CELERIUM UPDATE BRIEF

ASSETS MSPS MUST PROTECT INSIDE THEIR OWN CYBER HOUSE

CELERIUM.com

CURRENT STATE OF CYBERATTACKS ON MSPS

Your customers rely on you to keep them up and running and secure. You research, install and manage the very best cybersecurity solutions for your customers' enterprises to keep their assets safe from attackers.

But a growing number of cyber criminals are exploiting new attack vectors. **These cyber bandits are exploiting the IT assets of support companies – like yours – as a possible gateway into your customers' assets.**

As published by BlackFog, a global cybersecurity company, targeted cyberattacks on MSPs are on the rise and occur on a regular basis. In their research report, they describe the top five cyberattacks between 2023 and 2024.

Source: BlackFog

1.	Nov. 2023	CTS Cyberattack
2.	Jan. 2024	Tietoevry Ransomware Attack
3.	March 2023	Lumen Technologies Cyberattacks
4.	Dec. 2023	HTC Global Services Data Breach
5.	Oct. 2023	Sudwestfalen IT Ransomware Attack

The attackers are discovering that many of the companies they want to break into are well-protected. **So, these bad guys look to the support companies – like managed service providers (MSPs) --as a way into those well-protected enterprises.**

If a cyber thief wants to steal the personal identifiable information in your client's database, why not hack the MSP who has credentials to access that data.

ARE YOU DEPLOYING THE BEST CYBERSECURITY SOLUTIONS TO PROTECT YOUR OWN IT INFRASTRUCTURE?

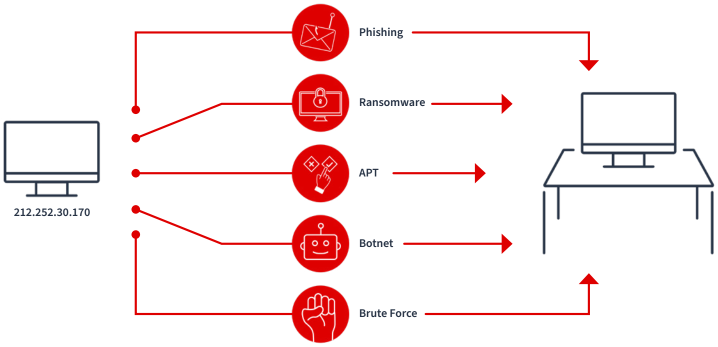
HOW MSPS SHOULD PROTECT THEMSELVES

First Line of Defense:
Automated Network Threat Detection and Blocking

Your firewall must be your first line of protection. But a lot of your IT assets are moving to the cloud. On top of that, modern cyber threats are evolving. So you need more than just your firewall to block and stop cyber threats.

You need automatic threat detection and blocking to help you secure your and your customer's business. **Celerium's Network Defender® is a viable way to identify the threats coming into your and your customer's network and automatically block them to stop bad actors from gaining access.**

Network Defender grabs threat intelligence from across the Internet, including intelligence from high-end threat feeds. It then correlates, compares and scores all that intelligence, enabling you to determine if a threat is a false positive or something you need to act upon. **It's 24/7 consistent defense.**



When Network Defender is configured correctly, it makes sure any connection from a malicious entity will be automatically locked and logged, and you will be notified. You can go into Network Defender and read the report, and with this quality information, you can optimize the setup of your devices going forward.

Given you have access to critical information in your clients' databases, **deploy Network Defender to detect and block anyone trying to access your network to get to your clients' assets.**

Protect your customers from cyber threats with Network Defender.

Automated network threat detection and blocking solution built for MSPs and MSSPs.

REQUEST A DEMO →

OTHER CRITICAL LINES OF DEFENSE

Your MSP portfolio may include clients from different industries. **Some of those industries have specific compliance requirements, for example, the medical, legal and financial industries.**

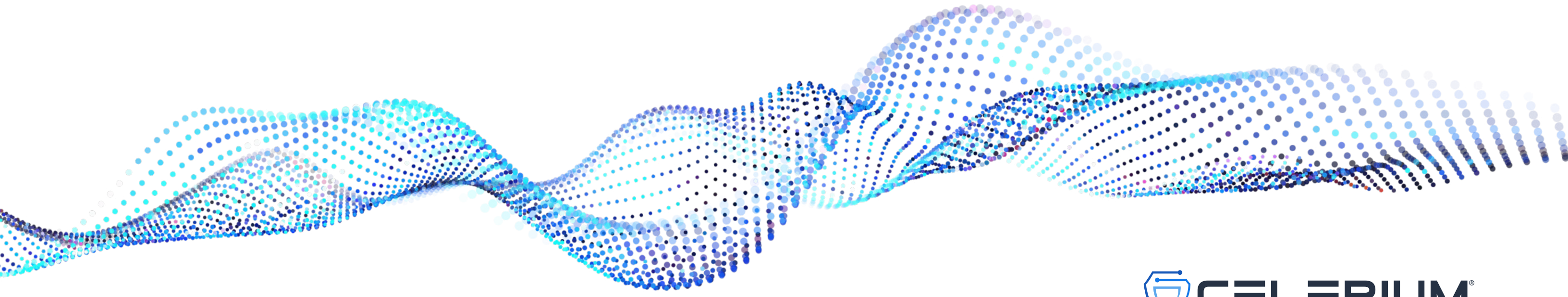
You probably helped your clients deploy the technology solutions that enable them to meet those compliance requirements. **Now, it's time for your organization to deploy the technology solutions needed to support those compliance requirements.**

For your clients who must comply with the Health Insurance Portability and Accountability Act (HIPAA), **your MSP organization must be HIPAA compliant as well.**

The same pertains to your clients' businesses that must comply with **PCI DSS (Payment Card Industry Data Security Standard).**

And, of course, your MSP business must be equipped to protect **PII (personally identifiable information).**

Network Defender provides a front-line defense for your personally identifiable information by automatically blocking malicious connections in and out of your network. **It contributes to your HIPAA and PCI security posture** by notifying you when those connections are attempted.



OTHER POSSIBLE ATTACK VECTORS

You should also look at other vectors that could circumvent your firewall – like **emails with malicious packages, phishing attempts, and mobile-device management and virtual private networks (VPNs).**

Be sure to tackle phishing attempts via robust training for your staff as well as audit-detection methods.

Network Defender also assists with your auditing capabilities by notifying when attempts are made to contact outside malicious entities, revealing and blocking those attempts that may have circumvented your existing infrastructure to infect your network.

Critically important is your implementation of a proper zero trust environment. The only people who need access to certain information should be given access to it. Period. Limiting access to information helps keep that data out of the reach of cyber thieves.

And, of course, there is **device management.** You must be able to secure devices that are owned and operated by your company. Once a device is infected and inside your network, your firewall won't work.

If infected devices enter your network, Network Defender notifies you and blocks those outgoing connections. You know more about what's attacking your network while being protected from further outside infection.

FOR HELP PROTECTING YOUR & YOUR CUSTOMERS' ASSETS, GO TO CELERIUM.COM.

ABOUT CELERIUM

Celerium® powers active cyber defense solutions to help protect organizations and communities from increasing cyberattacks. With a rich 16-year history of facilitating cyber threat sharing for critical industry sectors and government agencies, Celerium is an established leader in providing innovative cybersecurity solutions, with solution directions based on the evolving needs of the industry.

Learn more at www.Celerium.com and follow us on X at @CeleriumDefense

CELERIUM.com