CyberCNS

Sales Playbook

- OVERVIEW
- PITCH
- FEATURES
- PROBLEMS SOLVED
- TARGET CLIENTELE
- ENVIRONMENTS
- QUALIFYING QUESTIONS
- SALES SCENARIOS
- OVERCOMING OBJECTIONS
- COMPETITORS
- PSA INTEGRATIONS

CyberCNS

SECURITY

OVERVIEW

Developed BDRs in the MSP space (Zenith, Replibit) and have built several ConnectWise software solutions (Campaign Director, Chat, Cloud Console). Sold one software business to ConnectWise in 2019.

HQ – Vancouver, BC

Development in Bangalore, India

Founded in December 2018

50+ Employees

200 Partners (MSP/MSSPs)

Business Model: Channel only

Focus: Vulnerability/security assessments, vulnerability management (continuous monitoring)

Our solution fits in the "Identify" Function of NIST Cybersecurity Framework (CSF) and Controls 1, 2 & 7) for Center for Internet Security (CIS Controls version 8.0).

pax8

SECURITY

PRODUCT PITCH

Today's threat landscape requires continuous monitoring of vulnerabilities, new devices found on the network, and AD monitoring.

CyberCNS is meeting these needs by providing continuous monitoring, integration to PSAs and reporting to meet compliance and cyber insurance requirements.

CyberCNS

SECURITY

FEATURES

- Asset Discovery and Tracking Partial
- Subnet Scan
- Active Directory Discovery and Tracking
- Office 365 Assets Discovery and Tracking
- Windows Vulnerabilities
- Linux (Ubuntu/Redhat/CentOS/ AmazonLinux)
- Mac OS
- Active Directory Users and Groups Compliance
- SMB/CIFS Shares
- Software Inventory

All

pax8

CyberCNS

SECURITY

PROBLEMS SOLVED

Problem 1 – Managing vulnerabilities for all customers in one platform.

Solution 1 – CyberCNS handles both Network and WFH for all your clients with probes and lightweight agents (easily deployed through your RMM).

Problem 2– Active Directory security anomalies & proper AD risk management.

Solution 2– CyberCNS manages changes in AD and notifies you through tickets, messaging applications or other easy-to-setup alerts.

Problem 3– RMM functionality issues. RMMs are not full proof and may not be effectively patching.

Solution 3– CyberCNS provides a "trust but verify" approach to ensure patches are being properly applied.

SECURITY

TARGET CLIENTELE

- Financial - banks, credit unions, hedge funds, Registered Investment Advisors.
- Healthcare
- Defense Industrial Base (800-171 & CMMC)
- Biomedical, medical equipment
- Insurance

CyberCNS

SECURITY

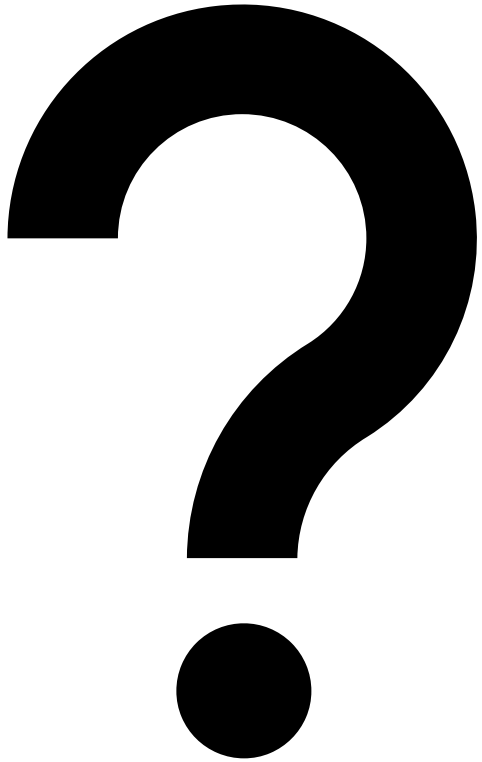
SUPPORTED ENVIRONMENTS

- In terms of the application, CyberCNS can run either in the Cloud or on-premises.
- In terms of asset discovery: Windows, Mac, Linux
  - **Cloud**
    - AWS Lightsail – each instance is dedicated, in region and meets GDPR Compliance
  - **On-premises** deployment options
    - VMWare
    - HyperV
    - MSP's Azure Instance
    - MSP's AWS Instance

CyberCNS

SECURITY

QUALIFYING QUESTIONS (1of 2, **scroll down** for more content)



Do you use any solution today to do one-time or continuous scans?

Can you share a little bit about how your MSP handles vulnerability management? Is it ad-hoc or part of your stack?

Does your MSP have your own internal security program, and does it align to a specific framework like Center for Internet Security (CIS) or NIST CSF?

SECURITY

DEEPER QUALIFYING QUESTIONS (2 of 2)

- How do you currently manage vulnerabilities that are not handled by your RMM?
- Who is responsible for managing risks not addressed by your current stack? Do your clients know you're not managing vulnerabilities outside of OS and 3rd party applications?
- Do you know your client's renewal schedules for their cyber insurance? Vulnerability management, along with MFA everywhere and EDR are just a few of the controls that most carriers are going to make mandatory.

CyberCNS

SECURITY

SALE SCENARIOS

Scenario
We are using RFT and are not happy.
Opening
What are the challenges you're facing?
Value Prop
Not only will you be able handle presales or risk assessments, but with CyberCNS you can continuously manage vulnerabilities, rouge devices, and AD anomalies.

Scenario
Customer is using Nessus.
Opening
How many clients are you managing? They have a min of 65 devices at $35 per device per year.
Value Prop
With CyberCNS, you can manage all clients for a fraction of the cost; CyberCNS is multitenant and integrates with your PSA.

CyberCNS

SECURITY

OVERCOMING OBJECTIONS

Objection
We use Rapidfire Tools (RFT) & we are locked into a contract.
Response
Are you using RFT for sales assessments or vulnerability management?

(A)Typically, it's sales assessments.

How do you handle vulnerabilities outside of Patch Management.? Do you have any concerns about the risks that face your customers around non-patched devices?

Objection
We don't have time to focus on this right now.
Response
What would it mean to your MSP if your top MRR customer was compromised through a known IOT or infrastructure vulnerability? What would it mean if a WFH device was compromised because your RMM agent was ineffectively patching?

pax8

CyberCNS

SECURITY

COMPETITORS

Qualys

RFT RapidFireTools A Kaseya COMPANY

Nessus®

tenable™

pax8

SECURITY

PSA INTEGRATIONS

PSA Integration	Y/N	Current Functionality
ConnectWise	Y	
Autotask	Y	
Tigerpaw	N	
Kaseya	Y	
Syncro	Y	

pax8