



IT NATION™

SECURE

hosted by  CONNECTWISE

Stack Them Up to Knock Them Down

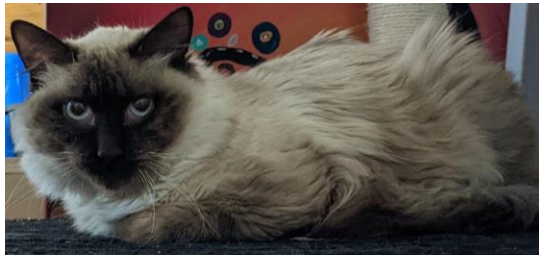


IT NATION™ **SECURE**

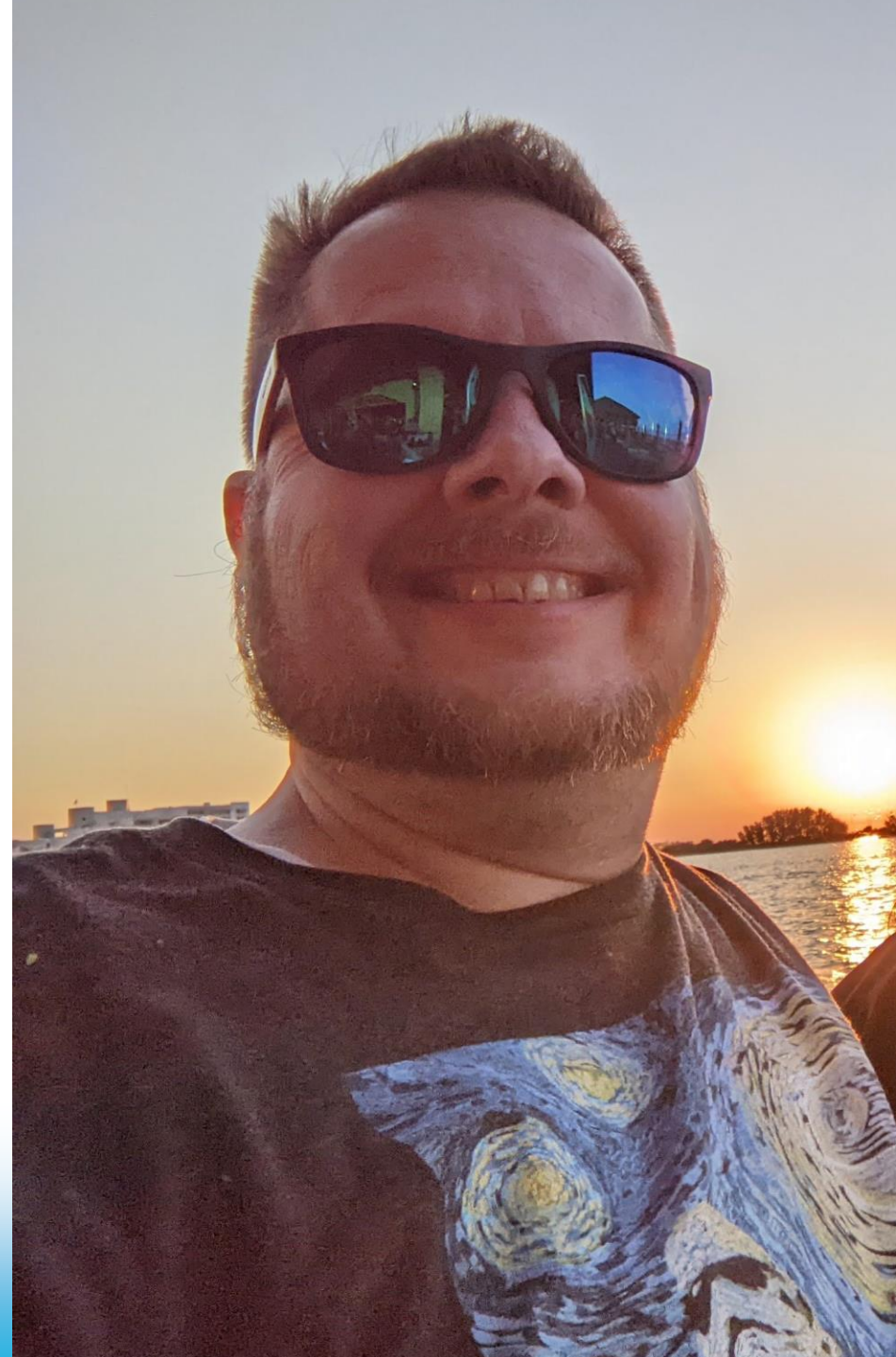
# Rob DeBok (DeeeeeBok)

## Software Training Consultant

- 9 years with ConnectWise
- Love cats
- Upcycle/repurpose
- Love helping partners



#





# MSPs Traditionally Offer ...

- Essential Protection
  - GPO Management
  - Antivirus
  - Patch Management
  - Web Content Filtering (Firewall)
  - Managed Firewall
  - IDS/IPS
  - Encryption
  - Backups





# Security-First MSPs Offer ...

- Emerging Protection Norms for SMBs
  - Security Awareness Training
  - Security Policies
  - Identity Access Management (IAM)
  - Secure Access Service Edge (SASE)
  - DNS Security
  - EDR/MDR
  - MFA/SSO
  - Dark Web Monitoring
  - SIEM
  - Continuous Risk Reporting



# ConnectWise Cybersecurity Ecosystem

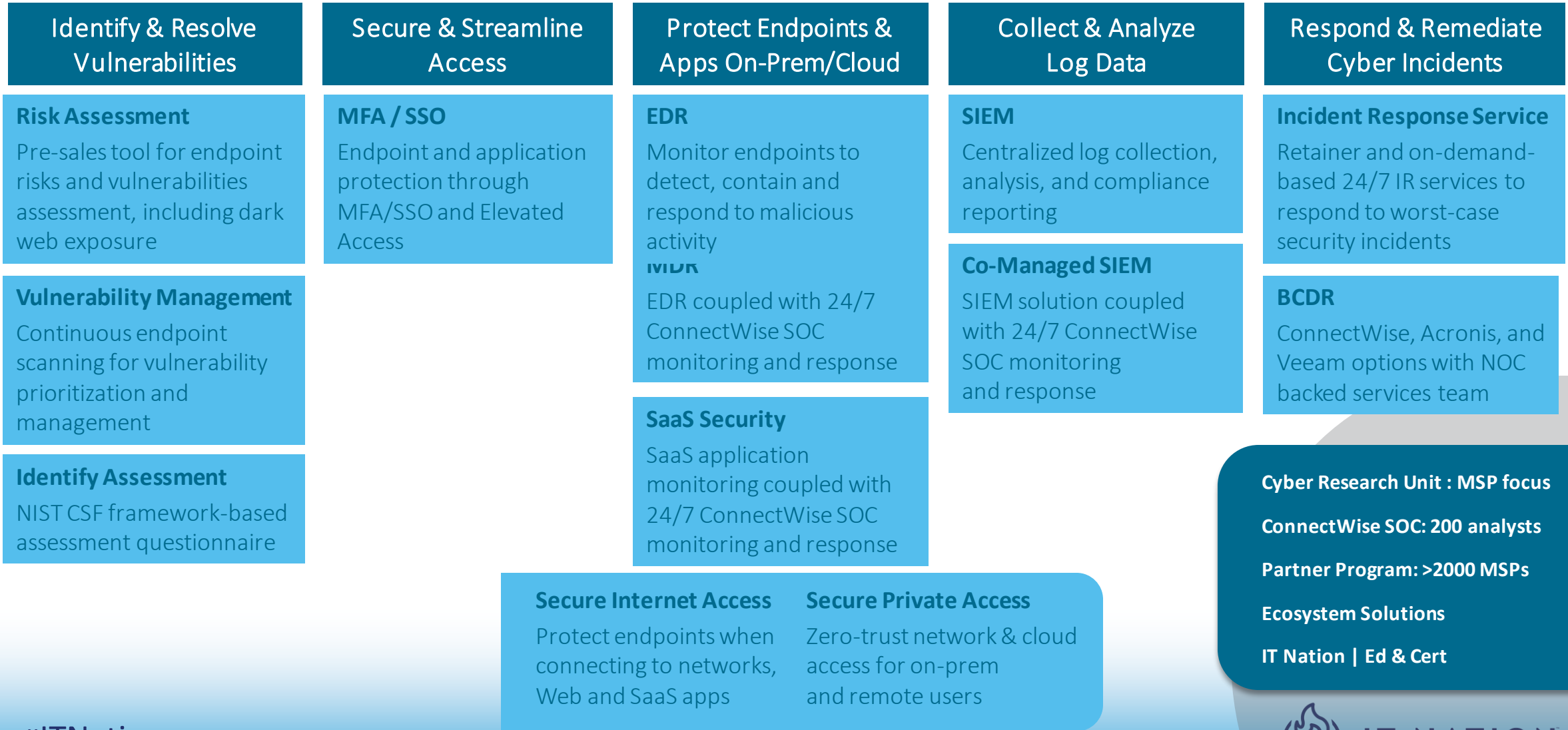
Diverse and Cohesive Stack



IT NATION™ **SECURE**

# ConnectWise Cybersecurity Management

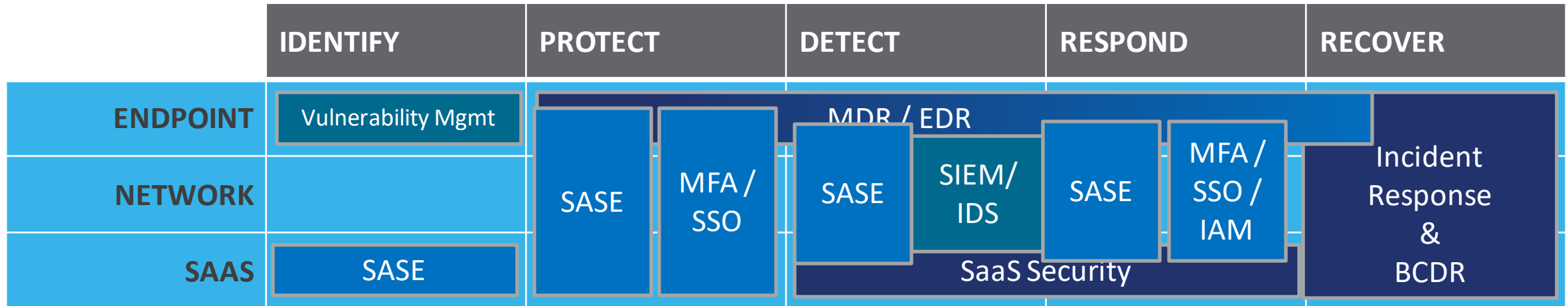
Everything you need to build, launch, and grow a successful cyber practice






**Cyber Research Unit : MSP focus**  
**ConnectWise SOC: 200 analysts**  
**Partner Program: >2000 MSPs**  
**Ecosystem Solutions**  
**IT Nation | Ed & Cert**



# ConnectWise Cybersecurity Ecosystem



-  ConnectWise Products
-  ConnectWise Expert Services
-  Third-Party, Strategic Resold Products





# ConnectWise Cybersecurity Ecosystem

Education



IT NATION™ **SECURE**

# ConnectWise Certify



I need help with

welcome back ROBERT

Sign Out  
Admin On / Off

Support ▾ Education ▾ Documentation ▾ Consulting ▾ Community ▾ System

- Degrees
- My Transcript
- MSP University
- Business Innovation Center
- University Calendar
- Certification Programs
  - ConnectWise Certify
  - ConnectWise Launch
- Webinar Series
- Paths to Product Proficiency
- Customer Journey

ow av and badges that validate your credentials and

TM

ers a variety of role-based train

<https://univ>

#ITNation

e-certify

IT NATION

# Cybersecurity Fundamentals

Three courses:

- Cybersecurity Fundamentals
- Cybersecurity Fundamentals for Sales and Owners
- Cybersecurity Fundamentals for Engineers

Content:

- 8+ hours
- Product agnostic
- MSP focused
- Risk-driven approach
- 30 question exam







# ConnectWise Cybersecurity Ecosystem

Identify & Resolve Vulnerabilities



IT NATION™ **SECURE**

# Identify

> Dunder Mifflin > NIST CSF Assessment 7/22/19, 10:09 AM

OVERALL RISK **MEDIUM**

IDENTIFY HIGH

PROTECT HIGH

DETECT MEDIUM

RESPOND LOW

RECOVER MEDIUM



- Low-cost, high margin practice you can apply to *all* customers AND offer to prospects
- Executed by sales
- Asking the questions and running a report takes about 40 minutes

# Identify

# Build a Road Map



## OVERALL RISK ASSESSMENT

Your overall risk rating is **LOW**

Congratulations! Your overall risk determined from the assessment conveys a diligence on your part to ensure you are doing what is needed to maintain the security of your organization.



## TOP RISK AREAS

- Critical** PR.AT-1 - All users are informed and trained
- High** ID.RA-1 - Asset vulnerabilities are identified and documented
- Medium** PR.AC-2 - Physical access to assets is managed and protected
- Medium** PR.PT-3 - The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
- Low** RC.RP-1 - Recovery plan is executed during or after an event



## TOP RISK AREA RECOMMENDATIONS

### PR.AT-1: All users are informed and trained

**Critical**

Q: Do you require Information Security training for your employees?

A: No

**Importance:**

*It is essential to your business to ensure your employees are trained on the constantly changing security threats and how to avoid these threats.*

**Remediation Steps:**

*There are several on-line security awareness training companies. Make it a priority to sign your employees up for annual security awareness training.*

### ID.RA-1: Asset vulnerabilities are identified and documented

**High**

Q: Does your organization have an internal process for assessing risk?

A: I'm not sure

**Importance:**

*You should know whether your firm performs periodic risk assessments so you can have knowledge of and plan for the remediation of those risks.*

**Remediation Steps:**

*Work with your company leaders to determine if you have performed a risk assessment and if not then you should create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.*

### PR.AC-2: Physical access to assets is managed and protected

**Medium**

Q: Do any of your users have admin access?

A: Yes



# Identify

## TOP RISK AREA RECOMMENDATIONS

---

**PR.AT-1: All users are informed and trained**

**Critical**

Q: Do you require Information Security training for your employees?

**A: No**

***Importance:***

*It is essential to your business to ensure your employees are trained on the constantly changing security threats and how to avoid these threats.*

***Remediation Steps:***

*There are several on-line security awareness training companies and sign your employees up for annual security awareness training.*

**ID.RA-3: Threats, both internal and external, are identified and documented**

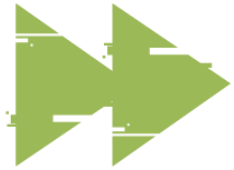
**Critical**

# Assessment Process

- Prepare
- Onboard
- Configure
- Conduct assessment
- Analyze
- Report and recommend
- Review and present
- Follow-up and support

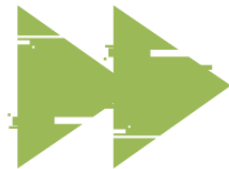


# Risk Assessment



## Scan and Report

Uncover unknown vulnerabilities and security gaps



## Prioritize and Remediate

Plan and initiate corrective measures

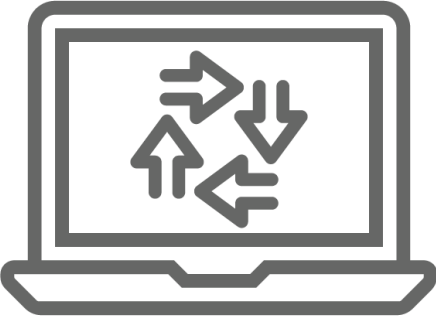


## Deepen Client Cyber Understanding

Improve security outcomes



# Risk Assessment



Generate and send to client / prospect a unique assessment download link



Prospective end users download and execute the ConnectWise utility tool—you monitor status



Download and share detailed findings and initiate POAM

**Super  
Simple &  
Efficient**

**Assessment Configurations**

Client Name \*  
Henry Charles

Recipient Email ⓘ  
henrycharles@cw.com

Domain Name \* ⓘ  
e.g. 'mydomain.com'

The domain(s) you enter must be owned by the site. Separate multiple domains with a comma (mydomain1.com, mydomain2.com, etc.).

Generate URL Send Email

Reactivate link Send Email

<https://connectwise.com/downloadassessment/georgemartin/TKNa4ee5ca1-cfbb-475d-899a-04f6c0eb2cb5>

This link is valid until Feb 23, 2022, 07:05:20 PM. Click Send Email to share the URL. COPY LINK

# Risk Assessment

## Comprehensive Assessment Utility

Create Assessment

Client Name	Creation Time	
6May2022-3	May 19, 2022, 08:38 AM	
Sanity -001 _ without Email	May 18, 2022, 09:50 AM	
Sanity -001 _ without Emails	May 18, 2022, 09:44 AM	
Test client 1	May 18, 2022, 09:43 AM	
11May2022-03	May 18, 2022, 09:42 AM	
sanity - 001_Master	May 18, 2022, 09:38 AM	
17May2022-2	May 17, 2022, 02:09 AM	
17May2022-1	May 17, 2022, 02:07 AM	
DCTesting-2	May 16, 2022, 06:01 AM	
16May2022-1	May 16, 2022, 05:53 AM	
passwordValidation	May 13, 2022, 05:06 AM	
Rahul-12	May 13, 2022, 05:02 AM	
Nishant-OS	May 13, 2022, 05:01 AM	
https://jira.connectwisdev.com/bro...	May 13, 2022, 04:50 AM	Not Started

Assessment Configurations
×

**Client Name \***

8Bytes Computing

**Recipient Email** ⓘ

RobertG@8bytesComputing.com, SarahT@8bytesComputing.com, PeterM@8bytesComputing.com

**Domain Name \*** ⓘ

8bytesComputing.com

The domain(s) you enter must be owned by the site. Separate multiple domains with a comma (mydomain1.com, mydomain2.com, etc).

Reactivate Link

Send Email

https://qa.setup.itsupport247.net/downloadassessment/8Bytes Computing/TKN04cfb79c-6196-4842-a2cc-4771c502e0c2

This link is valid until May 23, 2022, 12:49:27 PM.  
Click Send Email to share the link.

📄

Cancel

Finish

Scanned Devices	Actions
-	
1	↓
-	
-	
-	
1	↓
-	
-	
-	
-	
-	
-	
-	
-	
-	
-	
-	
-	
-	

# Risk Assessment: Dark Web Monitoring

## Dark Web Assessment

The dark web is a massive and widely used marketplace by cyber criminals. Malicious actors use stolen email credentials to impersonate the owner to commit theft or other fraud. The stolen records including identity and credit card information are often sold on the dark web.

**Risk Detected!**



14 EMAIL ID(S) EXPOSED



MULTIPLE EXPOSURES DETECTED



HIGH RISK SCORE

### Top 3 Exposures

Top Email Exposures	Exposure Count	Latest Exposure Date	Severity	Confidence	Risk Score
RonaldY@youngandyoungin.com	5	May 30, 2022	High	-	HIGH
McKen@youngandyoungin.com	1	June 01, 2022	Critical	-	HIGH
PorterM@youngandyoungin.com	3	May 30, 2022	High	Low	HIGH

\*Please refer to the detailed report to view all the records.

## How to stay Protected



Keep your identity safe by keeping complex passwords.



Knowing in real-time which passwords and accounts have been posted on the Dark Web allows you to be proactive in preventing a data breach.



We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

ENTER DOMAIN NAME:

continuum.net

If you enter a domain for e.g. 'mydomain.com', all associated email addresses will be checked. Domains entered must be the ones that the site owns. Avoid entering protocols and subdomains such as 'http://', 'https://', 'www'.

ENTER EMAIL ID:

jake@example.org, admin@example.org, kay@example.org

You may enter individual email addresses associated with a public email provider, for e.g. yahoo.com. gmail.com.

- Generate an alert when new data for a user of end customer appear on the dark web  
To enable Dark Web Monitoring click check box and then Finish. Configuration will be complete and live within 24 hours.

# Vulnerability Management

Dashboard / Vulnerability Mgmt

## Vulnerability Management

Run / Schedule



### Top Vulnerable Sites



**Creating New Feature**  
We are currently working on creating something fantastic which will be coming soon.

### Inactive Sites

26

Total 3

Search



<input type="checkbox"/>	Site Name ^	Severity	Scanned	Unscanned	Failed	Total
<input type="checkbox"/>	AniketTest	Not Available	0	0	0	0
<input type="checkbox"/>	P2Site01	<span>1</span> <span>25</span> <span>683</span> <span>245</span> <span>9</span>	4	0	1	5
<input type="checkbox"/>	P2Site02	<span>692</span> <span>986</span> <span>237</span>	1	0	3	4

Rows per page

100

1 - 3 of 3



# Vulnerability Management




→ Vulnerability Mgmt / Device Scan

## Device Scan

[Run / Schedule](#)

### Devices



Total	5
Scanned	5
Unscanned	0
Failed	0

### Unique Vulnerability Count

21	54	2310	1689	259
Unknown	Critical	High	Medium	Low

Total 5

<input type="checkbox"/>	Name	Friendly Name	Site Name ^	OS	Severity	Last Successful Scan	Last Scan Status
<input type="checkbox"/>	DESK-001	DESK-001	Autobros	Windows 10 P...	19 Critical 23 High 518 Medium 162 Low 4 Unknown	03/02/2023, 8:30 AM EDT	Scanned
<input type="checkbox"/>	Joom	Joom	Autobros	Windows Serv...	4 Critical 43 High 25 Medium 1 Low	03/02/2023, 8:32 AM EDT	Scanned
<input type="checkbox"/>	CW-ED...	CW-EDU...	Autobros	Windows Serv...	17 Critical 41 High 1471 Medium 647 Low 18 Unknown	03/02/2023, 8:44 AM EDT	Scanned
<input type="checkbox"/>	SENSO...	SENSOR...	Autobros	Windows Serv...	4 Critical 38 High 27 Medium 2 Low	03/02/2023, 8:35 AM EDT	Scanned



# Vulnerability Management



Device Scan / Vulnerabilities

## Vulnerabilities



### Vulnerabilities



**No Available Data**  
Error while fetching data please try again

### Top 5 Vulnerabilities

CVE-2020-17095	<div style="width: 100%;"></div>	2
CVE-2021-28476	<div style="width: 100%;"></div>	2
CVE-2016-0799	<div style="width: 100%;"></div>	2
CVE-2016-2177	<div style="width: 100%;"></div>	2
CVE-2016-2182	<div style="width: 100%;"></div>	2

Total 72

Search



Severity and CVSS	Device Name	Site Name	Company	Vulnerability Description	CVE ID	Last Detected
<b>10 CRITICAL</b>	CW-EDU-H...	Autobros	Autobros	A remote code execution vulner...	CVE-2020-1350	03/02/2023, 8:44 AM EDT
<b>10 CRITICAL</b>	CW-EDU-H...	Autobros	Autobros	An elevation of privilege vulnera...	CVE-2020-1472	03/02/2023, 8:44 AM EDT
<b>9.9 CRITICAL</b>	CW-EDU-H...	Autobros	Autobros	A security feature bypass vulner...	CVE-2019-1384	03/02/2023, 8:44 AM EDT
<b>9.9 CRITICAL</b>	CW-EDU-H...	Autobros	Autobros	An elevation of privilege vulnera...	CVE-2019-1365	03/02/2023, 8:44 AM EDT
						03/02/2023, 8:30 AM

# Vulnerability Management

## Run Vulnerability Scan ✕

Run Now

Schedule

**Schedule**

Start \*   Trigger

Recurrence \*

Start \*

Repeat \* Every\*

End \*



# ConnectWise Cybersecurity Ecosystem

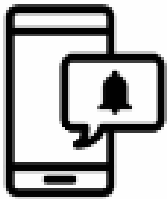
Secure and Streamline Access



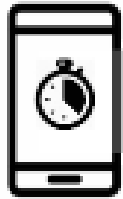
IT NATION™ **SECURE**

# Identity and Access Management (IAM)

Authentication Options:



Push



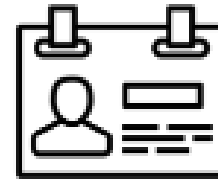
Soft Key



Yubikey



Hard Key

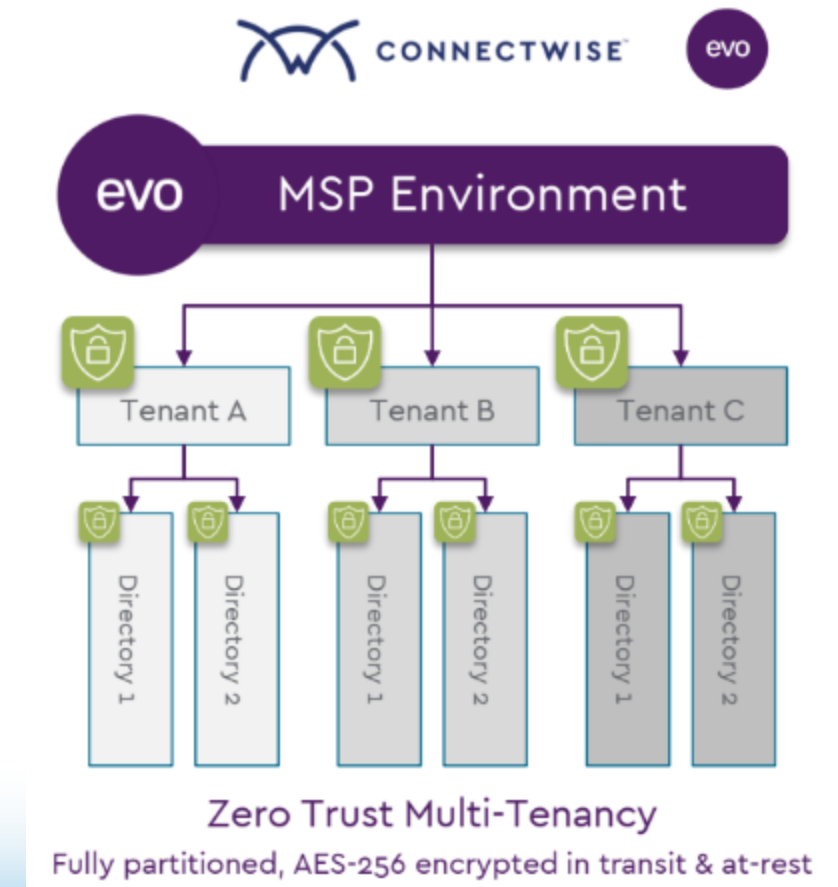


Smartcard

- Multi-Factor Authentication (MFA)
- Single Sign-On (SSO)
- Elevated Access
- Unified Directory Services

**Also included:** Multi-Tenant Management, Role-Based Access Controls, Policies, User and Device Visibility and Management, Automated Customer Onboarding Campaigns, Self-Enrollment, End User Password Resets

#ITNation



# ConnectWise Cybersecurity Ecosystem

Protect Endpoints & Apps On-Prem/Cloud



IT NATION™ **SECURE**



# Managed Detection and Response (MDR)

BEFORE



DURING



AFTER



# Managed Detection and Response (MDR)

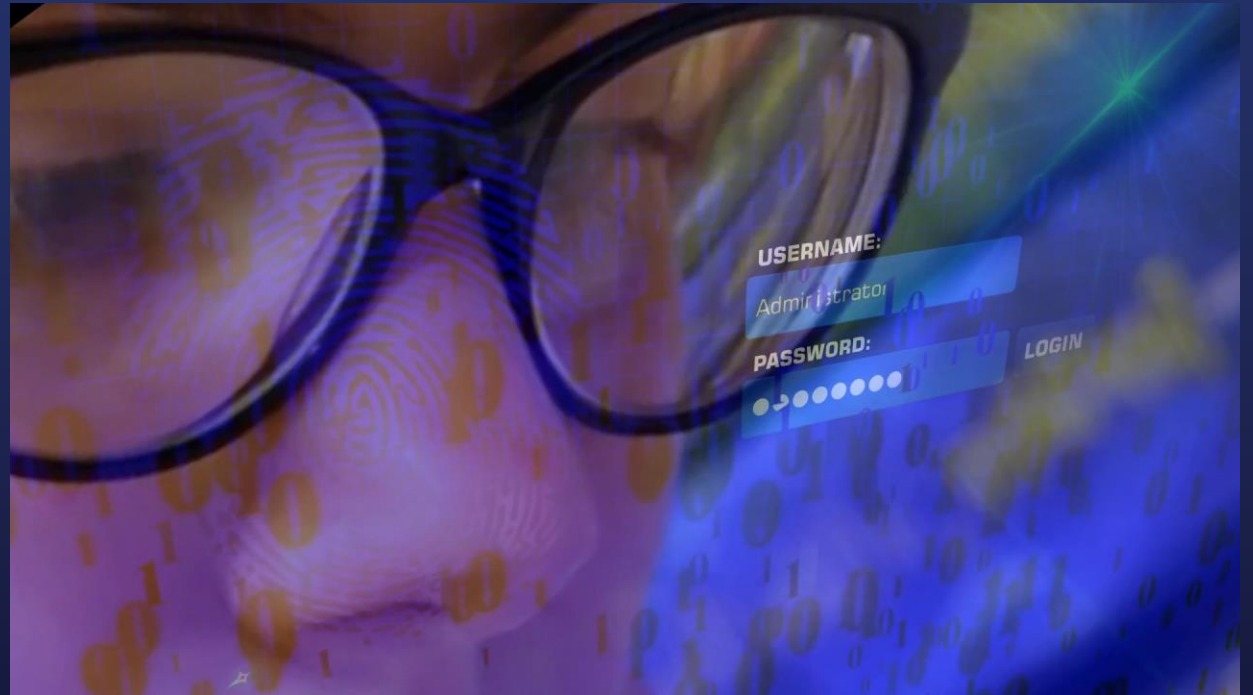
 SentinelOne®

OR

Bitdefender®



ConnectWise SOC  
Services™



# Managed Detection and Response (MDR)

- Accelerate your practice
- Avoid expensive upfront costs
- 24/7/365 Monitoring and Response





SENTINELS ENDPOINTS TAGS POLICY BLACKLIST EXCLUSIONS NETWORK CONTROL DEVICE CONTROL PACKAGES UPGRADE POLICY SITE INFO GROUP RANKING

Firewall Network Quarantine

Select filters...

New rule Actions Reorder rules No Items Selected

1 Rules 50 Results Columns

Firewall Control is on

Name	Tags	Status	Scope	Description	OS	Application	Direction	Protocol	Local Host	Local Port	Remote Hosts	Rem
LP Test		Enabled	Account		Windows	Path	Any	Any	Any	Any	Any	Any



General

Details

Notifications

Settings

Communication

Update

Security Telemetry

Antimalware +

Sandbox Analyzer +

Firewall +

Network Protection +

Patch Management

Device Control +

Policy Details

Name: \* AutoBros Default

Allow other users to change this policy

History

Created by: Robert Debok

Created on: 28 February 2023, 08:58:13

Modified on: 08 March 2023, 07:30:44

Inheritance Rules *i*

Module Section Policy +

Module Section Inherit from Action

Save

Cancel



# SaaS Security

ConnectWise SaaS utilizes ConnectWise SIEM and SOC to secure:

- Microsoft 365®
- Azure AD
- OneDrive

Provides:

- Multi-tenancy dashboard
- Out of the box reporting and alerting
- Real-time analysis of threats

## Overview of Alerts by Applications

### 1.1 Microsoft: Overview of Alerts

Overview of alerts last month vs this month



### 1.2 Microsoft: Breakdown of Alerts

Breakdown of the alerts

Impossible Travel Alert 40	Access to google Drive 30	Failed Logins 20
	Bulk Upload Data 20	Lorem Ipsum 20
	Bulk Download Data 20	Lorem Ipsum 20

### 1.3 Microsoft: Top 5 most Vulnerable email IDs

Breakdown of the alerts



- ←
- Favorites
- Dashboards
- Clients
- Service Delivery
- Devices
- RMM Tools
- Security**
  - Overview
  - Profiles
  - Activation
  - Vulnerability Mgmt
  - Assessment
  - Reporting
  - SaaS Security**
  - Exception Management
- Sales
- Finance
- Reporting

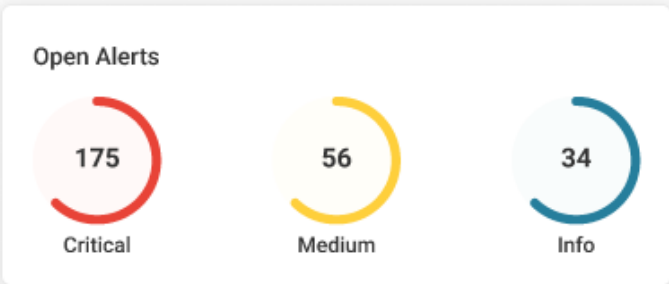
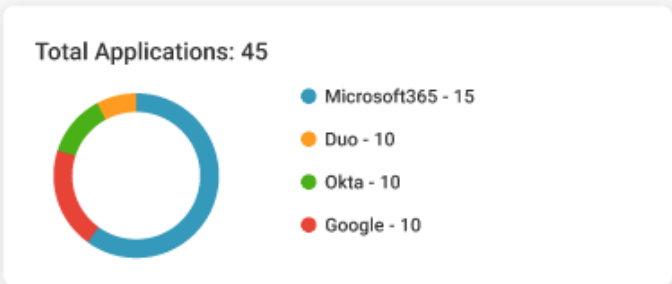
SaaS Security / Arti ATX

## Company: Arti ATX

- Alerts**
- Applications Configured
- Rules
- Reports

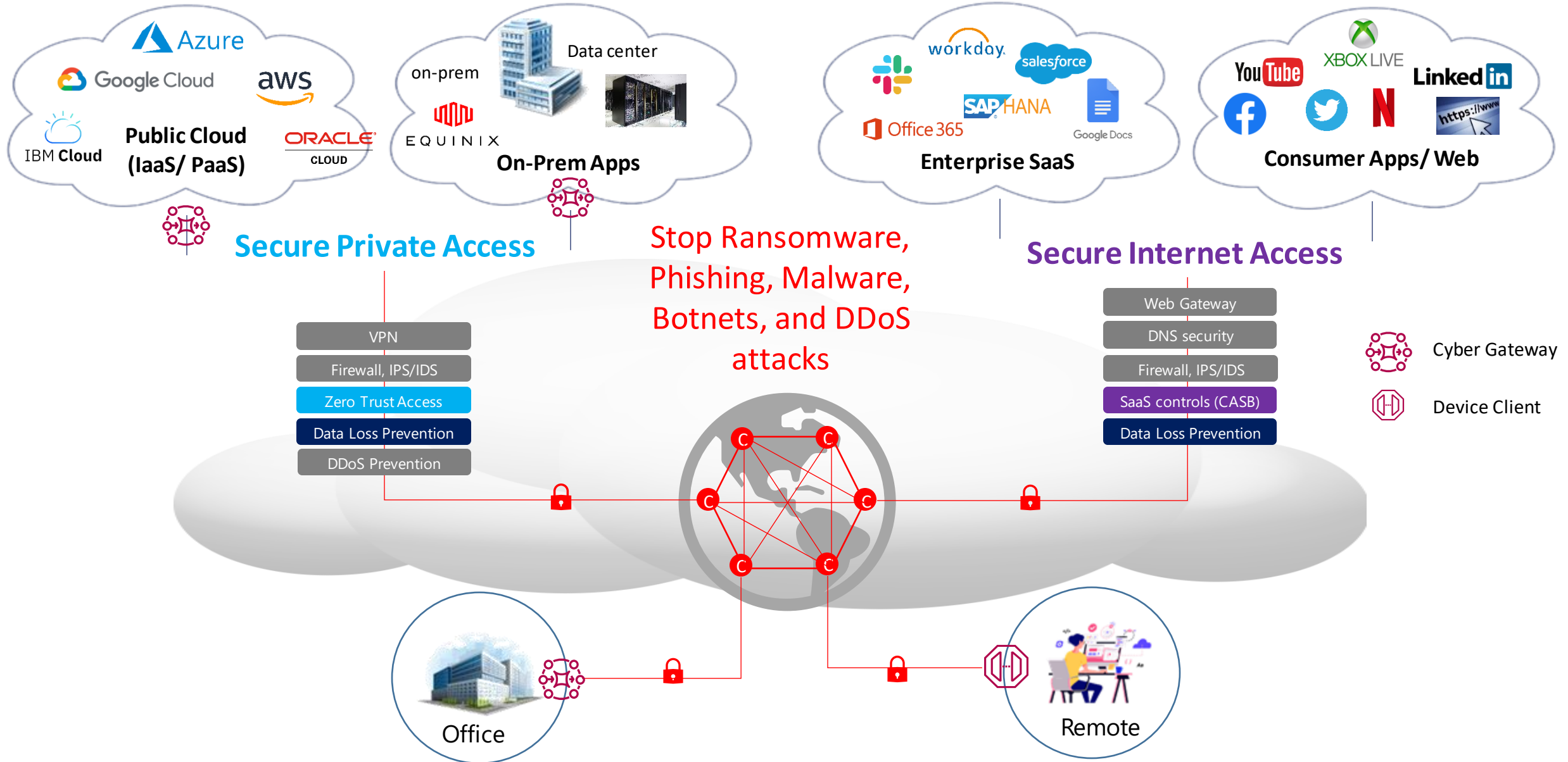
- Remediate
- False Positive

- Ask Community
- Settings
- Download




<input type="checkbox"/>	Alert	Description	Application	Severity	Detected On	Status	Action
<input type="checkbox"/>	Login Alert	Login Alter details XYZ	Microsoft Office 365	CRITICAL	12/16/2022 - 6:03 am EDT*	Not Reviewed	<a href="#">View Details</a>
<input type="checkbox"/>	Unusual Traveling	Lorem Ipsum	Okta	MEDIUM	12/16/2022 - 6:03 am EDT*	Investigating	<a href="#">View Details</a>
<input type="checkbox"/>	Failed Login Attempt	Lorem Ipsum	Microsoft Office 365	INFO	12/16/2022 - 6:03 am EDT*	On Hold	<a href="#">View Details</a>
<input type="checkbox"/>	Unusual Login	Lorem Ipsum	Google	INFO	12/16/2022 - 6:03 am EDT*	Escalated	<a href="#">View Details</a>
<input type="checkbox"/>	XYZ Alert	Lorem Ipsum	Microsoft Office 365	MEDIUM	12/16/2022 - 6:03 am EDT*	Escalated	<a href="#">View Details</a>

# SASE Secure Access Services Edge



# SASE

### Legacy Secure Access



VPN

IPS

Secure Web Gateway

Firewall

SD WAN

DNS

Security Personnel, Policies/Configs, Contracts....

### Secure Access Services Edge (SASE)



Single, Integrated Platform

Zero Trust  
Granular Security

Cloud Service

Simpler, Lower TCO & Delivered as a Service

# ConnectWise Cybersecurity Ecosystem

Collect & Analyze Log Data



IT NATION™ **SECURE**





- Home
- Intelligence
  - Alerts
  - Escalations
  - Suppressions
  - Communities
  - Indicators
  - Sensors
- Marketplace BETA
  - Explore
  - Manage
- Perchybana
- Metrics
  - Hero Dashboard BETA
  - Usage
  - Integration Health
  - Onboarding

Date Range  
Last 7 days

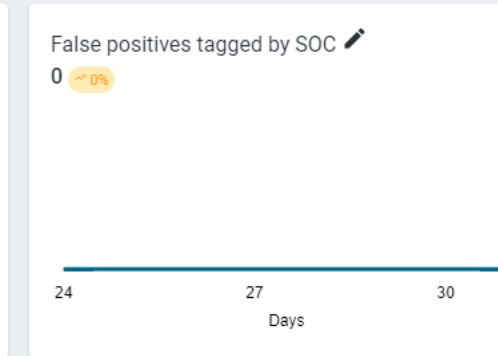
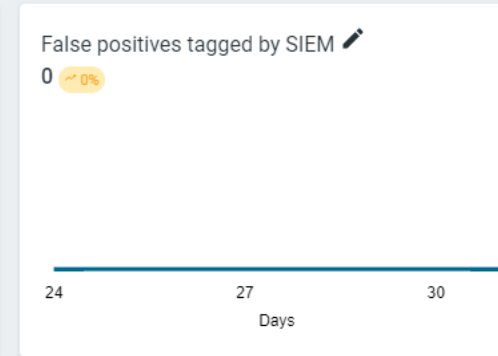
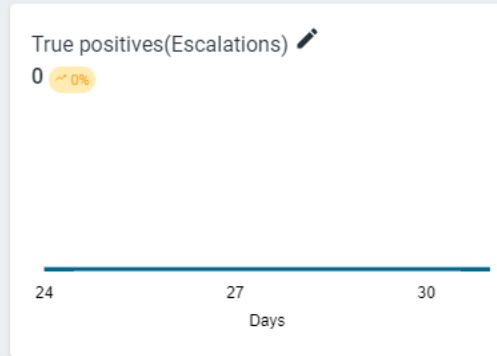
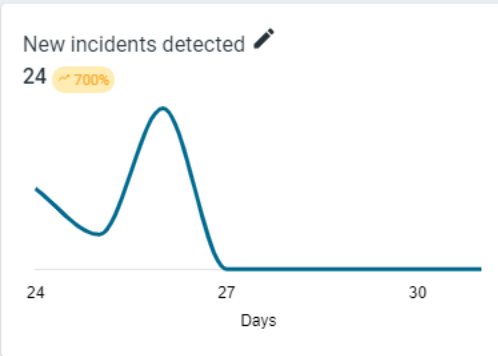


### Executive Summary

ConnectWise SIEM ingested and processed **477,705** logs sent by data sources to the SIEM from **November 24, 2022** to **December 01, 2022**. All ingested data is analyzed through both automated and manual processes developed by ConnectWise's Security Operations team based on industry best practices. This analysis resulted in a total of **24** potential threats.

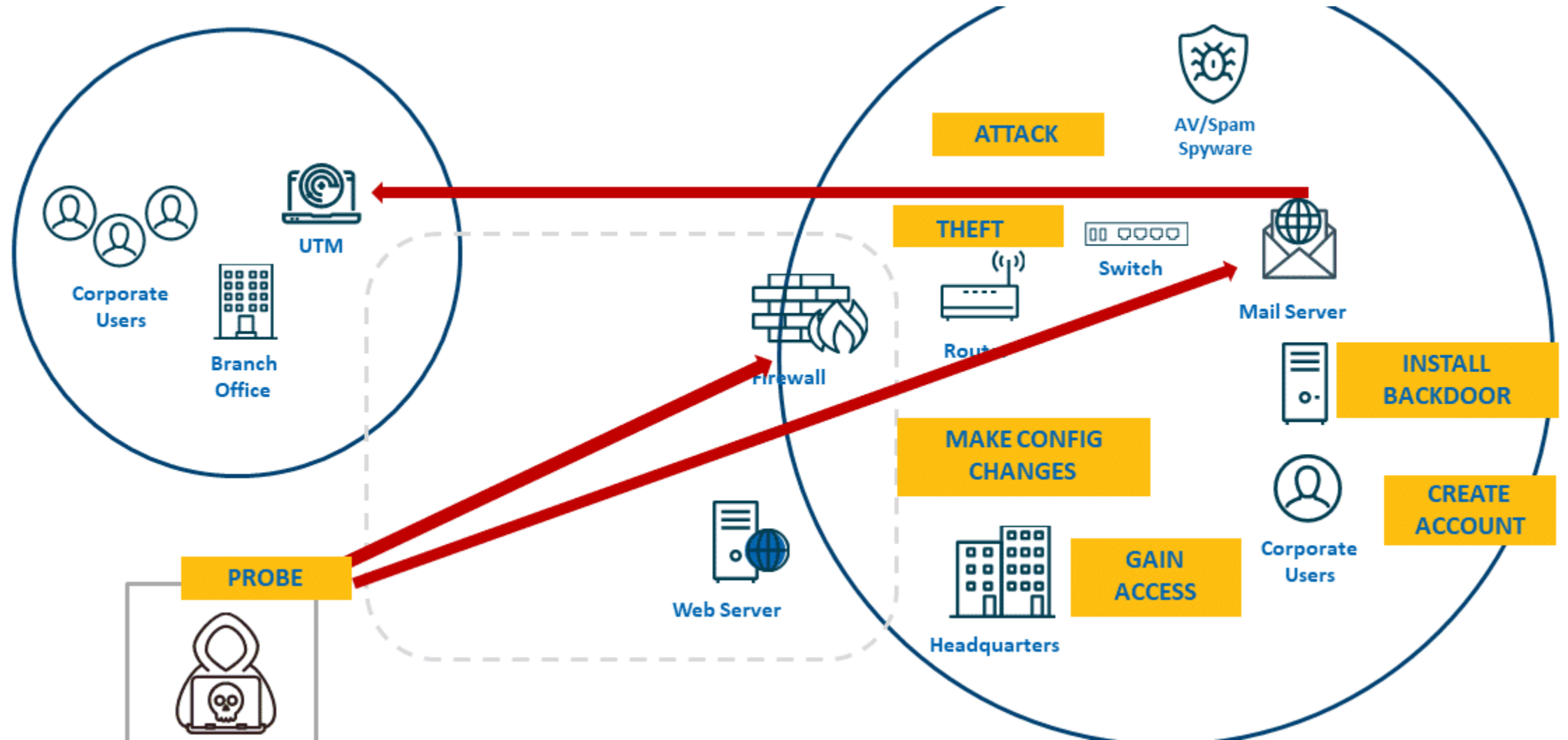
### Remediated & Escalated

ConnectWise SIEM/SOC reviewed **24** alerts for your organization from **November 24, 2022** to **December 01, 2022**. An escalation is sent whenever a high-severity alert (or requested notification) occurs. These escalations are sent as a result of the finely tuned rules created together with the SOC and your organization, and are usually limited to items that require immediate action unless you've provided alternative notification instructions to the SOC. In addition to the requested notifications, the Security Operations Center staff escalated **0** alerts as part of the threat analysis performed for your organization.



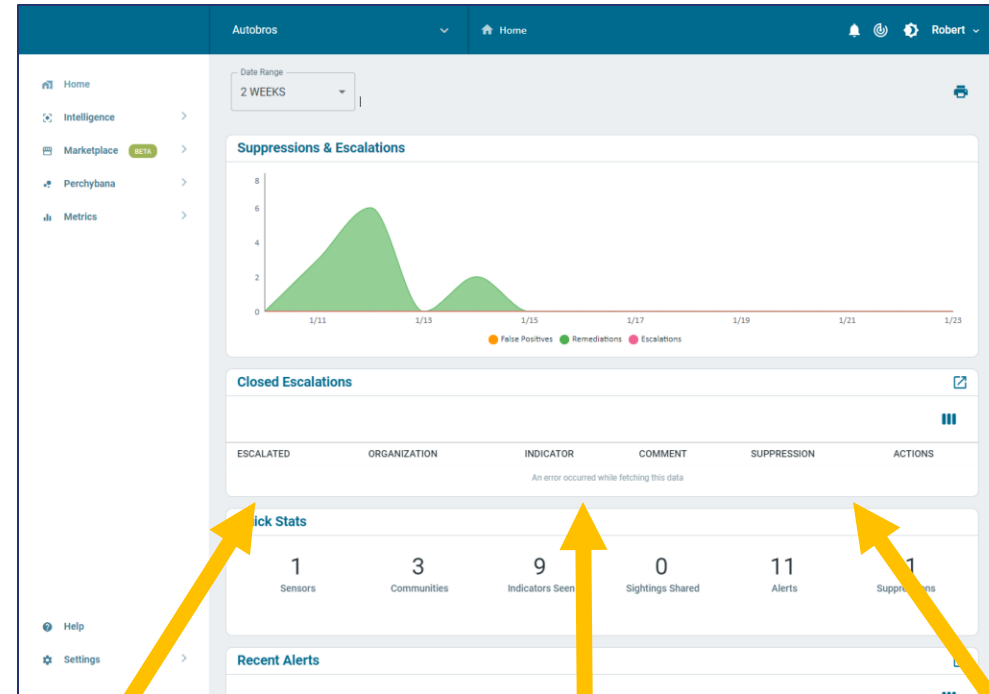
- Help
- Settings

# Security Information and Event Management (SIEM)



# Components for the SIEM

- SIEM App (Web)
- Sensors
- Log Shipper
- Integrations





# ConnectWise Cybersecurity Ecosystem

Respond & Remediate Cyber Incidents



IT NATION™ **SECURE**

# Incident Readiness

- Develop an Incident Response Plan
- Identify Critical Assets
- Backup Critical Data
- Conduct a Risk Assessment
- Train Your Staff
- Implement Security Controls
- Conduct Regular Testing and Drills
- Engage Third-Party Experts
- Test Backups



# Incident Response Services

1. Contain the threat quickly
2. Remotely assess and remediate intrusion to be back operational quickly
3. Determine root cause and patient zero to recommend additional security controls to enhance security
4. **Monitor environment after incident for 30 days to capture re-infections**
5. Option to purchase monitoring service beyond 30 days

## Retainer-Based



- Establish incident preparedness
- Knows who to contact at company
- Act quickly by understanding basics of customer environment

## On-Demand



- Get help in an emergency
- 24/7 hotline



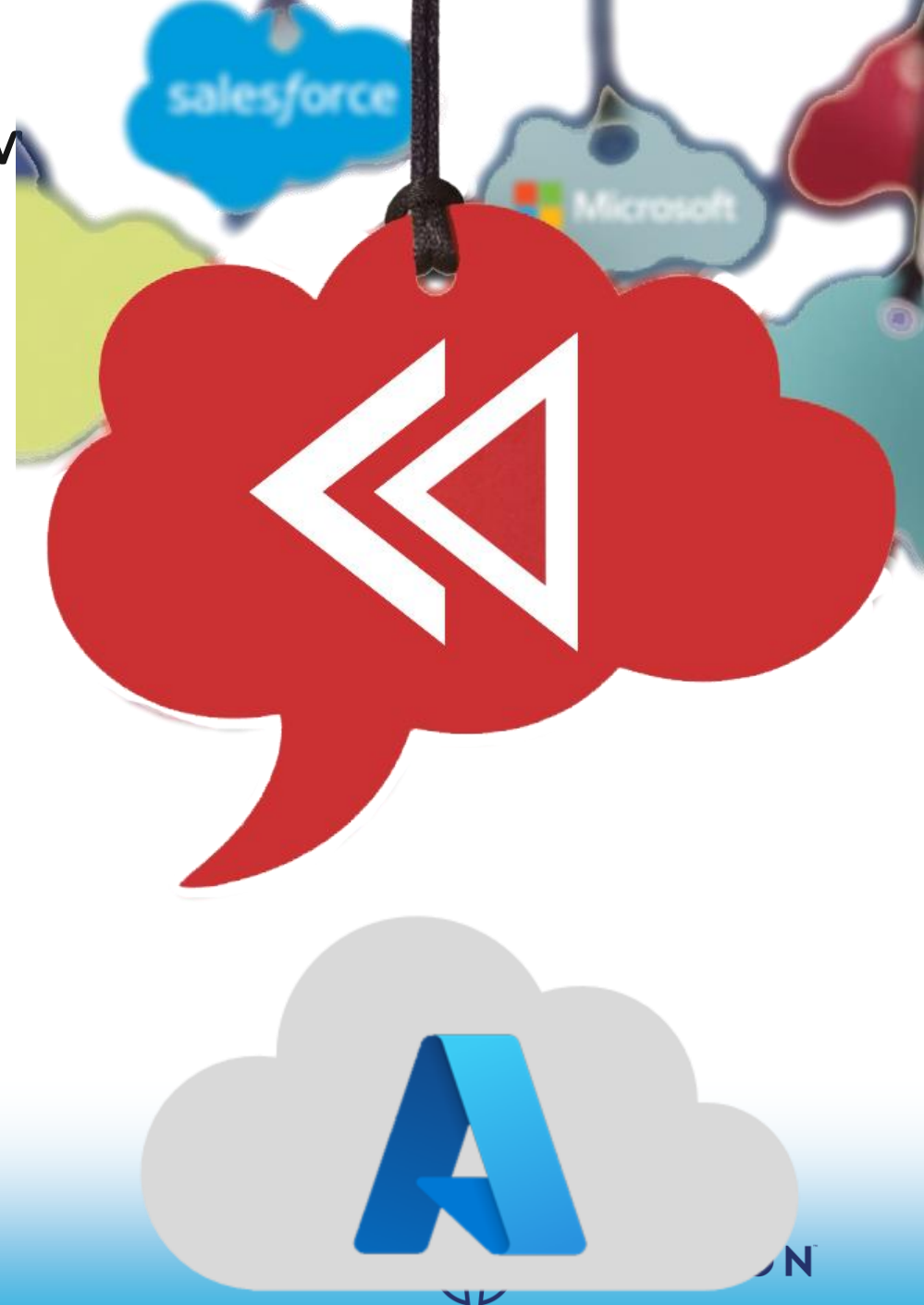


# ConnectWise SaaS Backup™

ConnectWise Recover SaaS delivers a single, integrated view of SaaS data backups.

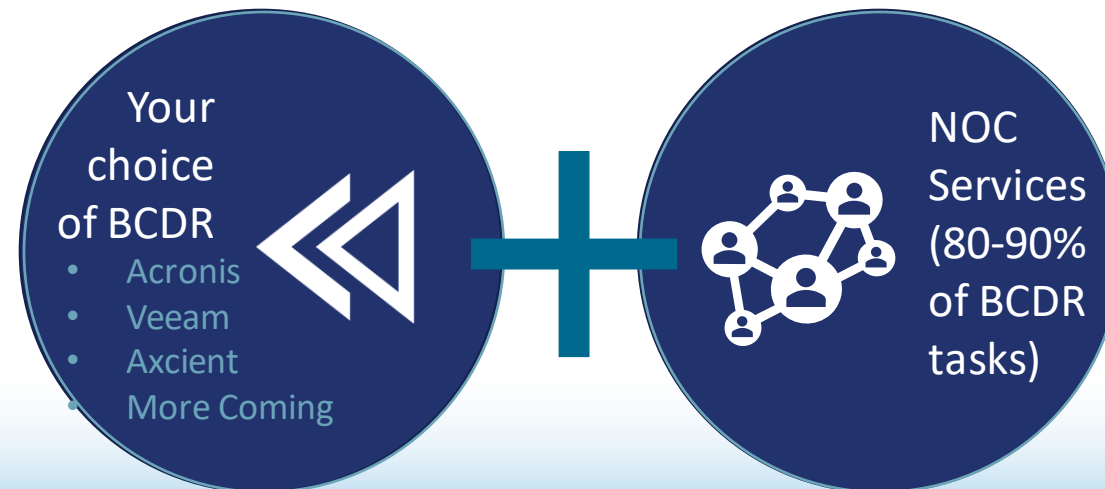
- Full cloud data protection
- Easy set up; easy recovery
- Configurable retention
- Quickly find and restore

Azure AD Backup is FREE!



# ConnectWise Co-Managed Backup™

*If you Manage multiple backup services, This will be a fit for you. With this solution, our NOC can take 80-90% of backup and disaster recovery tasks off your internal technicians' to-do lists. You select the BCDR of your choice and our team monitors all your BCDRs through a single console.*



# ConnectWise Partner Program

## REGISTERED PARTNER

Grow at your own  
pace



### SELF-PACED JOURNEY

- Access to on demand education
- Brandable marketing assets
- Marketing automation platform
- Free fundamentals certification

## ACCELERATE PARTNER

Grow with expert guidance



### BUSINESS READINESS

- Sales, marketing, tech readiness
- Optional internal assessment
- Implement ConnectWise cybersecurity
- Pricing and bundling tips
- Free advanced certifications



### LEAD GENERATION

- Dedicated marketing concierge
- Market Development Funds
- Earn Co-Op Funds on growth
- Ready to use campaigns and assets for clients & prospects
- Access to Subject Matter Experts for events



### CLOSING DEALS

- Dedicated partner development manager
- Sales training for your team
- Sales framework coaching
- Access to pre-sales resources
- Co-Sell opportunities
- Sales debrief

#ITNation

**New cybersecurity tracks:** *Compliance, cyber insurance, and addition of BCDR to the Partner Program*



IT NATION

# Next Steps

- Register for the Partner Program today
  - Registered or Accelerated Partner
- Take advantage of our diverse and cohesive ecosystem
- Become ConnectWise Cybersecurity Certified in the University
  - ConnectWise Certify™ Training: Sales and Technical
- Get Started Now >> Choose progress over perfection



*Don't forget to fill out your*

# **SESSION SURVEY**