Why data diodes are becoming a billion-dollar market

Kirill Zhuklinets, Connecting Software

Kirill Zhuklinets is CTO of Connecting Software

The technology is becoming an indispensable part of high-security networks globally

June 11, 2025 Have your say

Data diodes are a humble-looking piece of tech, but they are much more important than their appearance might convey. Slowly but surely, they're becoming an indispensable part of high-security networks globally. The market is already worth $500 million and is predicted to double that in ten years.

Data diodes are designed to offer an important upside to high-security networks – such as those used in government, banks, and other businesses. Typically, when a server network was too critical to be exposed to the potential risk of hackers accessing it from the Internet, organizations would airgap it, physically cutting it off from the rest of their internal network. This presents a logistical challenge, however, given that even simple changes to the internal network could only be made frustratingly slowly – sometimes troubleshooting would need to be done by writing down proposed changes and physically relaying them into the server space.

Manually transferring data between segmented networks using USB drives or other physical methods, beyond being inconvenient and time-consuming, also introduces serious security risks and potential compliance violations if sensitive information is misplaced or lost.

Data diodes bridge this gap by providing a way that information can be quickly and efficiently transferred in while stopping bidirectional direct communication. They are designed to enforce strict one-way data flow between networks from a high-security network to a low-security one, or vice versa. Unlike traditional firewalls or software-based solutions, a data diode physically prevents data from traveling in the opposite direction, providing the same security in that direction as the air gap.

Solutions like these stop unauthorized data exfiltration (the theft or leaking of sensitive information) because bidirectional direct communication is impossible – meaning that while authorized employees can exchange data, attackers can't send commands to steal it.

Data diodes are also known for preventing lateral movement, as attackers can't move within the network, traveling from one system, server, or segment to another, usually to locate sensitive data or escalate privileges after gaining an initial foothold. If an attacker were to gain a foothold in a less secure network connected to a high-security network via a data diode, they would be physically unable to send commands or malicious traffic back through the diode to compromise systems within the high-security zone.

Alternatively, some organizations will purchase SaaS that allows them to set up data diodes going *both ways* – both to and from the network. This allows them to strictly limit the information that can be transmitted or the programs that can communicate with the network. While less secure than a one-way diode, this allows them to maintain synchronization while effectively reducing their 'surface of attack' to bad actors.

Those providing such critical infrastructure and the public sector as a whole face increasing tension: balancing their security with the benefits that a more interconnected and Internet-integrated business can have.

Why have data diodes become so critical?

It's somewhat fair to say that data diodes serve a rather niche use case. After all, not every business has a high security network they need to protect – but for those that do, they are increasingly becoming a 'no-brainer' security investment.

When we work with government agencies, we hear that cybersecurity threats facing critical government, business, and financial networks are escalating annually as cybercriminals get access to new AI powered tools.

The FBI's recently released Internet Crime Report revealed that 2024 saw a new record for reported losses of $16.6 billion. The FBI separately highlighted that "critical manufacturing, healthcare, government facilities, financial services, and information technology were the top critical infrastructure sectors targeted."

Those providing such critical infrastructure and the public sector as a whole face increasing tension: balancing their security with the benefits that a more interconnected and Internet-integrated business can have. For many organizations, having vital information stored in a place that is, by design, so inflexible and disconnected represents an undesirable bottleneck.

Data diodes represent a shift in how these secure networks can be protected. Secure organizations now see data diodes and how they physically enforce a one-way data flow as a way to leverage the benefits of being connected to the rest of their business. In effect, they can represent a ‘best of both worlds’ solution - allowing faster communication to cloud resources without compromising the integrity and confidentiality of critical data and systems.

The demands of data diodes

Despite their benefits, businesses adopting data diodes do face some challenges in adoption. Firstly, designing and maintaining strict rules about what data can be sent out requires careful effort and expertise. Depending on the compliance and security requirements, complex reporting, documentation, and approval processes might also be required for using data diodes – above and beyond what might be expected in a traditionally air-gapped system.

Secondly, data diodes often have issues with software compatibility, which can require skill and manpower in setting up. While data diodes are much better at facilitating data flows than an air-gapped solution, companies can find challenges in setting up automatic exchanges of information via a data diode because of the difficulty in finding adequate software, which is most often set up for bi-directional networks.

In a practical sense, this can present roadblocks if, say, an organization wished to synchronize calendars between those working in the high security environment and those not. In-house development of programs to facilitate this transfer is often time-consuming and expensive, although some SaaS does exist to solve this problem.

The growth of data diodes as a market indicates the caution of an expanding number of businesses over their data. As more information moves online, more public and private sector organizations will have something to protect – and the demand for devices like these is a key indicator of that growth. So long as hackers are trying to access this vital information, data diodes and the software that supports them will continue to be indispensable.

Tags

Connecting Software

Kirill Zhuklinets