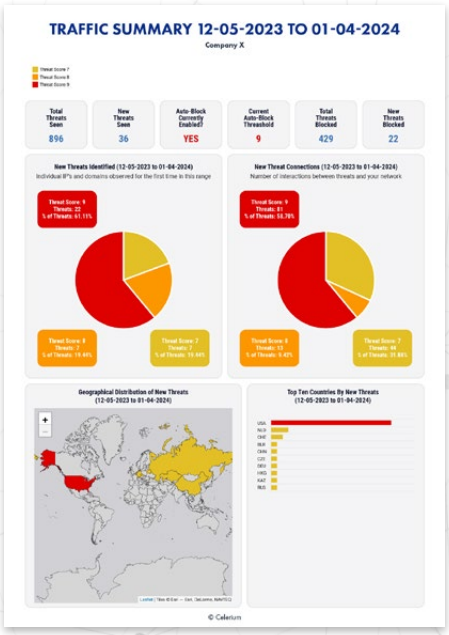
HOW TO SELL CDN NETWORK DEFENDER TO YOUR SMALL BUSINESS CLIENTS

Our partners and potential partners often ask us about the best way to sell CDN Network Defender to their small business clients, and our answer, like our solution, is straightforward: the best way to sell CDN Network Defender to small businesses is to show the small business what threats will be successfully connecting to their networks in the absence of CDN Network Defender.

So, with that in mind, here is how we recommend our MSP partners sell CDN Network Defender, step-by-step.

STEP 1

Contact your CDN Network Defender Customer Success representative, and give them the name or names of the accounts for which you'd like to deploy a prospecting sensor, or a free, 30-day sensor to an end-user you'd like to sell CDN Network Defender to. You can request as many prospecting sensors as you like.



STEP 2

Deploy the CDN Network Defender prospect sensor. CDN Network Defender's sales engineering team can assist if requested through your Customer Success representative.

STEP 3

Wait until the end of the month while the CDN Network Defender sensor collects data on the prospect's firewall.

STEP 4

When the prospect's monthly report is delivered early the next month, meet with the prospect and show them what threats were seen on their network that could have been blocked by CDN Network Defender's platform.

It is possible that no new threats will be seen by CDN Network Defender at the prospect's firewall, but it's unlikely. In April, for example, only 4% of all CDN Network Defender sensors deployed detected no new threats at their respective firewalls, so there's a 96% chance there will be compelling data to show your prospect.

What is CDN Network Defender Blocking?

When you present the CDN Network Defender report to your clients, they are likely to ask what kinds of threats constitute a 9 or an 8. To answer that question, we recommend leveraging some examples below of actual level 9 and 8 threats our platform has detected and blocked on the networks of our MSP Partners' clients:

- An Iranian Telecom company identified for exploiting SQL server vulnerabilities attacking a K-12 school district in the Southeast US
- A Chinese device associated with brute force attacks (automated attempts to identify weak passwords) also attacking the K-12 school district's offices
- A German IP launching a Telnet open port scan and potential SNMP (Simple Network Management Protocol) attack was stopped attempting to connect to an animal hospital in the US
- A Chinese host scanning for, and then potentially attacking, a web application vulnerability in the ThinkPHP attacking the offices of a specialty pharmacy chain
- A known phishing site in Germany connecting to the network of a State Regulatory Agency office in the southern US
- A host - located in the US - associated with brute force SSH attacks (the objective of which is to use the SSH protocol to execute commands on a remote computer) was blocked by CDN Network Defender on the network of the offices of a small municipality in the southwest US
- Servers running Shodan scanning software that catalogs internet-facing devices and software. Shodan data is used primarily by pen testers and hackers to more efficiently identify their targets.
- Command and control servers for the Mirai botnet, malware that hijacks target devices and uses them in DDoS attacks
- A command and control