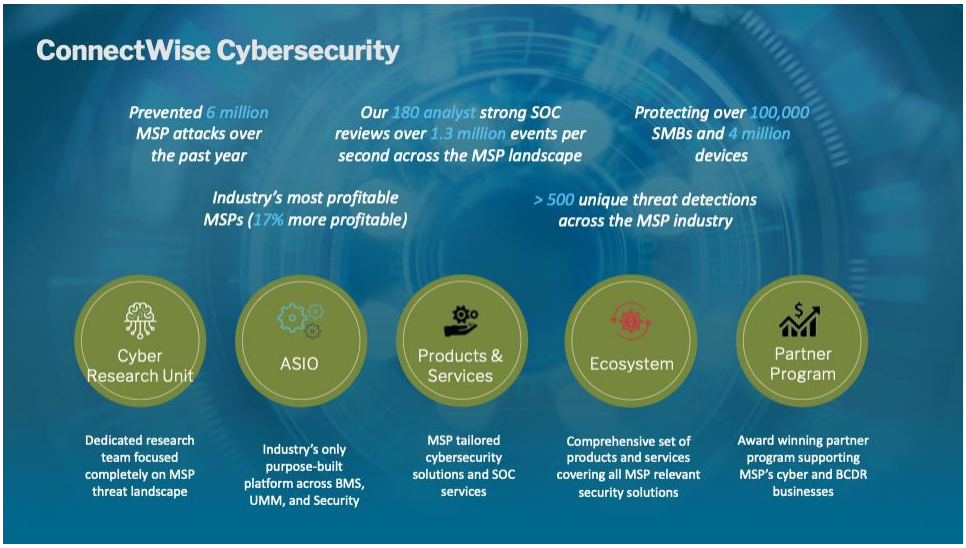
IT NATION Secure

Cybersecurity Management Prep

Have the best Business Management conversations at IT Nation Secure after you've reviewed this sheet!

Keynote Highlights



a. Product Announcements (see next section)
b. CW security ecosystem is growing -> added Proofpoint as partner, **[DO NOT TALK ABOUT THESE IN PUBLIC!]**
c. On BCDR side, new announcement of Axcient partnership and Auvik for network monitoring

Product Announcements

- **CW SaaS Security Essentials**
    - Why does this matter for the MSP?
        - SaaS applications are being used more and more in organizations which also leverage managed service providers and technical service providers. These applications need to be secured.
        - SaaS Security Essentials will continue to grow in capability with the demands of the cloud security industry.
        - Guidance in mitigation and investigation gives our partners confidence in taking action.
    - Launching End of June
    - Microsoft 365 alerting
    - Google Workspace alerting
    - All Alerts will be pre-curated by the Global Security Operation team

- Self-service integration installation
- Self-service opt in and out of alerts
- Lives fully in Asio
- FAQ-
    - ***What is the cost?*** List price is 3 dollars per user. As this is cloud based detection and alerting, the usage will be based per user.
    - ***Can Partners create their own rules?*** Not within this product. It is meant to be simple. If a partner would prefer to be able to create their own rules, they would want to subscribe to CW SIEM or CW Co-Managed SIEM.
    - ***Is there guidance for processing the alerts?*** Yes, we have a knowledge base in CW University with guidance on many of the different alerts and how one can go about investigating them.
    - ***Do we have reports available?*** Not in this first release, however it is meant to follow in our second major release.
    - ***How is this different from the SIEM?*** This contains a subset of the rules that are available for O365 in the SIEM. There's currently no SOC option with SaaS. SIEM has endpoint and perimeter monitoring, SaaS does not.
    - ***Will other integrations be made available?*** Yes, okta and duo are in line next, after which we will be considering additional impactful integrations.
    - ***How is this different from the existing SaaS Security solution*****?** This is completely self-managed, not under the control of the SOC. Integration of cloud services can be done completely by our partners. All alerts are viewable in Asio, there's no need to log into another portal to see your SaaS Security Essentials Alerts.
    - ***What happens to partners on the existing SaaS Security solution*****?** Currently, there is no change for existing SaaS Security customers. Existing SaaS Security Customers are welcome to transition to SaaS Security Essentials, if they would prefer a self-managed SaaS monitoring product within Asio.

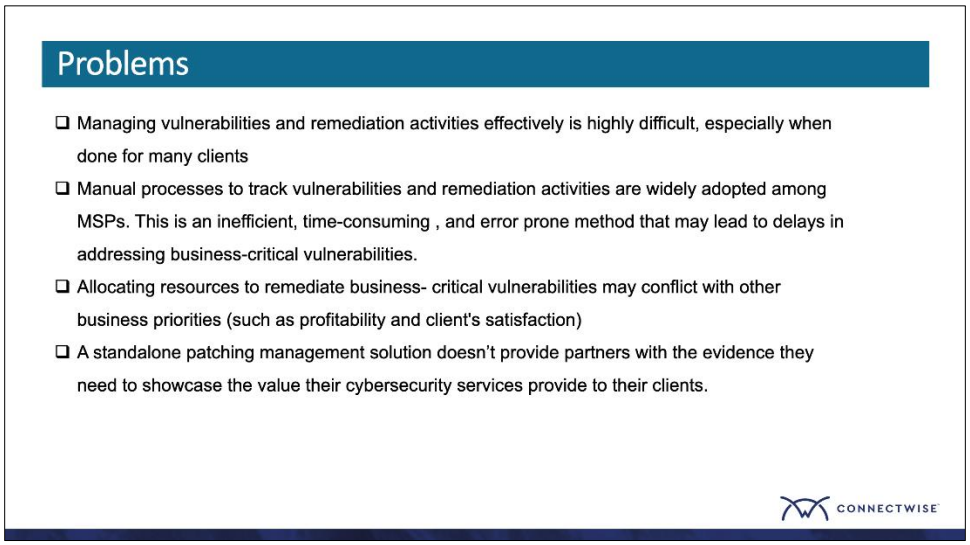
SaaS v SaaS Security Essentials Comparison

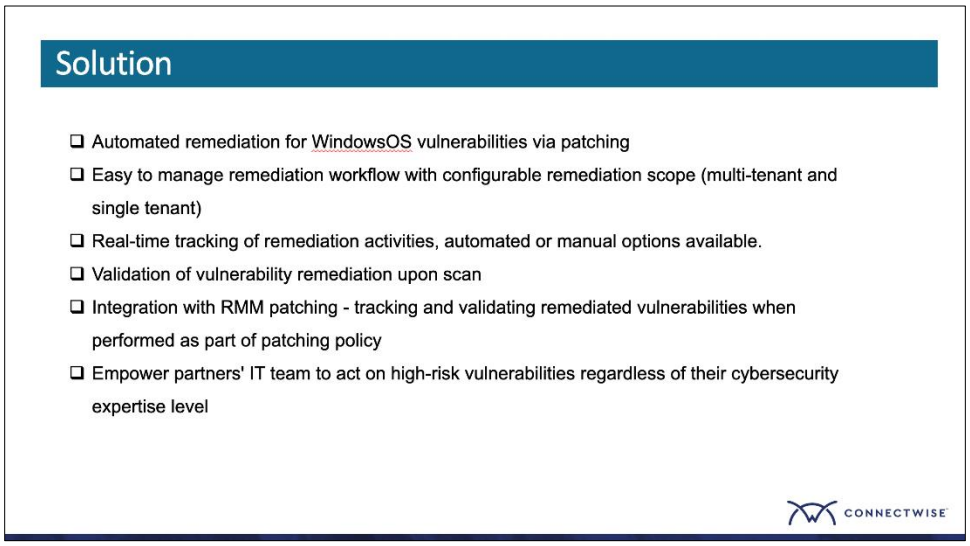
Feature	SaaS V2	SaaS V1
SOC Alert Analysis	N	Y
SaaS Integration Monitoring	Y - O365, Gsuite first iteration	Y - Only O365
Endpoint Monitoring	N	N
Asio Integrated Access	Y	N
Custom Rule Creation	N	N
Security Operations Curate Rules	Y	Y
Simple Remediation Instructions	Y	N
Report generation	Y	Y
Field normalization across indexes	N (eventually, with ECS effort)	N (eventually, with ECS effort)
External Enrichment (reputation lookups, etc)	N	N
Executive reports (audit friendly)	N (not in first iteration, future iteration, yes)	Y - minimal, limited by only O365 data
CRU Driven (threat intel driven alerting)	Y	Y
Alert Chaining	N	N

- Vulnerability Management

- What's New / Feature Release Timeline
  - *Vulnerabilities Patch Management – MVP* Mid-June
    - Partner can automate vulnerability remediation via patching of Windows OS devices
    - If automated remediation isn't available, and a remediation method is publicly available, partner can easily access the information on either vendor site or NVD catalog
    - Partner can easily filter vulnerabilities by remediation status, to only focus on high priority vulnerabilities that remediation solution is publicly available
  - *Vulnerabilities Patch Management – Phase 2 Time TBD*
    - Remediation via patching Windows OS – Enhance Coverage
    - Partner can automate remediation of vulnerabilities detected in MacOS devices
    - Partner can automate remediation of vulnerabilities detected in 3rd party applications

- On-demand Vulnerability scanning
- Remediation workflow management & Vulnerability patching (WindowsOS) features- Launching Mid-June
- The new features will be available to every partner with an active vulnerability management entitlement
- Problems and Solutions





- Vulnerability Management FAQs
  - ***What is vulnerability management? Vulnerability management is an Information Security Continuous Monitoring (ISCM) capability that identifies Common Vulnerabilities and Exposures (CVE) likely to be used by attackers to compromise on an asset and use it as a platform from which to extend compromise to the network. For MSPs, it helps identify vulnerabilities, prioritize risk, enable patch management, address compliance requirements,***

enhance client trust and reputation, support incident response and recovery, and adopt a proactive security posture.

2Q: How does ConnectWise Vulnerability Management fit within an MSP cybersecurity stack?

A: It helps MSPs take a proactive security approach and improve their posture with continuous scanning. Clients seek an automated and flexible Windows OS patching solution to initiate and monitor remediation of high-business risk vulnerabilities at global, site, and individual levels. ConnectWise Vulnerability Management helps MSPs and TSPs minimize risks and maintain security postures by managing vulnerabilities efficiently and proactively remediating business-critical vulnerabilities quickly. It empowers partners' IT and security teams to act on high-risk vulnerabilities regardless of cybersecurity expertise and maturity levels.

3Q: Are standalone patching management products adequate vulnerability solutions?

A: Patch management is part of vulnerability management, a much broader process for identifying and fixing security issues. Only about 30 % of vulnerabilities cannot be remediated with patching and it doesn't satisfy compliance auditing and reporting needs.

4Q: Is ConnectWise Vulnerability Management integrated with other ConnectWise solutions?

A: Yes. ConnectWise Vulnerability Management is integrated with ConnectWise RMM patching and will track and validate remediated vulnerabilities when performed as part of patching policy. Our product goal is to integrate with the entire CW ecosystem.

5Q: Who can currently use ConnectWise Vulnerability Management?

A: Yes. ConnectWise Vulnerability Management was announced November 2022 and is already part of the CW Asio platform. It is globally available under Product Code CW-VULNERABILITYMGNT with usage-based tiered pricing starting at $2 per endpoint and available to CW RMM or Command partners. The new remediation feature is available to those CW RMM or Command partners with an active vulnerability management entitlement.

6Q: What are the main challenges the vulnerability management remediation feature helps resolve?

A: Effectively managing vulnerabilities and remediation activities are difficult, especially for multiple clients. Manual processes widely adopted among MSPs are inefficient, time-consuming, and error-prone and often lead to delays in addressing exposures. Additionally, allocating resources to remediate vulnerabilities may conflict with other business priorities such as profitability and client satisfaction.

7Q: Will ConnectWise Vulnerability Management be featured at ITN Secure 2023?

A: Yes. Please attend the Vulnerability Management Focus Group, June 6, 1:00 PM and general session, “Vulnerability Management: Why You Need it and How ConnectWise Can Support You”, June 7, 3:15 PM. A live demo will be available at the ConnectWise booth.

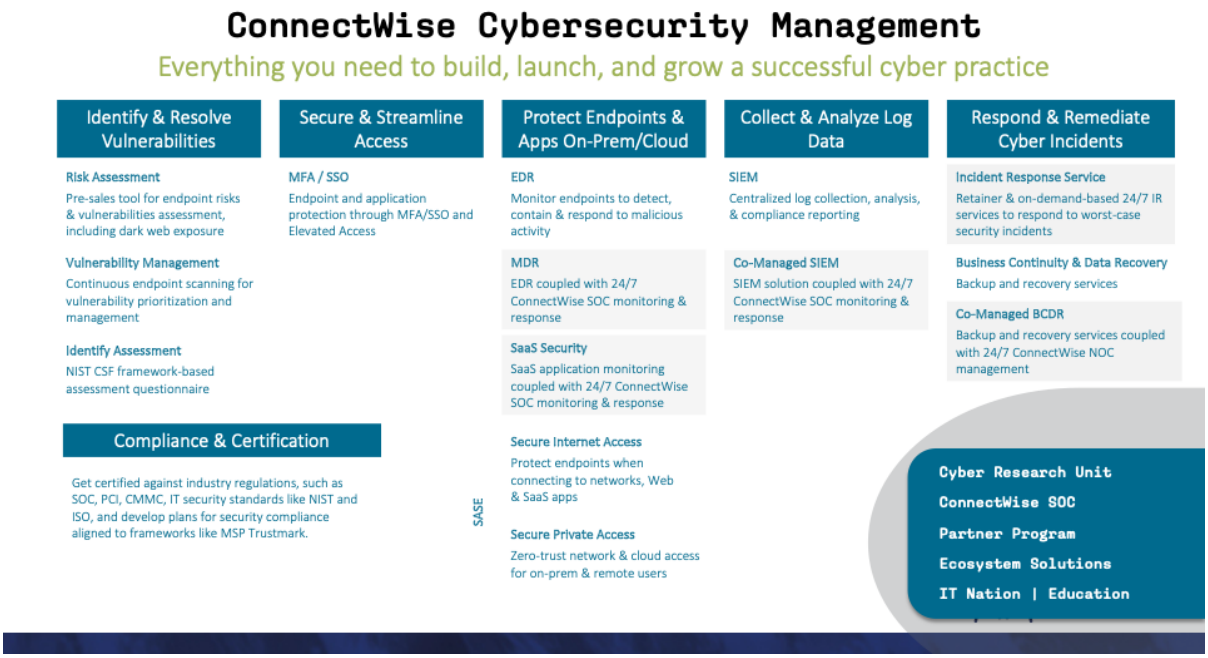
New ConnectWise SIEM 3.0 Features

- **Microsoft Azure security monitoring** using new and specifically focused rule sets provides full visibility into Microsoft Azure platform activity. Partners can now provide their clients with comprehensive Microsoft 365 security monitoring that includes Azure-level activity.
    - Monitors all Microsoft 365 alert and activity sources from the underlying Azure infrastructure for access
    - Provides insight into alerts, violations, and activity sources and types including Top Users, Top Workloads, Top Operations, and Exports
    - Download rule sets from the ConnectWise Marketplace and add Azure security monitoring capabilities to ConnectWise SIEM
    - Available mid-June
- **Endpoint Threat Detection** improvements help monitor EDR data within ConnectWise SIEM, provide better threat detection, and help co-sell ConnectWise MDR and SIEM.
    - **New EDR and IDS Dashboards** monitor EDR data with ConnectWise SIEM to show the value of combining high-fidelity and targeted alert information to assist investigations.
        - Delivers alert from our EDR platform (initial set is Sentinel One) and IDS capability (ConnectWise SIEM)
        - IDS component displays network traffic and monitoring to reduce analyst investigation time
        - Available now in the ConnectWise Marketplace
- **True Retention** allows analysts to search the retention period that was purchased with certain performance constraints. Search default period is 30 days to 12 months with upgrade. Data archiving is coming soon.
- **ECS Common Schema** normalizes field name and event type data for easier analysis.
    - **Field Normalization** leverages the same (standardized) field names across all data sources to support advanced correlation, simpler search capability and dashboard creation.
    - **Categorization** groups event sets by monitored behavior types for easier, more efficient correlation (used in rules creation) and alert understanding.
    - First rule set coming soon
- **SOC Value Report** conveys to partners and their clients ConnectWise SIEM capabilities and the value MDR provides to security postures.
    - Presents suspicious alerts, true and false positives, and investigated alerts with ticket handling for the previous month
    - Features easy-to-understand visual graphs
    - Available only through Asio
    - Available in late June
- **ConnectWise Q1 2023 MDR + SIEM Promo Campaigns** are now available to drive Cybersecurity business growth.

Product	Offer

MDR + Co-Managed SIEM	$14/user/endpoint, if the partner purchases MDR and Co-Managed SIEM SKUs they get a 30% discount on those SKUs.
MDR+ SIEM+ SASE	$20/User/endpoint, if the partner purchases MDR and SIEM and SIA SKUs they get a 30% discount on the MDR and SIEM SKUs. RESTRICTION: Discount can apply to either SIA or SPA, but not both.

In-Market Solutions



ConnectWise Lead Sessions

Session Name and Location	Speaker(s)
June 5th	
ConnectWise Cybersecurity Keynote - General Session Ballroom	**Patrick Beggs, Peter Melby, Raffael Marty, Jason Magee**
June 6th	
Don't Miss Your Targets: Applying Modes, Maturity, and Matchmaking to Your Cybersecurity Practice - Miami	Scott Scrogin, Brad Schow, Tim Weber,Mike Ritsema
Zero Trust for MSPs - Understanding What it is, Why it Makes Securing Clients Easier, and Improves - Sarasota	**Jay Ryerse, CISSP,Drew Sanford**
SIEM v3.0 – Today & Future Roadmap - Tampa	Alicia Jeatsa, Roopak Patel
The ConnectWise Cybersecurity Vision & Roadmap - Osceola 1-3	**Raffael Marty**
Hosted Guest Lunch & Solution Pavillion Time - Desoto 1-3	Ameer Karim, Patrick Beggs, Jay Ryerse, CISSP,Raffael Marty,Drew Sanford,Jason Magee
How ConnectWise Business Management Solutions Support Your Cybersecurity Business - Naples	**James Riley,April Taylor**
Stack It Up to Knock Them Down - Sanibel	Robert DeBok
Workshop: Create your Cybersecurity Marketing Strategy - Miami	**Brianna Allen**
Engineering Resilience Culture: An Operational Approach - Sarasota	Matt Topper
MSP Threat Report- Top Threats Facing our Industry and Predictions for the Next 6-12 Months - Osceola 1-3	**Bryson Medlock, Drew Sanford**
Eliminate shared admin passwords and protect customers from security threats with ConnectWise Access - Sarasota	Ciaran Chu,Scott Linak, Jake Morgan
Vulnerability Management: Why You Need it and How ConnectWise Can Support You - Naples	**Tammy Cohn, John Helms**
Trust Issues: How to Select a Trusted Vendor - Sanibel	Patrick Beggs, Sean Lardo
Service Leadership –How High OML MSPs Sell More Security More Profitably - Osceola 4-6	**Peter Kujawa**
SaaS Security – You Can't Ignore That Your Data Lives in the Cloud, So What Are We Going to Do ? - Naples	Alicia Jeatsa, Roopak Patel
June 7th	
Navigating the Future: Balancing Innovation, Value, and Risks in the Era of AI for MSPs - Tampa	**Tony Thomas**
Acquiring Clients 101: Creating Demand & Closing Deals - Miami	Tim Weber, Ed Correia, Mark Banens, Maddie Metheny, Jay Ryerse, CISSP
Radical Resilience: A radical series of ideas, utility, and challenge to the status quo - Naples	**Matt Topper**
The Hidden Powers of Combining Network and Endpoint Detection - Naples	Raffael Marty, Roopak Patel
ConnectWise MDR: True Managed Endpoint Protection - Sanibel	**Robert DeBok**
Leverage the Opportunity: Make the most of the Partner Program co-sell and marketing resources - Osceola 1-3	Brad Schow
Maximize Profit: ConnectWise Co-Managed Backup with Axcient - Tallahassee	**Mike Goldberg**
A Partner's Journey from MSP to MSSP - Miami	Jeff Wynn, Tim Weber, Mike Ritsema, Natalie Suarez
Simply SIEM - Tampa	**Robert DeBok**
Market & Sell Cybersecurity on a Budget - Tallahassee	Maddie Metheny, Jay Ryerse, CISSP
Is the Price Right? Pricing & Packaging Cybersecurity - Miami	**Jay Ryerse, CISSP**
What Happens If: Tabletop Methodology and Live Exercise - Osceola 4-6	Matt Topper