xage SECURITY

POLICY-BASED CONTROL

OVER UNIDIRECTIONAL AND BIDIRECTIONAL DATA FLOW

Introduction

A Better Way Of Controlling the Direction of Data Flow Into and Out Of Highly Secure Environments

Operational ability to control the direction of data flow is one of the established best practices for securing contested networks. Depending on the organizational operational, security and business needs, there are different variations of controlling the direction of the data flow. For example, to protect a highly secured network from external attacks, organizations restrict the transfer of data from secured networks to unsecured networks, and strictly disallow the reverse. Other organizations that want to stop any exfiltration of sensitive data from a confidential network would allow data into the confidential network, however, would strictly disallow any movement of confidential data to unsecured networks.

Whether the organizations decide to only allow data into their secured networks or only allow data out of their secured networks, they can improve their network security posture to some extent. However, they lose a lot of operational flexibility by using traditional methods for this. For example, when organizations adopt a solution that only allows data to flow in one direction, from secured networks to unsecured networks, they lose the ability to remotely access assets in the secured network. This means they are unable to maintain their critical business assets remotely, as that would require a connection from the unsecured network into the secured network.

An ideal solution would allow organizations to control the direction of data flow at a granular level so they can simultaneously protect and maintain their mission critical networks and assets.

© Xage Security 2023 | All Rights Reserved

xage

Existing Solutions and Challenges: The Many Problems with Data Diodes

Historically, data diodes and unidirectional gateways have partially served the purpose by strictly restricting the flow of data in a single direction. However, they also create a plethora of operational challenges for the organizations. Some of the challenges introduced by data diodes include:

1. **Impossibility of remote access and multi-user session collaboration:** In the post-COVID era, the ability to remotely connect and do multi-user session collaboration are required for achieving business continuity. However, data diodes make this difficult or impossible, as all such remote operations are TCP based and require a 2-way network connection handshake.

2. **Inability to update or patch:** Since data diodes and unidirectional gateways are meant to be one-way only, updating or patching the critical infrastructure assets with new security measures or software updates won't be possible remotely. This can leave assets vulnerable to new and emerging cybersecurity threats, and constantly requires technicians to patch the systems by physically going to the corresponding sites, which will increase costs and is not scalable.

3. **Dependence on hardware:** Data diodes and unidirectional gateways are hardware-based devices to achieve the desired physical security, which means that they can be expensive, difficult to implement, often require careful configuration and testing to ensure that they are working properly and may require costly upgrades to maintain security. Additionally, they are not applicable in cloud deployments. With the advent of Gov Clouds and intelligent clouds, more classified data and data centers are moving to the cloud, where these hardware-based tools will be a non-starter.

4. **Unable to protect data integrity inside secure environments:** While data diodes and unidirectional gateways prevent data from entering more secure networks from less secure networks, they do not necessarily prevent attacks from occurring on the more secure side of the network in the first place. If the attackers gain access to the more secure network, these data diodes are unable to detect any tampering of the data and are also unable to stop the attackers from accessing the business-critical assets from inside the more secure network zones and sites.

5. **Physical switch override:** Many data diode vendors can provide a physical switch to turn off the one-way data flow enforcement, enabling two-way data flow. This ultimately creates the need for physical security to prevent an operator from manually opening a high-side network and exposing it to a potential breach.

6. **Obstacles to cybersecurity modernization practices:** Data diodes and unidirectional gateways, while they can be effective at preventing certain types of attacks, break other cybersecurity requirements by impeding the ability of security personnel to remediate or perform live forensics via centralized EDR/XDR/SOAR tools. To adopt modern security tooling, organizations end up deploying alternate network paths and access methods such as USBs and Access Gateways. Giving such tools access into the secured networks circumvents the whole purpose of data diodes, which can result in a false sense of security. Additionally, data diodes and unidrectional gateways can make it impossible to insert multifactor authentication (MFA). MFA is one of the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-sector performance goals (CPGs) for critical infrastructure. Critical infrastructure providers that want to achieve the CPGs will find data diodes to be a stumbling block.

© Xage Security 2023 | All Rights Reserved

The Xage Security Solution

Xage introduces a new type of solution that enables highly customizable and granular control of data flow while enabling secure remote access and identity-based access control to the data. In addition to controlling the flow of data at a per user, application and device level, the Xage Fabric also protects all business-critical assets from any unauthorized access, either remotely or from the local site, even when the attacker may have breached the physical security of the network. The Xage Fabric is a highly configurable, granular, and policy-based Zero Trust Access Control and Data Security solution that not only allows organizations to control the direction of the data flow, but also protects that data's integrity. Here are some of the key advantages of Xage's solution:

1. **Policy based data flow direction enforcement:** Xage's solution can not only enforce unidirectional data flow but can also enforce that at a per device, user, application level via central policy management. This allows organizations and administrators to segment the direction of the data flow based on the business needs. For e.g. policies can be defined that would deny all incoming data from any user and/or application from an unsecured network into the secured network, however, would allow a trusted technician to make a secure connection through the Xage fabric via multi-hop encrypted tunnels to a secured device inside the secured network to apply a patch.

2. **Data identity and fingerprinting to protect data integrity:** Each data object as it passes through the Xage fabric is hashed at the ingress points and verified cryptographically at the egress point to ensure the data integrity. This allows organizations to prove the authenticity of the data transferred across the network.

3. **Secure file transfer** with authenticity, integrity, filtering, granular control on destination along with malware scanning.

4. **Secure data transfer via multi-hop encrypted tunnels:** Data always flows through encrypted tunnels that provide security from any man-in-the-middle attacks that otherwise pose a rise of data tampering. Optionally, data can be encrypted using Xage generated key or customer provided external key.

5. **Remote access and Session collaboration in conjunction with one-way data movement:** One of the biggest advantages of Xage's solution is that it can selectively allow 2-way interactions between pre-configured, and policy based trusted users and devices utilizing Xage Fabric multi-layer proxy and protocol break that blocks malware and ensures authenticity and integrity. This allows organizations to remotely access or collaborate on their assets without compromising the security.

6. **Secure Administrative console access with MFA and YubiKey hardware token:** Xage's solution provides hardware level security assurance to protect its policy management via hardware token-based MFA to allow authorized access only.

7. **Equally applicable to on-premises, private cloud, and public cloud deployments:** Given Xage's solution doesn't require hardware and can be deployed on an array of virtual form factors, it allows organization to enforce unidirectional data flows even in the case of public cloud.

© Xage Security 2023 | All Rights Reserved

8. **Enforce remote and local access policies at the individual device level, even if a site goes offline:** The Xage Enforcement Point (XEP) is an optional hardware appliance that can be installed as a bump in the wire for even more granular control. This empowers organizations to protect their business critical assets in the secured networks against any attack, even if the attackers somehow get into the secured site. This provides protection against attacker intrusion from outside, as well as against lateral movement in the East-West corridor. Blocking these tactics, techniques, and procedures (TTPs) that attackers use to proliferate and expand their footprint is a vital step in preventing attacks from working at all, instead of just detecting them in the aftermath.

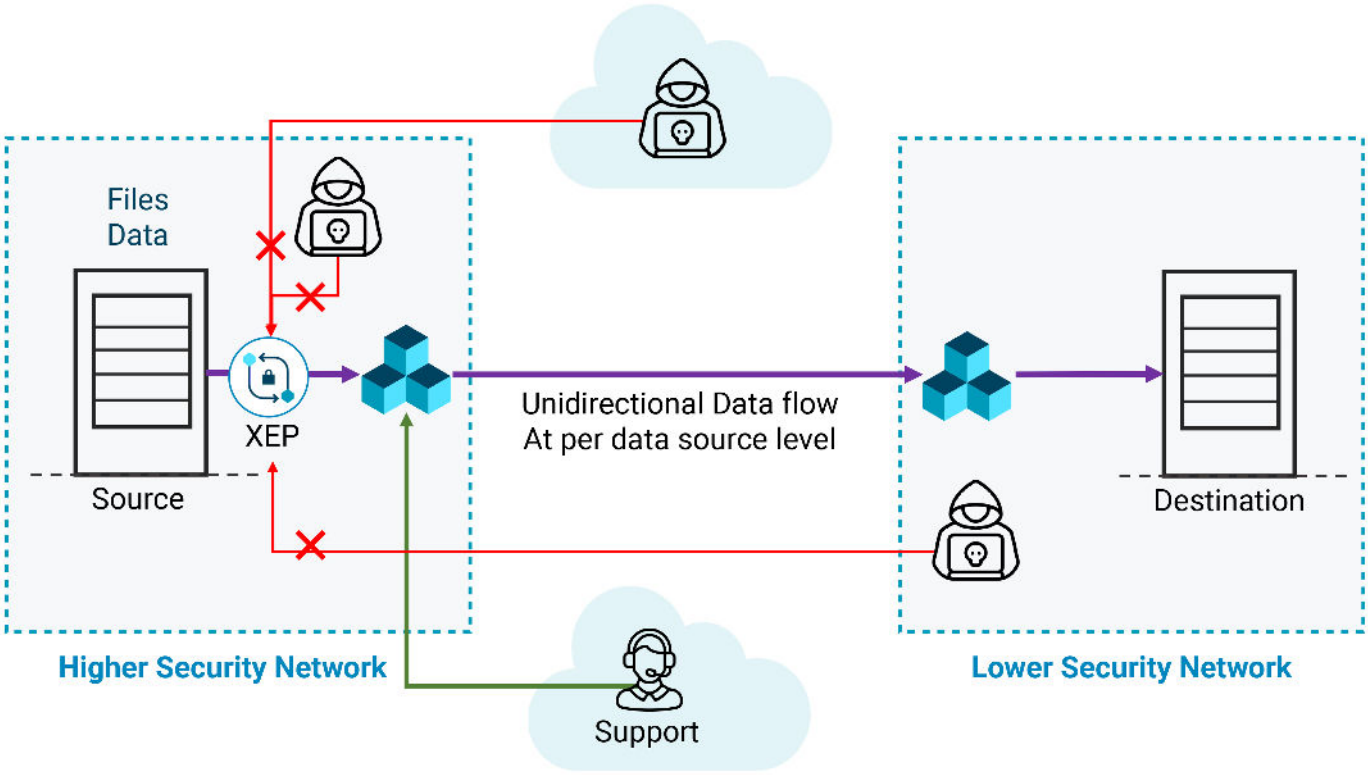

Figure 1: The Xage Fabric enables control of data-flow direction without creating obstacles to security modernization.

Automatic, Distributed, Non-disruptive Deployment

The Xage Fabric protects all digital interactions between users, data, and assets without requiring disruptive changes or the replacement of existing infrastructure. Distributed deployment of the Xage Fabric is fully automated and can be completed in a few hours.

Xage's Zero Trust Data Exchange and Identity-based Access Management solutions together empower organizations to not only control the data flow across the networks at a granular level, but also protects the assets even if the attackers breach the highly secured network. Xage doesn't just detect attacks, it prevents them to protect every asset and piece of data in your environment.

© Xage Security 2023 | All Rights Reserved