common and organizationally specific scenarios and procedures. Response plans should be updated within a risk-informed time frame following the lessons learned portion of any exercise or drill [CPG 2.S].
- **Automate and validate vulnerability scans on all public-facing enterprise assets**. Implement appropriate compensatory controls to prevent common forms of abuse and exploitation. Disable all unnecessary OS applications and network protocols on public-facing assets [CPG 2.W].
- **Use well-tested, high-performing cybersecurity solutions** to automate the detection of unsuccessful login attempts [CPG 2.G].
- **Integrate an incident detection system** to help prioritize incidents [CPG 3.A]. Integrate systems that immediately block access to compromised devices suspected of being malicious and disconnect established connections to systems.
- **Deploy security.txt file** to allow security researchers to submit discovered weaknesses or vulnerabilities in a timely manner. All public-facing web domains should have a `security.txt` file that conforms to the recommendations in Request for Comments (RFC) 9116 [CPG 4.C]. Organizations should also have a properly defined and organizationally supported vulnerability disclosure policy, which supports the `security.txt`.
- **Regularly back up all systems that are necessary for daily operations**. Backups should be stored separately from the source systems and tested on a recurring basis—no less than once per year [CPG 2.R].

- **Have annual trainings on basic security concepts** (such as phishing, business email compromise, basic operational security, password security, etc.) and make them mandatory for all employees and contractors to foster an internal culture of security and cyber awareness [CPG 2.I].
- **Implement a strong identity and access management solution** that verifies identity with phishing resistant multifactor authentication (MFA) [CPG 2.H].
- For the most consequential systems, **use hardware-enforced unidirectional technology** to push forensic, audit, and other security data from sensitive networks to IT-based or cloud-based SOAR security and access monitoring systems. This hardware application mitigates cyberattacks pivoting through the cloud or internet back into protected networks through the unidirectional hardware [CPG 2.Q].
- **Permit access based upon the principles of least privilege**. Users should only have access to resources that are needed on a just-in-time basis. Users and devices need to be identified and verified in a strict manner for each access request [CPG 2.E].
- **Establish an adoption roadmap and deployment strategy**. Brainstorm how SASE benefits your organization based on the SASE objectives [CPG 5.A].
- **Draft a flexible SASE roadmap** where every capability has a strong plan behind it. With SASE, this strategy consists of combining IT with business-oriented goals. Each organization must give input on what benefits SASE has for its business needs [CPG 5.A].
- **Place collaboration, strategies, technologies, and applications into a testing environment** before going fully operational with SASE solutions [CPG 2.S].
- **Implement technical security measures to protect your organization, such as Mail Transfer Agent Strict Transport Security (MTA-STS)**—which provides strict encryption to mail traffic sent to a domain. Use DNS-based authentication of named entities (DANE), which allows network administrators to bind Transport Layer Security (TLS) certificates to domain names.[8]
- To prevent the entire system from being exploited and to protect sensitive information, **only grant specific remote-user access as it pertains to the user's role within the organization** [CPG 2.W].
- **Use FWaaS** to protect your organization's digital assets from web-based threats [CPG 2.Q].
- To increase network security, **use ZTNA to limit user access and applications** via a trust broker [CPG 2.X].

Organizations should conduct the following when transitioning from VPN solutions to SSE/SASE (bearing in mind that migration may take proper planning and sequential implementation):

- Prevent access to the control plane.
- Use a dedicated management interface.
- Patch, generate, and analyze network telemetry related to the VPN solution.
- Consider pre-authenticating users.
- Use MFA.
- Version control the running configuration (i.e., actively look for device configuration changes).

Following these best practices and initiating a complete assessment of an organization's security posture can effectively help organizations implement SASE and SSE solutions. These solutions help organizations enhance security capabilities, access cloud resources more securely, and support a more robust approach to network security while ensuring compliance with regulatory requirements.

REFERENCES

[1] Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN | Volexity

[2] Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | CISA

[3] #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability | CISA

[4] Ending the Zero Trust, SSE, and SASE Confusion

[5] What Is SASE? - Palo Alto Networks

[6] Segmentation 202: Unidirectional Architectures – Waterfall Security

[7] 7 common VPN security risks: the not-so-good, the bad, and the ugly | Imprivata

[8] Implementation guidance: email domain protection (ITSP.40.065 v1.1) - Canadian Centre for Cyber Security

RESOURCES

- CISA's Cloud Security Technical Reference Architecture Version 2
- CISA's Implementing Phishing-Resistant MFA
- CISA's Trusted Internet Connections (TIC)
- CISA's Zero Trust Maturity Model
- Implementation guidance: email domain protection (ITSP.40.065 v1.1)
- Guidance on securely configuring network protocols (ITSP.40.062)
- Managing edge devices: Five Challenges and recommendations when using edge devices

ACKNOWLEDGEMENTS

Waterfall Security contributed to this guide.

DISCLAIMER

The United States Government, through CISA of the Department of Homeland Security (DHS), and the authoring organizations, do not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise is

provided for informational purposes and does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the authoring organizations.