

OPSWAT.

WHITEPAPER

Cracks in the Armor

Firewall Vulnerabilities in Today's Threat Landscape





Executive Summary

Securing critical networks is becoming increasingly more important and—simultaneously—more complex. As the previously clear distinction between Information Technology (IT) and Operational Technology (OT) networks continues to erode and the overall attack surface expands, the tools the cybersecurity industry has relied on for decades are becoming ineffective alone against mitigating the precision of modern cyberattacks. The sophistication and frequency of cyberattacks are evolving rapidly, which means the methods put in place to meet them head on must follow suit. This brings us to the concept of firewalls. Traditional firewalls, once considered bastions of cybersecurity, have revealed vulnerabilities causing major concerns for organizations, their employees, and those they serve.

This whitepaper aims to advocate for security gateways, and more specifically OPSWAT's NetWall, by highlighting challenges associated with traditional firewalls and how the technology that underpins and powers NetWall can help protect networks by ensuring the secure transfer of critical data.

Table of Contents

01	A Brief History of Firewalls
02	Challenges with Traditional Firewalls
03	Compliance Mandates
04	OPSWAT NetWall: Next-Level Security Gateway and Data Diode
05	Defense-in-Depth Cybersecurity

01

A Brief History of Firewalls

Firewalls have a rich history dating back to the early days of computer networking. The concept of a firewall, in its simplest form, emerged as a response to the need for security in the growing networked computing environment. The term “firewall” was originally borrowed from the physical world, where it referred to a wall designed to contain fires within a building. In the context of computer networks, a firewall was envisioned as a security barrier that could control the flow of data between a trusted internal network and untrusted external networks, such as the nascent internet. The first-generation firewalls primarily focused on packet filtering, allowing or blocking network traffic based on source and destination IP addresses and port numbers.

Over time, firewalls evolved in response to the increasing complexity of cyberthreats and the expansion of networked environments. Second-generation firewalls introduced stateful inspection, which allowed them to track the state of active connections and make more intelligent decisions about allowing or denying traffic. The advent of application-layer gateways and proxy servers marked the third generation of firewalls, enabling deeper inspection of network packets and application-level filtering. In the late 1990s and early 2000s, the rise of e-commerce, increased internet connectivity, and the proliferation of cyberthreats led to the widespread adoption of firewalls in both corporate and home network settings.

Today, firewalls are one of the most commonplace appliances in network security and they can be found in virtually every networked environment.




02

Challenges with Traditional Firewalls

The proliferation of firewalls is partly the reason why they present a series of challenges in the modern cybersecurity landscape; threat actors have learned to target these often-vulnerable and seemingly always-present devices in order to gain access to essential networks and exfiltrate critical data. What follows are some of the more common challenges with traditional firewalls.

Zero-Day Vulnerabilities

Traditional firewalls can be vulnerable to zero-day threats, or unknown flaws with no available patch—some specific examples include:

 <p>In September of 2023, research conducted by VulnCheck identified that nearly 12,000 Juniper firewall devices were vulnerable to CVE-2023-36845. This exploit can allow unauthenticated threat actors to execute arbitrary code on Juniper firewalls without creating a file on the system, putting critical networks at risk.</p>	 <p>Known as CVE-2019-8452, a vulnerability was found allowing attackers to gain unauthorized access to information and execute arbitrary code. This issue could potentially be exploited to compromise secured environments and extract sensitive data.</p>	 <p>Over the years, Fortinet has encountered several vulnerabilities. One such instance, CVE-2018-13379, permitted remote code execution without authentication. Malicious actors could exploit this vulnerability, leading to unauthorized access and data breaches.</p>
--	---	--

Discover more about specific CVEs directly tied to firewalls.

[Read Blog](#)



Configuration Errors

We're all intimately familiar with the saying, "a chain is only as strong as its weakest link." Unfortunately, when it comes to the world of cybersecurity, the aforementioned weakest link is almost always the human element. Beyond zero-day vulnerabilities, traditional firewalls face the challenge of human error in configuration and improperly configured firewalls can lead to a range of cybersecurity consequences. Here are some examples of cyberthreat impacts that may result from firewall misconfiguration:

- Expanded Attack Surface** The last thing we want is to widen or expand the attack surface; a simple misconfiguration allowing vast IP address ranges can lead to potential exposure to malicious actors.
- Unauthorized Access** If a firewall is misconfigured to allow traffic that should be blocked, it can grant unauthorized users or threat actors access to sensitive systems, data, or resources within the target's network. This can lead to data breaches, unauthorized system modifications, and other security incidents.
- Data Exfiltration** Improper firewall configuration may fail to detect or block outbound traffic originating from malware or attackers. This can enable data exfiltration, where sensitive information is sent outside the organization's network without detection. Data loss and compliance violations may occur as a result.
- Malware Infection** A misconfigured firewall can inadvertently permit malware to enter the network, as it may not block known malicious sources. Once inside, malware can propagate, compromise systems, steal data, and carry out other malicious activities.

- Denial-of-Service (DoS) Attacks** Mistakes in a firewall's configuration may not effectively mitigate DoS or Distributed Denial-of-Service (DDoS) attacks. Attackers can overwhelm network resources, causing service disruptions, downtime, and potential financial losses.
- Lateral Movement** Inadequate segmentation due to firewall misconfigurations can enable lateral movement within the network. Once attackers gain access to one part of the network, they may exploit misconfigured firewall rules to move laterally, also known as "living on the land," and compromise additional systems.
- Policy Violations** Firewalls are often used to enforce security policies and compliance requirements. Misconfigurations can result in policy violations, potentially leading to regulatory penalties, fines, or legal liabilities.
- Security Gaps** Firewall misconfigurations can create gaps in security, allowing attackers to exploit weaknesses and evade detection. These gaps are often not apparent until a security incident occurs and it is too late.
- Loss of Trust** Firewall misconfigurations erode trust in the overall security infrastructure. Users—and customers—may lose confidence in the organization's ability to protect their data, leading to permanent reputational damage.
- Outdated Rules** Organizations need to regularly review and update their firewall configurations, neglecting to update or decommission outdated rules can cause additional security vulnerabilities.
- Bi-Directional By Design** Firewalls are designed for data to flow through in both directions. Aside from the inherent risk of sharing routable information between networks, when one-way data transfers are needed, a misconfigured firewall can open some of the most critical networks to disastrous vulnerabilities.
- Elevated Cost** Ultimately, any combination of manually mitigating or responding to these vulnerabilities leads to a ballooning operational cost for the organization or entity.

03

Compliance Mandates

Critical industries are no strangers to regulation. As cyberattacks and their consequences continue to rise in severity, governing bodies are being tasked with ensuring that organizations are doing their part to stay protected. Aside from not following best practices and being vulnerable to attack, non-compliance also means fines—sometimes upwards of \$1 Million USD daily. And when it comes to the topic of regulation and compliance mandates firewalls are, simply put, not enough. In order to make certain of the safety of critical data and networks, many key regulations stipulate the use of unidirectional gateways or data diodes to ensure data integrity and security. What follows are mandates that factor in the use of security gateways and/or data diodes:



NERC CIP

This regulates security standards for North America's bulk electric system, with some standards necessitating unidirectional gateways for data communication between networks.

Nuclear Regulatory Commission (NRC)

The NRC has guidelines for the nuclear power industry, emphasizing the importance of data diodes for securing critical systems.

ISA/IEC 62443

These standards, designed for industrial automation and control system security, advocate the use of unidirectional gateways.

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework emphasizes the importance of network segmentation to isolate critical assets from less trusted parts of the network. Data diodes or security gateways are recommended to achieve this segmentation, helping organizations align with NIST guidelines.

ISO 27001 [Information Security Management System]

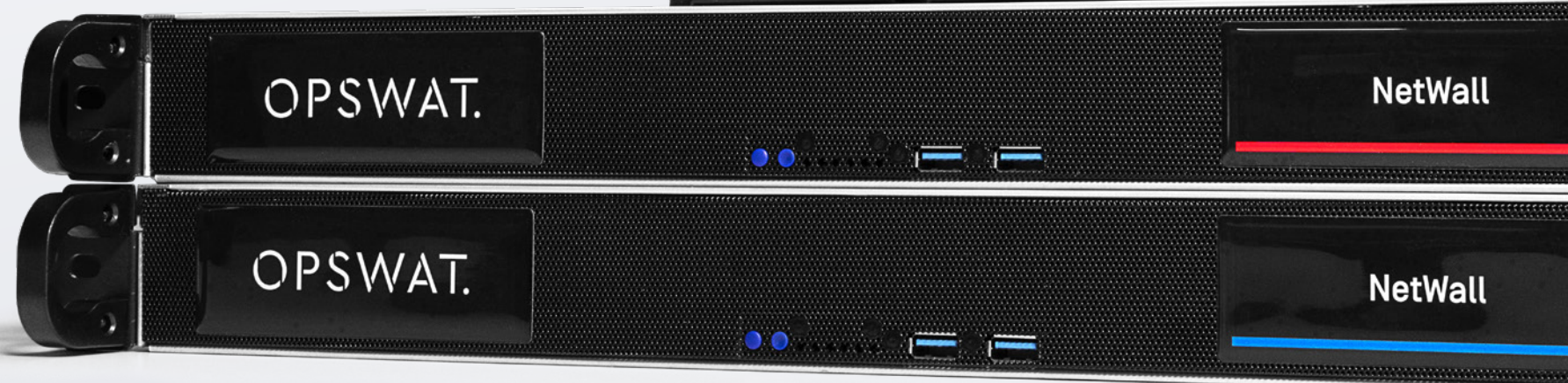
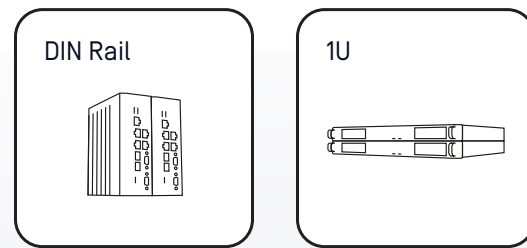
ISO 27001 is an international standard for information security management. Organizations should strongly consider the use of data diodes or security gateways to meet the standard's requirements for secure data access and controlled communication between networks.

04

OPSWAT. NetWall® Series

Next-Level Security Gateway and Data Diode

Taking into consideration the totality of challenges and vulnerabilities that face traditional firewalls and the air-gapped networks they stand to protect, OPSWAT has developed NetWall. Offered in a variety of simple to use form-factors and models, NetWall Security Gateway or Optical Diode puts unprecedented control over data flow in the hands of the organization—all backed with patented technologies trusted globally to defend some of the world’s most critical environments.



Key Advantages

Unidirectional Data Flow

OPSWAT NetWall USG and Optical Diode facilitate unidirectional data flow, ensuring that data moves only from one network side to the other—and does it reliably. This design prevents potential unauthorized access or data leakage.

Minimized Human Error

The inherent design of each OPSWAT NetWall vastly reduces the chances of configuration mishaps thanks to a user-friendly design.

Scalability

With 100 Mbps, 1 Gbps, or 10 Gbps throughput options, OPSWAT NetWall is highly scalable to meet current and future requirements.

Compliance Compatibility

The shift in mandates towards security gateways and data diodes positions OPSWAT NetWall to help organizations meet industry standards such as: NERC CIP – NIST CSF, ICS, 800-82, 800-53 – IEC 62443 – NRC 5.71 – CFATS ISO 27001, 27032, 27103 – ANSSI – IIC SF, and more.

Full Support for Industrial Protocols

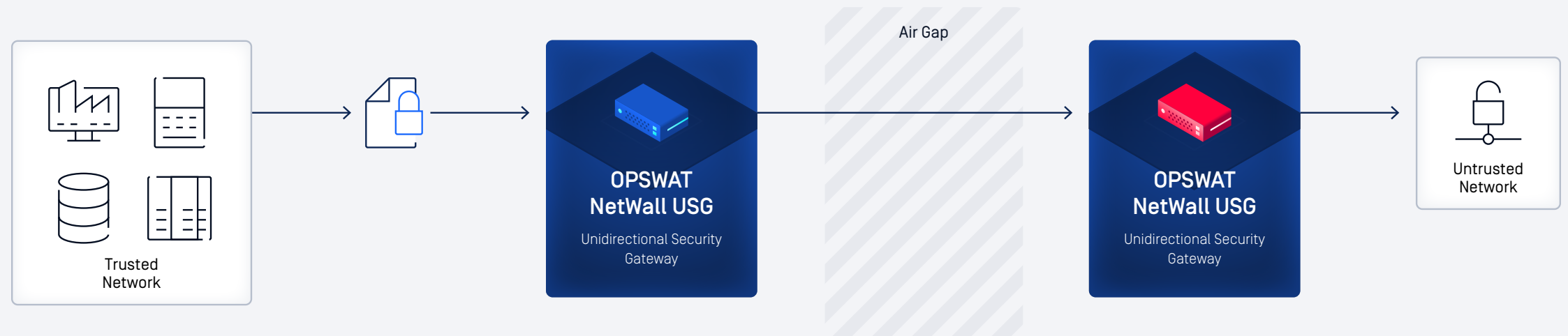
OPSWAT NetWall exceeds industry standards with support that includes TCP, UDP, HTTPS, FTP, SFTP, FTPS, SMB, Windows file Share, CIFS, SMTP, Video, AVEVA PI, Modbus, OPC DA/AE/UA, MQTT, DNP3, IEC-104, and Screen View.

The Right NetWall for the Challenge

OPSWAT NetWall was designed with integration and support in mind—that's why we have a NetWall for every scenario:

NetWall Unidirectional Security Gateway (USG)

Enables secure unidirectional OT/IT data transfers using a patent pending assured data delivery mechanism, with the full benefit of speed, low latency, and functionality with complete reliability and no data loss.



NetWall Bilateral Security Gateway (BSG)

Performs real-time replication of the data (with no data loss) and uses a bilateral mechanism to handle data responses without compromising the security and integrity of the OT network.



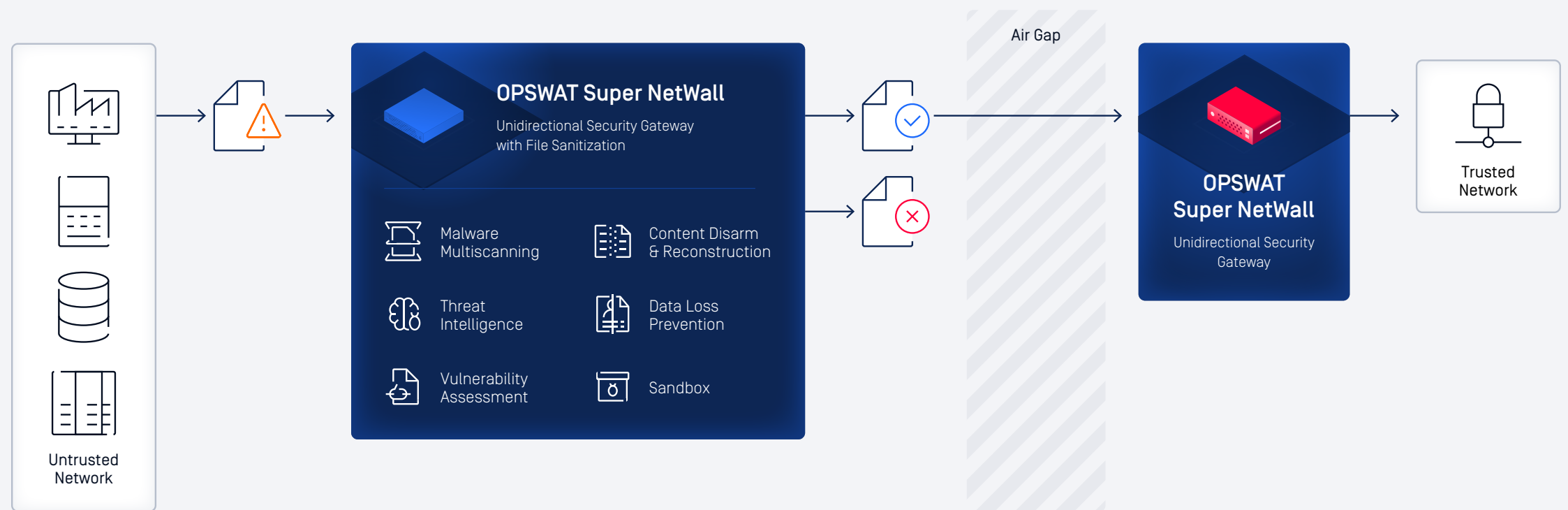
NetWall Optical Diode

Provides a hardware-enforced unidirectional transfer of real-time OT data and enables secure IT-OT data transfers over a reliable, high speed, low latency optical link.



Super NetWall

Assures uncompromising security for IT/OT communications—especially for moving files, patches, and software updates by providing a secure file scanning and transfer solution that delivers unsurpassed performance, reliability, and security with built-in MetaDefender technology.



05

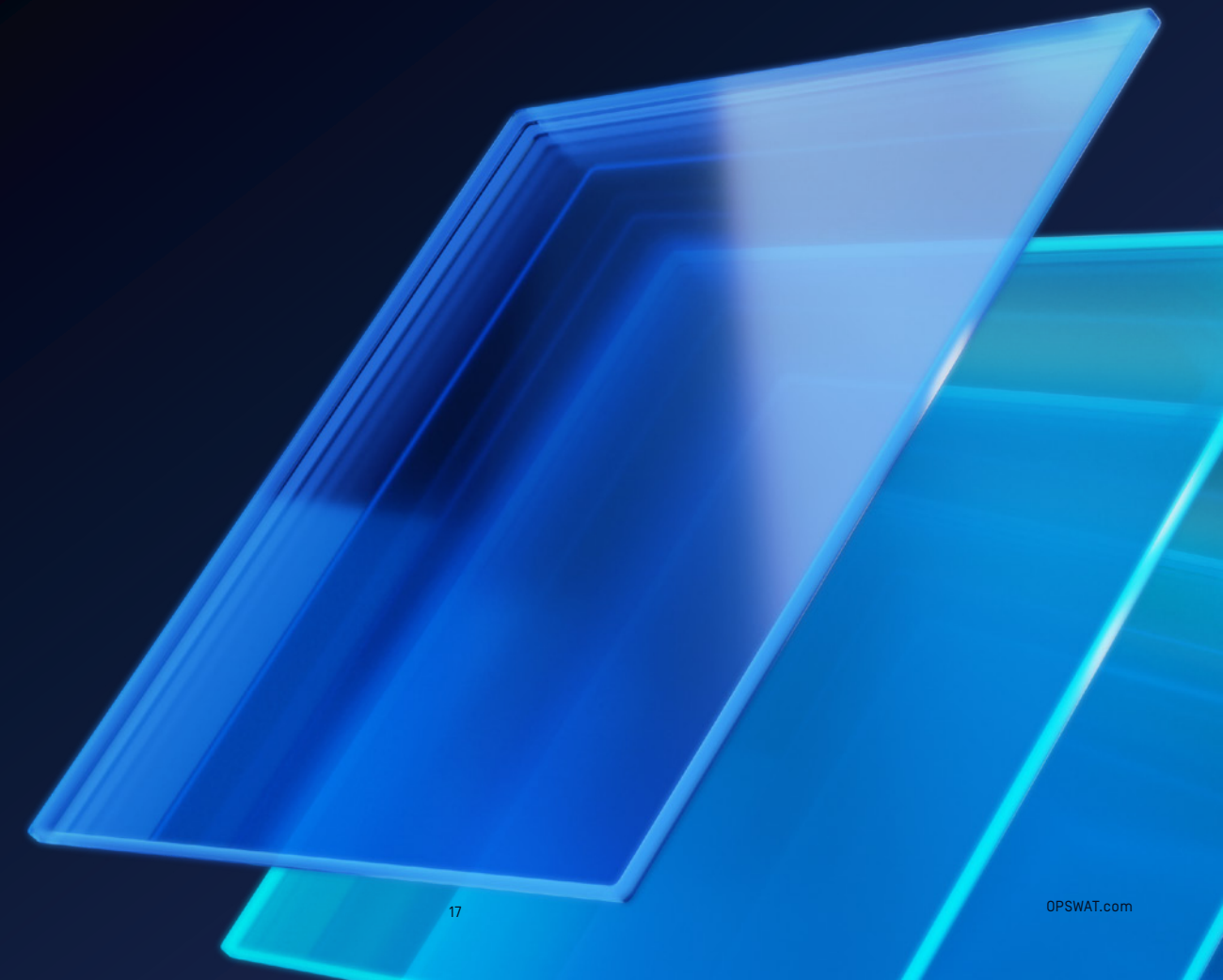
Defense-in-Depth Cybersecurity

So ultimately, what does the future hold for traditional firewalls? For starters, there's no panacea when it comes to cybersecurity, so even those with the most mature postures will still find usefulness in them. In a well-designed defense-in-depth cybersecurity strategy, a multi-layered perimeter of defense is constructed around critical and/or air-gapped environments—shrinking the attack surface and limiting points of entry for threat actors. With that in mind, traditional firewalls still have a role to play; by leveraging the added protection of a NetWall Optical Diode or USG sitting inside the DMZ and placing firewalls on either side, together they add additional lines of defense against threats.

Conclusion

While traditional firewalls have historically been the frontline defense and were once considered the north star of network protection across key verticals, evolving threats and industry requirements have necessitated more fortified solutions. Traditional firewalls can no longer be relied upon the way they were in the past—especially when it comes to securing the world's most critical environments; simply put, a strong solution is not a "nice to have," but a crucial investment for every organization. OPSWAT NetWall addresses the vulnerabilities and challenges traditional firewalls present, making it a compelling choice for safeguarding critical networks.

Discover how OPSWAT NetWall can level-up overall security posture and provide peace of mind knowing that the transfer of critical data is under control and safe. Talk to one of our experts today about a free demonstration.



GET STARTED

Are you ready to put OPSWAT on the front lines of your cybersecurity strategy?

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats. Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,500 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations. Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.