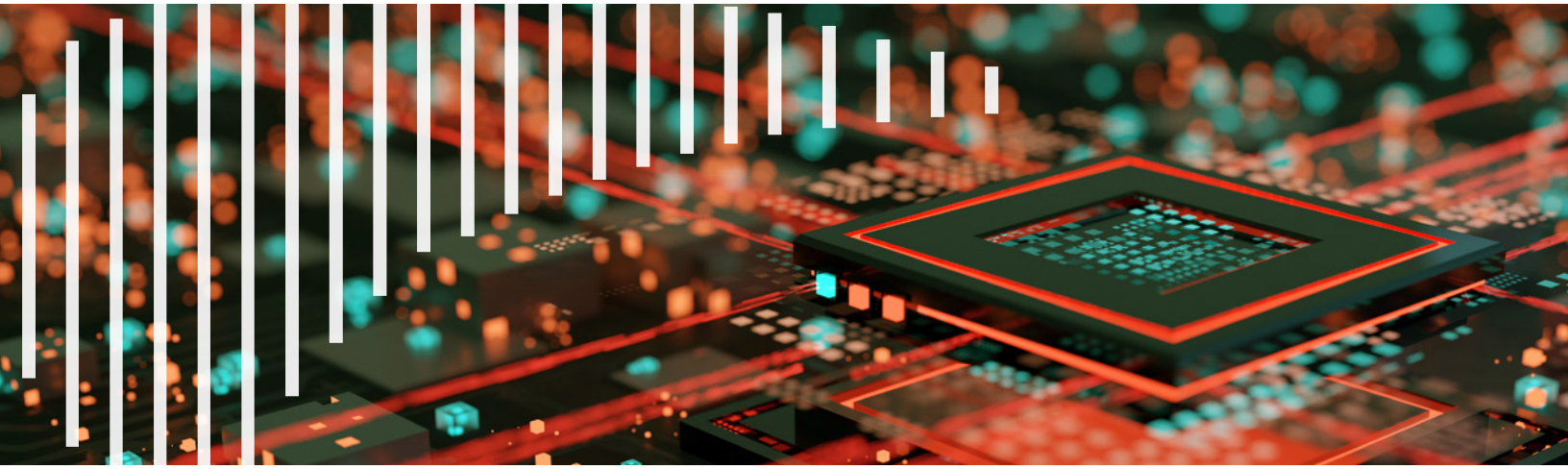
SONICWALL®



How Secure is Your Closed Network?

A closed network is not an invincible network. Here's how to identify and fill the security gaps in your isolated environment.

What is a closed network?

In a typical network, endpoints are free to connect to the internet and to one another, allowing data and information to travel more or less freely. This model has many advantages for productivity, communication and collaboration, but it also has a number of downsides — including the possibility of data leakage and theft, malware, intrusion attempts and more.

In contrast, a closed network is typically isolated and has no connection to the outside public. Closed networks are often used by those who handle highly sensitive or classified information — for example, the U.S. Department of Defense (DoD) operates many closed networks. These networks, also known as secure or classified networks, are used to safeguard and control access to sensitive military information and systems.

Because they play a crucial role in protecting classified information, supporting secure communications and enabling military operations, these networks are a critical component of the DoD's overall strategy. As such, they're subject to rigorous security standards and controls to safeguard national security interests.

The role of cybersecurity in closed network environments

The implementation of such safeguards is typical in the sorts of environments that require closed networks. With all these security standards and policies protecting them, closed networks seem much more secure than open networks — but should cybersecurity still be a concern within a closed network environment?

The answer to that question depends on your unique deployment, but in many cases, the answer is "yes." Here are a few reasons to consider securing your closed network:

1. Insider Threats: Closed networks typically have authorized users, who have access to the network and its resources. However, these users can still pose a threat if they misuse their privileges or if their accounts are compromised. Insider threats can result in data breaches, unauthorized access and other malicious activities.
2. Vulnerabilities and Exploits: Closed networks are not immune to vulnerabilities and exploits. The software and systems used in closed networks can still have vulnerabilities that can be exploited by attackers. Without proper security measures, these vulnerabilities can be leveraged to gain unauthorized access or disrupt network operations.
3. Physical Security Breaches: While closed networks may have restricted access, there is still a possibility of physical security breaches. If an unauthorized individual gains physical access to the network infrastructure or devices, they can compromise the network's security.
4. Malware and Viruses: Closed networks can still be affected by malware and viruses. These malicious programs can enter the network through various

means, such as infected external devices, compromised software updates or social engineering attacks on authorized users. Once inside, malware can propagate and cause damage to the network and its resources.

5. Data Leakage: Even in a closed network, sensitive data may need to be shared or transmitted to external entities, such as partners, suppliers or clients. If proper security measures are not in place, there is a risk of data leakage during these interactions. Additionally, data within the closed network itself may still be at risk if not adequately protected.
6. Regulatory Compliance: Depending on the nature of your organization or the industry you operate in, there may be regulatory requirements for maintaining a secure network environment. Failing to comply with these regulations can result in legal and financial consequences, even in closed networks.

The role of cybersecurity in closed network environments

If any of these factors apply to your network, it's important to take stock of what you need to protect as well as your organization's unique risk profile. This will help you determine the correct type and level of protection. There are some key things to consider when building a security strategy for a closed network:

1. Physical Security:
   - » Ensure that physical access to the network infrastructure is strictly controlled. Use access controls, locks, surveillance cameras and alarm systems to protect the network equipment and server rooms.
   - » Limit the number of individuals who have physical access to the network and maintain a visitor log.
   - » Consider employing security guards or personnel to monitor and control access to the network facility.
2. Access Control:
   - » Implement strong authentication mechanisms, such as multifactor authentication (MFA), for all users accessing the network. This could include the use of smart cards, biometrics or other approved authentication methods.
   - » Maintain a strict user access policy and enforce the principle of least privilege, granting users only the permissions necessary to perform their specific duties.
   - » Regularly review and update user access rights to ensure they are both current and appropriate.
3. Encryption:
   - » Use strong encryption algorithms to protect data in transit and at rest. Implement encryption protocols such as IPsec (Internet Protocol Security) or TLS (Transport Layer Security) for network communications and secure file storage.
5. Network Monitoring and Intrusion Detection:
   - » Deploy intrusion detection and prevention systems (IDS/IPS) to monitor network traffic for any signs of unauthorized access or malicious activity.
   - » Utilize security information and event management (SIEM) solutions to aggregate and analyze log data from various network devices, servers and applications. This will allow you to detect security incidents more quickly.
6. Security Patching and Updates:
   - » Regularly update and patch all network devices, servers and software to address known vulnerabilities.
   - » Establish a process to promptly apply security patches and updates to minimize the risk of exploitation.
6. Security Awareness and Training:
   - » Conduct regular security awareness programs to remind employees about the importance of security practices and the potential risks associated with classified information.
   - » Train employees on safe computing practices, including the identification of social engineering attempts and the proper handling of sensitive data.
7. Incident Response:
   - » Develop and maintain an incident response plan that outlines the steps to be taken in the event of a security breach or incident.
   - » Establish procedures for reporting and responding to security incidents, including roles and responsibilities; communication protocols; and steps for containment, investigation, and recovery.

How can SonicWall help cover the gaps?

The safest way to protect closed networks and the sensitive data they contain is by deploying a multi-layer security strategy.

One layer should consist of a firewall, which will allow you to divide your network into separate security zones or segments and to take advantage of access control lists (ACLs). Doing so will allow you to regulate traffic and enforce strict rules on communications.

Many firewalls can also inspect east-west traffic and internal VLAN traffic, and this is important in a closed network as well. No network is without vulnerabilities, and without this inspection, your network could be breached without administrators being aware.

While SonicWall has a full line of firewalls that provide Reassembly-Free Deep Packet Inspection (RFDPI) for any size network, the requirements of keeping all traffic within a network boundary can limit some of the functionality of a cloud sandbox approach. To bring our most powerful inspection weapon to those who are unable or unwilling to employ cloud-based inspection, SonicWall has introduced the Capture Security Appliance (CS*a*).

CS*a* offers SonicWall's patented Real-Time Deep Memory Inspection (RTDMI™) in a single 1U, on-prem appliance. RTDMI is capable of blocking zero-day and unknown threats at the gateway — even those that hide their weaponry via encryption or have not yet exhibited malicious behavior. Using CS*a* with any of our firewalls will increase real-time visibility of your critical infrastructure, bolstering security.

It's important to note that the specific security requirements for classified networks can vary depending on the classification level and the governing authority. Therefore, it is crucial to consult with security professionals and follow any specific guidelines or regulations provided by the relevant governing body in your jurisdiction.

If you would like more information on securing your closed network, please contact a SonicWall security expert.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

Misc-FY24ClosedNetworks-JK-8858