IT NATION™ SECURE

hosted by CONNECTWISE

Zero Trust for MSPs

Presented by Jay Ryerse & Drew Sanford

IT NATION™ SECURE

Relentless Focus on Cybersecurity

No other company invests more to help **secure your business, secure your customers, and grow your cybersecurity practice**.

ADVANCE

Cybersecurity Management Software Solutions

24/7, Global SOC Services

Cybersecurity Partner Program

Incident Response Service

10x 2020

3x 2022

Cybersecurity Investments

Threat Reports

Cyber Research Unit

Cybersecurity Conference

Security Certifications

Security Training

PROTECT

Comprehensive, Compliant Strategy

Partner Trust Center

Third-Party Threat Hunting

24/7 Critical Monitoring

24/7 Emergency Hotline

Incident Response Service

Top Challenges MSPs Face

Accelerating Recurring Revenue
How quickly can you go to market with a new managed service?

Scaling Staff Productivity
Use of multiple individual tools negatively impacts productivity and gets worse with portfolio expansion.

Sales Growth + Go-to-Market
Lack of visibility into SMB trends and pain points makes it challenging to target the most preferred customer segments.

Conveying Business Value
More providers are transforming into MSPs, so conveying business value and service differentiation is getting harder.

Attracting + Retaining Talent
Increasingly, MSPs are competing against global technology firms to hire and keep talent.

Increased Risk + Liability
MSPs are now actively targeted by threat actors, and customers tend to blame MSPs for breaches.

Why Cybersecurity and Why Now?

IT NATION™ SECURE

The MSP Cybersecurity Opportunity

SMBs *want* MSPs to manage cybersecurity but will switch providers if services don't meet their specific needs.

89%

of SMBs are already using an MSP

YET

42%

plan to change to a different MSP in the near future

94%

would consider using or moving to a new MSP if they offered the “right” cybersecurity solution

SMBs are willing to pay

39%

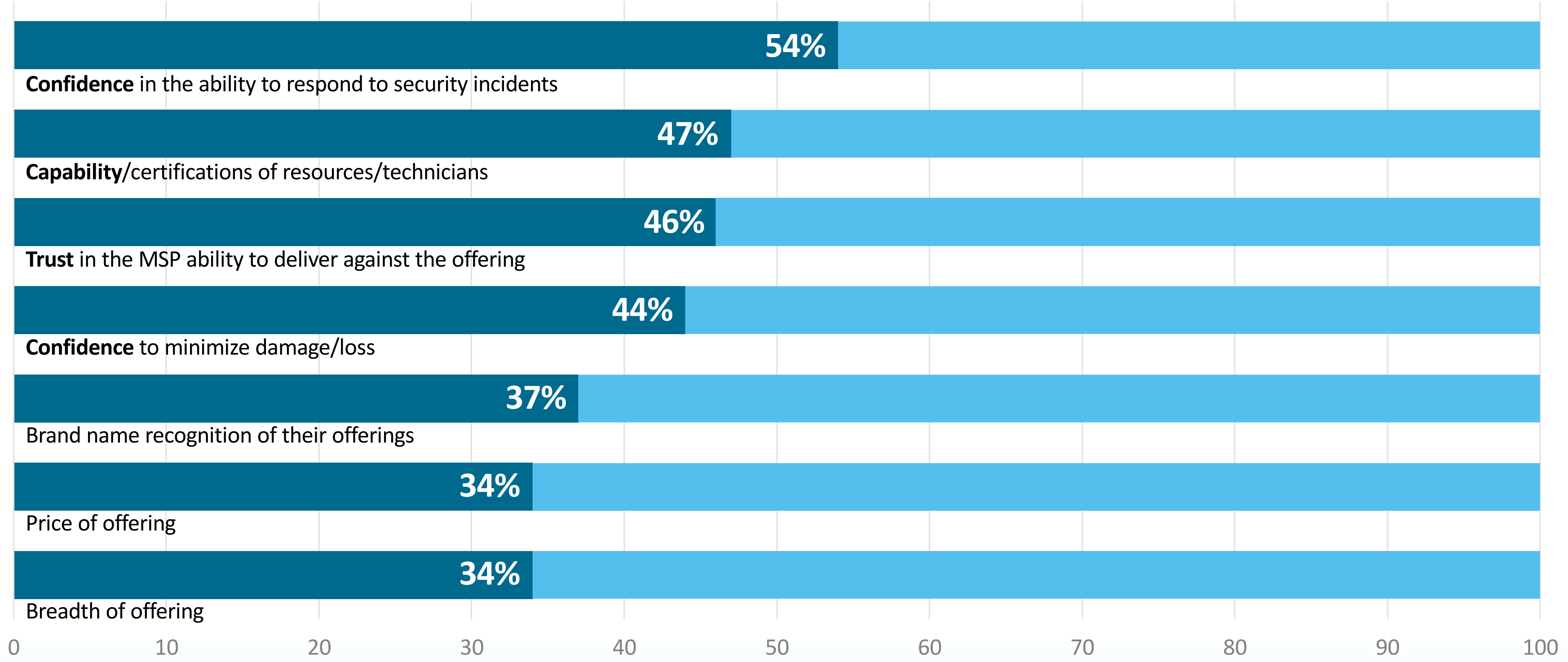
More per year for the “right” cybersecurity solution

#ITNation

*Data from Vanson Bourne survey and report: "The State of SMB Cybersecurity in 2022"

IT NATION

What SMBs Look for in Cybersecurity Services



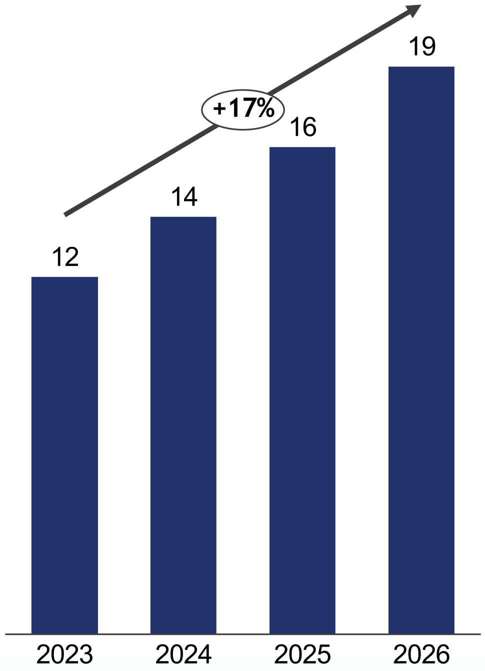
#ITNation

*Data from Vanson Bourne survey and report: "The State of SMB Cybersecurity in 2022"

IT NATION

NA SMB managed cybersecurity grows to ~$20B by 2026

NA SMB Managed Cybersecurity TAM, $B

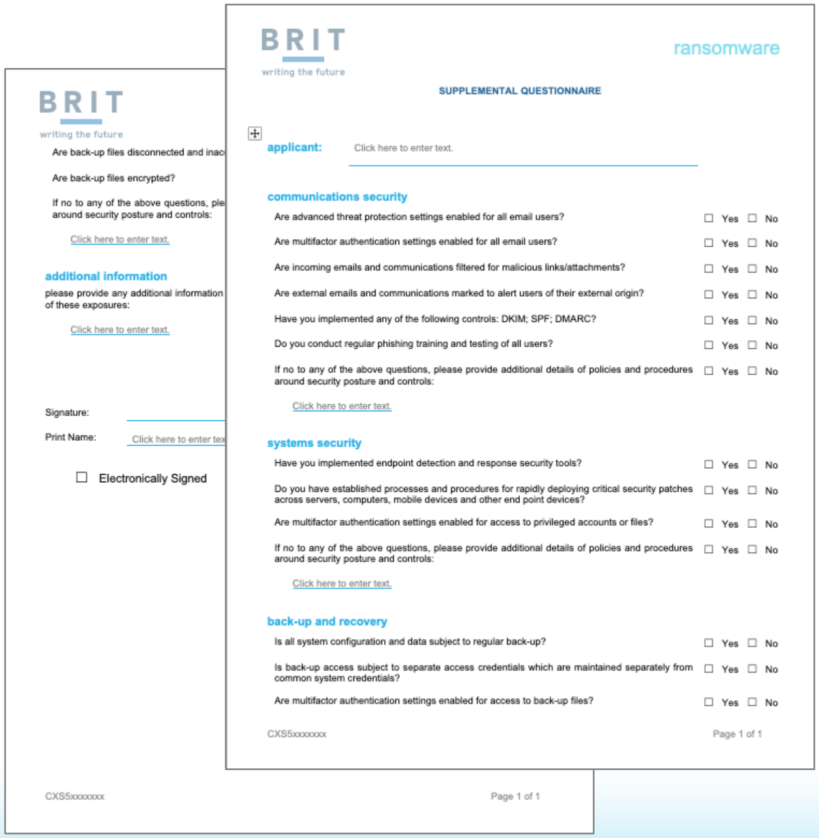


Key Security Investment Drivers and Trends

- **NA SMBs are Financially More Attractive Targets:** Average SMB revenue and digital maturity of NA SMBs much higher than observed in other regions; almost 1 in 3 US SMBs that experienced a cyberattack had to shut down their business
- **Being Prepared is Top of Mind:** Incident response preparedness is becoming important for NA SMBs – vulnerability testing, training, rehearsing responses to actual cyber events are on the rise
- **Improving security readiness:** 1 in 2 SMBs have a security plan and another 30% are in the process of putting one together
- **360° Protection Driving Spend:** Opting for holistic security given more digitalization - on-prem/cloud workloads, devices, physical/virtual servers, endpoints, networks and web gateways
- **NA MSPs Maturing Rapidly :** NA MSPs have more experience with cybersecurity and have been developing their V-CISO capabilities over the last few years – overall more strategic in their approach and service offerings
- **Cybersecurity Insurance on the Rise:** More SMBs are opting for cyber-insurance; insurers now require SMBs to have adequate controls and protection in place to minimize their losses

Source – Analysys Mason and Internal ConnectWise analysis of various public sources (Gartner, Statista, Orange.com, US GAO, Up City, etc.)

Cyber Insurance (and renewals)



BRIT
writing the future

Are back-up files disconnected and inac

Are back-up files encrypted?

If no to any of the above questions, ple
around security posture and controls:

Click here to enter text.

additional information

please provide any additional information
of these exposures:

Click here to enter text.

Signature:

Print Name: Click here to enter tex

□ Electronically Signed

CXS5xxxxxxx Page 1 of 1

BRIT
writing the future

ransomware

SUPPLEMENTAL QUESTIONNAIRE

applicant: Click here to enter text.

communications security

Are advanced threat protection settings enabled for all email users? □ Yes □ No

Are multifactor authentication settings enabled for all email users? □ Yes □ No

Are incoming emails and communications filtered for malicious links/attachments? □ Yes □ No

Are external emails and communications marked to alert users of their external origin? □ Yes □ No

Have you implemented any of the following controls: DKIM; SPF; DMARC? □ Yes □ No

Do you conduct regular phishing training and testing of all users? □ Yes □ No

If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls: □ Yes □ No

Click here to enter text.

systems security

Have you implemented endpoint detection and response security tools? □ Yes □ No

Do you have established processes and procedures for rapidly deploying critical security patches across servers, computers, mobile devices and other end point devices? □ Yes □ No

Are multifactor authentication settings enabled for access to privileged accounts or files? □ Yes □ No

If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls: □ Yes □ No

Click here to enter text.

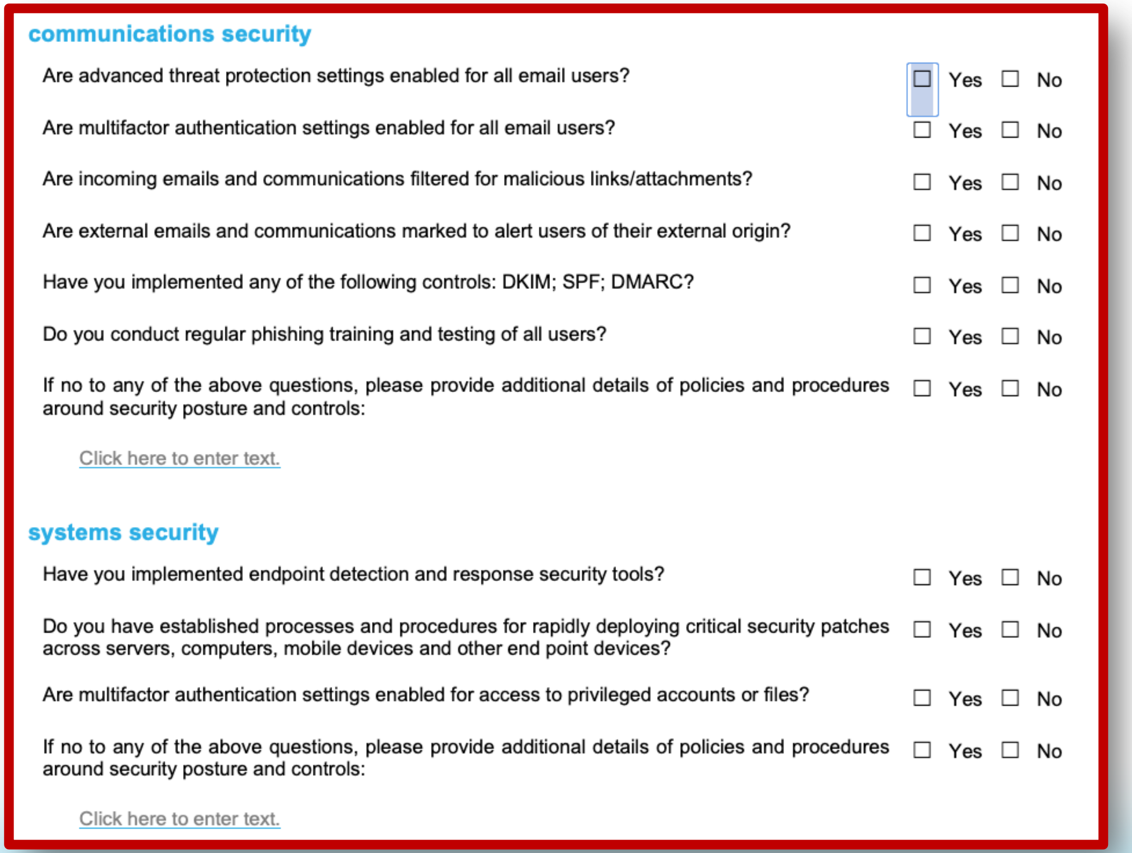
back-up and recovery

Is all system configuration and data subject to regular back-up? □ Yes □ No

Is back-up access subject to separate access credentials which are maintained separately from common system credentials? □ Yes □ No

Are multifactor authentication settings enabled for access to back-up files? □ Yes □ No

CXS5xxxxxxx Page 1 of 1



communications security

Are advanced threat protection settings enabled for all email users? □ Yes □ No

Are multifactor authentication settings enabled for all email users? □ Yes □ No

Are incoming emails and communications filtered for malicious links/attachments? □ Yes □ No

Are external emails and communications marked to alert users of their external origin? □ Yes □ No

Have you implemented any of the following controls: DKIM; SPF; DMARC? □ Yes □ No

Do you conduct regular phishing training and testing of all users? □ Yes □ No

If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls: □ Yes □ No

Click here to enter text.

systems security

Have you implemented endpoint detection and response security tools? □ Yes □ No

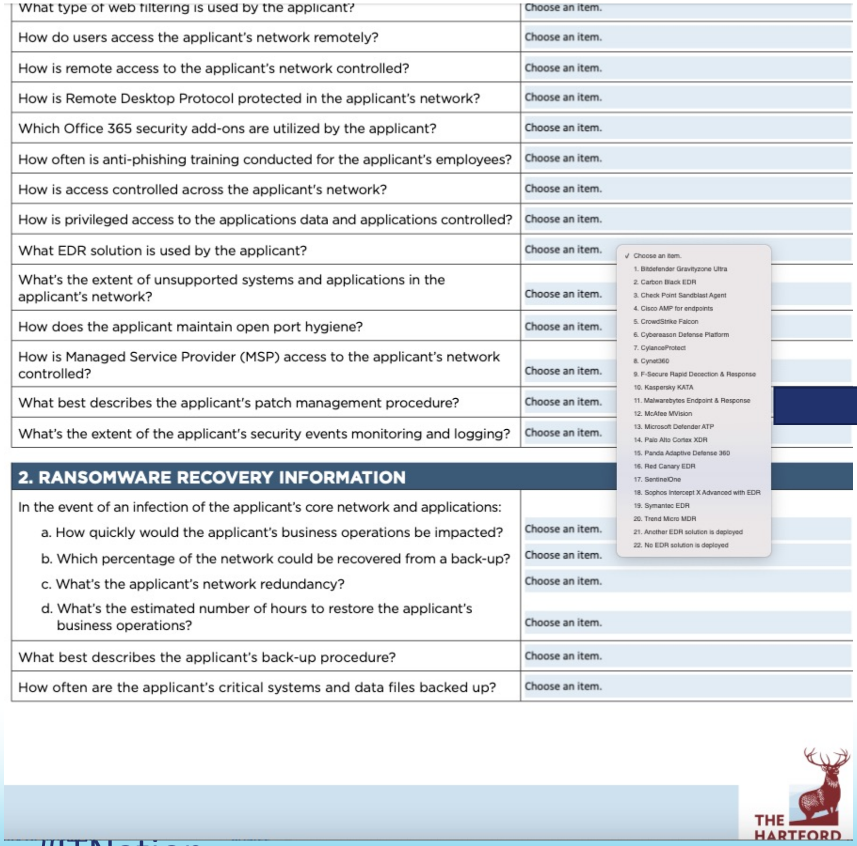
Do you have established processes and procedures for rapidly deploying critical security patches across servers, computers, mobile devices and other end point devices? □ Yes □ No

Are multifactor authentication settings enabled for access to privileged accounts or files? □ Yes □ No

If no to any of the above questions, please provide additional details of policies and procedures around security posture and controls: □ Yes □ No

Click here to enter text.

Cyber Insurance (and renewals)



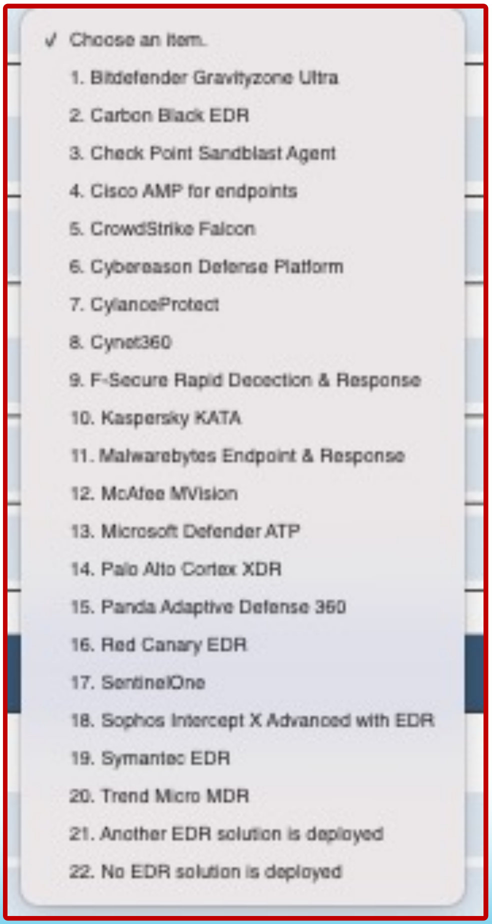
What type of web filtering is used by the applicant?	Choose an item.
How do users access the applicant's network remotely?	Choose an item.
How is remote access to the applicant's network controlled?	Choose an item.
How is Remote Desktop Protocol protected in the applicant's network?	Choose an item.
Which Office 365 security add-ons are utilized by the applicant?	Choose an item.
How often is anti-phishing training conducted for the applicant's employees?	Choose an item.
How is access controlled across the applicant's network?	Choose an item.
How is privileged access to the applications data and applications controlled?	Choose an item.
What EDR solution is used by the applicant?	Choose an item.
What's the extent of unsupported systems and applications in the applicant's network?	Choose an item.
How does the applicant maintain open port hygiene?	Choose an item.
How is Managed Service Provider (MSP) access to the applicant's network controlled?	Choose an item.
What best describes the applicant's patch management procedure?	Choose an item.
What's the extent of the applicant's security events monitoring and logging?	Choose an item.

2. RANSOMWARE RECOVERY INFORMATION

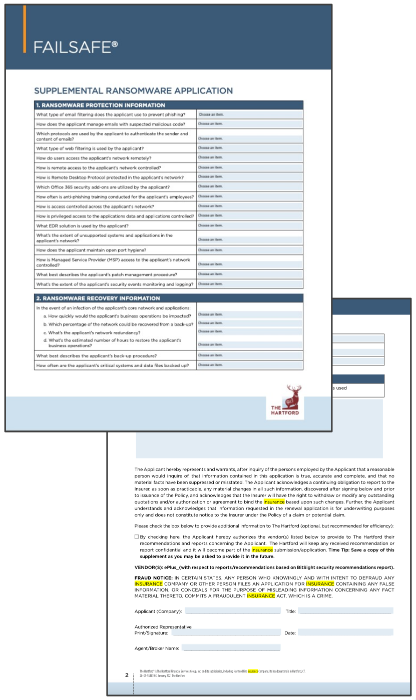
In the event of an infection of the applicant's core network and applications:	
a. How quickly would the applicant's business operations be impacted?	Choose an item.
b. Which percentage of the network could be recovered from a back-up?	Choose an item.
c. What's the applicant's network redundancy?	Choose an item.
d. What's the estimated number of hours to restore the applicant's business operations?	Choose an item.
What best describes the applicant's back-up procedure?	Choose an item.
How often are the applicant's critical systems and data files backed up?	Choose an item.

✓ Choose an item.
1. Bitdefender Gravityzone Ultra
2. Carbon Black EDR
3. Check Point Sandblast Agent
4. Cisco AMP for endpoints
5. CrowdStrike Falcon
6. Cybereason Defense Platform
7. CylanceProtect
8. Cynet360
9. F-Secure Rapid Dececion & Response
10. Kaspersky KATA
11. Malwarebytes Endpoint & Response
12. McAfee MVision
13. Microsoft Defender ATP
14. Palo Alto Cortex XDR
15. Panda Adaptive Defense 360
16. Red Canary EDR
17. SentinelOne
18. Sophos Intercept X Advanced with EDR
19. Symantec EDR
20. Trend Micro MDR
21. Another EDR solution is deployed
22. No EDR solution is deployed

THE HARTFORD



✓ Choose an item.
1. Bitdefender Gravityzone Ultra
2. Carbon Black EDR
3. Check Point Sandblast Agent
4. Cisco AMP for endpoints
5. CrowdStrike Falcon
6. Cybereason Defense Platform
7. CylanceProtect
8. Cynet360
9. F-Secure Rapid Dececion & Response
10. Kaspersky KATA
11. Malwarebytes Endpoint & Response
12. McAfee MVision
13. Microsoft Defender ATP
14. Palo Alto Cortex XDR
15. Panda Adaptive Defense 360
16. Red Canary EDR
17. SentinelOne
18. Sophos Intercept X Advanced with EDR
19. Symantec EDR
20. Trend Micro MDR
21. Another EDR solution is deployed
22. No EDR solution is deployed



FAILSAFE®

SUPPLEMENTAL RANSOMWARE APPLICATION

1. RANSOMWARE PROTECTION INFORMATION

What type of email filtering does the applicant use to prevent phishing?	Choose an item.
How does the applicant manage emails with suspected malicious code?	Choose an item.
Which protocols are used by the applicant to authenticate the sender and content of emails?	Choose an item.
What type of web filtering is used by the applicant?	Choose an item.
How do users access the applicant's network remotely?	Choose an item.
How is remote access to the applicant's network controlled?	Choose an item.
How is Remote Desktop Protocol protected in the applicant's network?	Choose an item.
Which Office 365 security add-ons are utilized by the applicant?	Choose an item.
How often is anti-phishing training conducted for the applicant's employees?	Choose an item.
How is access controlled across the applicant's network?	Choose an item.
How is privileged access to the applications data and applications controlled?	Choose an item.
What EDR solution is used by the applicant?	Choose an item.
What's the extent of unsupported systems and applications in the applicant's network?	Choose an item.
How does the applicant maintain open port hygiene?	Choose an item.
How is Managed Service Provider (MSP) access to the applicant's network controlled?	Choose an item.
What best describes the applicant's patch management procedure?	Choose an item.
What's the extent of the applicant's security events monitoring and logging?	Choose an item.

2. RANSOMWARE RECOVERY INFORMATION

In the event of an infection of the applicant's core network and applications:	
a. How quickly would the applicant's business operations be impacted?	Choose an item.
b. Which percentage of the network could be recovered from a back-up?	Choose an item.
c. What's the applicant's network redundancy?	Choose an item.
d. What's the estimated number of hours to restore the applicant's business operations?	Choose an item.
What best describes the applicant's back-up procedure?	Choose an item.
How often are the applicant's critical systems and data files backed up?	Choose an item.

THE HARTFORD

s used

The Applicant hereby represents and warrants, after inquiry of the persons employed by the Applicant that a reasonable person would inquire of, that information contained in this application is true, accurate and complete, and that no material facts have been suppressed or misstated. The Applicant acknowledges a continuing obligation to report to the Insurer, as soon as practicable, any material changes in all such information, discovered after signing below and prior to issuance of the Policy, and acknowledges that the Insurer will have the right to withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance based upon such changes. Further, the Applicant understands and acknowledges that information requested in the renewal application is for underwriting purposes only and does not constitute notice to the Insurer under the Policy of a claim or potential claim.

Please check the box below to provide additional information to The Hartford (optional, but recommended for efficiency):

□ By checking here, the Applicant hereby authorizes the vendor(s) listed below to provide to The Hartford their recommendations and reports concerning the Applicant. The Hartford will keep any received recommendation or report confidential and it will become part of the insurance submission/application. **Time Tip: Save a copy of this supplement as you may be asked to provide it in the future.**

VENDOR(S): ePlus_(with respect to reports/recommendations based on BitSight security recommendations report).

FRAUD NOTICE: IN CERTAIN STATES, ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

Applicant (Company): ______ Title: ______

Authorized Representative
Print/Signature: ______ Date: ______

Agent/Broker Name: ______

2 The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.
20-65-554859 © January 2021 The Hartford

Zero Trust <> SASE

BUILDING OPERATIONAL MATURITY

IT NATION™ SECURE

EXPECTATIONS

CONNECTWISE

ALL USERS

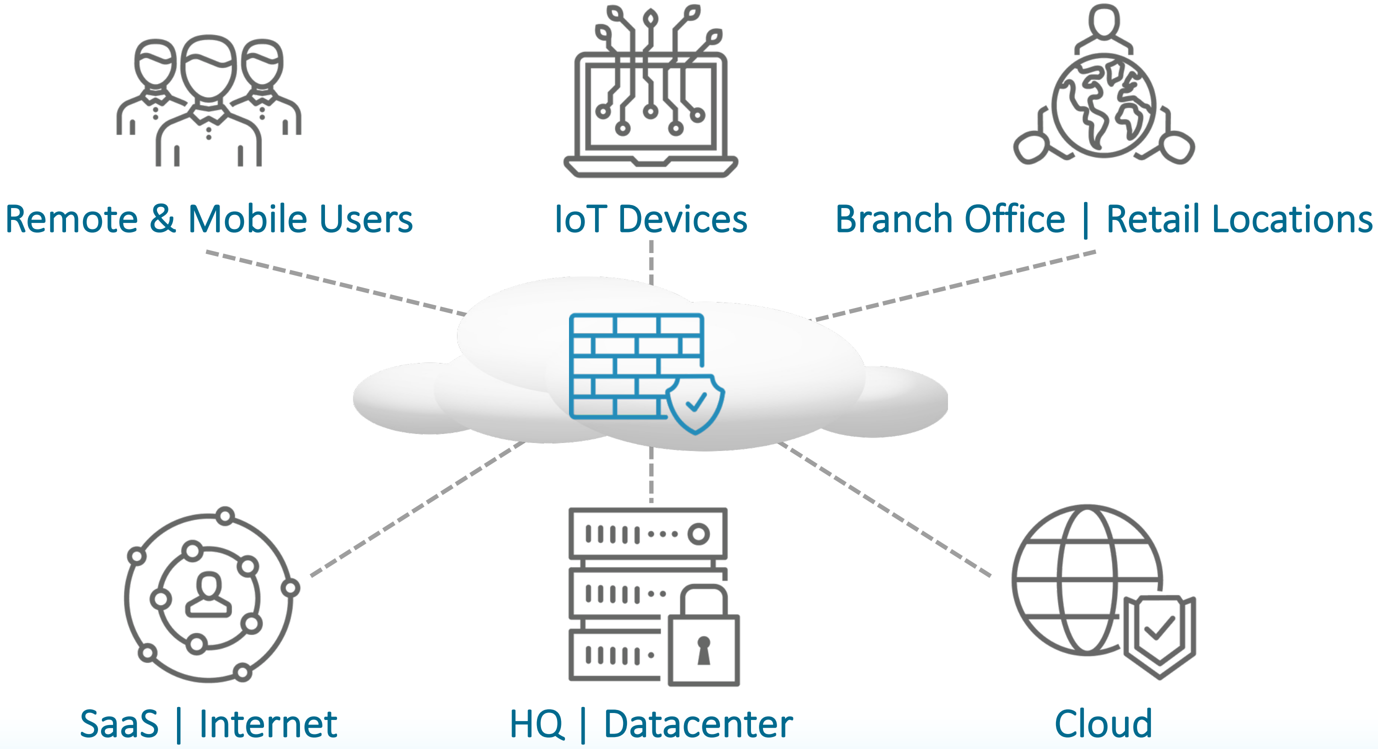
ANY DEVICE

ANY TIME

ANY CONNECTION
ANYWHERE IN THE WORLD

ANY DATA SOURCE

What does it mean to protect business data?



Remote & Mobile Users

IoT Devices

Branch Office | Retail Locations

SaaS | Internet

HQ | Datacenter

Cloud

Voice of your Peers — "Our Customers are Evolving"

- Clients are shifting to hybrid office models
- More work and data is being created and contained in the cloud
- Users pushing adoption of cloud-based tools—expanding the attack surface
- We're struggling with best way to secure clients' new cloud computing edge

> "The old HQ-based network & security edge is gone. We need to deliver secure, anywhere access at the edge of the cloud"

Secure Access Services Edge (SASE) by ConnectWise + Exium

Introduced by Gartner in 2018, SASE is a modern security framework for all endpoint, data resource, and network connection, without compromise

Unified

Security and Network Automation on a single cloud native platform, eliminating hardware clutter and service chaining.

Zero-trust & Identity Centric

The user is the center of policy creation, not the technology. Whether on or off corporate premises the focus shifts from traffic-flow-centric to **identity-centric** with granular access control.

Comprehensive

SASE **covers all network and user endpoints**:
Users, IoT devices, Locations & Application destinations.

SASE **service is real-time scalable and complete – no point products**
e.g., Internet security for users includes DNS, URL filtering, secure web gateway, threat prevention, and CASB etc. all tightly integrated.

CONNECTWISE

SASE by ConnectWise & Exium

What is SASE?
Instead of the security perimeter being entombed in a box at the data center edge, the perimeter is now everywhere an enterprise needs to be—a dynamically created, policy-based secure access service edge (Gartner)

What is Zero-Trust?
Zero trust ensures that every user and device granted access to an organization's resources is who or what they say they are and continuously verified—"If you can't trust anyone, it's best to trust no one."

EXIUM

Who is EXIUM?
Exium delivers a full suite of network security offerings from a unified platform that securely connect users, locations, and devices to applications in the cloud or private data centers. Exium makes security easier for users by delivering multiple layers of protection through a single client—all managed from an easy to use, single platform.

Too Many Tools

CONSOLIDATE & SIMPLIFY

your technology stack to increase operational efficiencies and improve margins

WHY THIS MATTERS

- Typical partner supports between 7-25 different tools
- Overlapping tools (AV, EDR, & firewalls)
- Product certs
- Firmware management & maintenance
- Software management & Updates
- Inability to correlate data between tools
- Crushes margins

Most MSPs Don’t Have Dedicated Cybersecurity Talent

CYBERSECURITY TALENT

is difficult to attract, grow, and retain in a highly competitive market where enterprise is targeting and hiring staff from MSPs

WHY THIS MATTERS

- Talent to manage these tools
- Difficult to attract and retain
- Continuing education is required
- Expensive (Tier 4 Engineer)
- 24x365 coverage model
- Turnover (single point of failure)

Cybersecurity Tech Stack | Industry POV Circa 2022

Standard for Most MSPs

- ✓ **Assessment tools**
- ✓ Anti-spam
- ✓ **GPO Management**
- ✓ **Anti-virus**
- ✓ **Patch management**
- ✓ **Web content filtering** (firewall)
- ✓ Managed Firewall (Hardware)
- ✓ IDS/IPS
- ✓ Encryption
- ✓ **Backups**

New Normal in 2022

- ❑ Password Manager
- ❑ **Security Awareness**
- ❑ **Endpoint D&R**
- ❑ Multi-factor Authentication
- ❑ **DNS Security**
- ❑ **Dark Web Monitoring**
- ❑ **SIEM**
- ❑ **Threat Intelligence / Sharing**
- ❑ **Risk Reporting**

2023 and Beyond

- ❑ Threat management
- ❑ Compliance reporting
- ❑ Continuous Vulnerability Scanning
- ❑ Mobile Device Security
- ❑ Application Whitelisting
- ❑ Zero Trust / SASE
- ❑ Identity & Access Management
- ❑ Privileged Access Management
- ❑ Data Loss Prevention (DLP)

2023 & Beyond

Email Security by ConnectWise & Proofpoint

Essentials

- ✓ Assessment tools
- ✓ **EDR/MDR ~~Anti-virus~~**
- ✓ Patch management
- ✓ Security Awareness
- ✓ Phishing Simulation
- ✓ Dark Web Monitoring

SASE by ConnectWise & Exium

- ✓ Web content filtering
- ✓ DNS Security
- ✓ IDS / IPS
- ✓ Cloud Access Security Broker (CASB)
- ✓ Data Loss Prevention (DLP)
- ✓ *Mobile Device Security*
- ✓ Virtual Private Network (VPN)
- ✓ Zero Trust Network Access
- ✓ Cloud Delivered Virtual Firewall

Other SASE Benefits

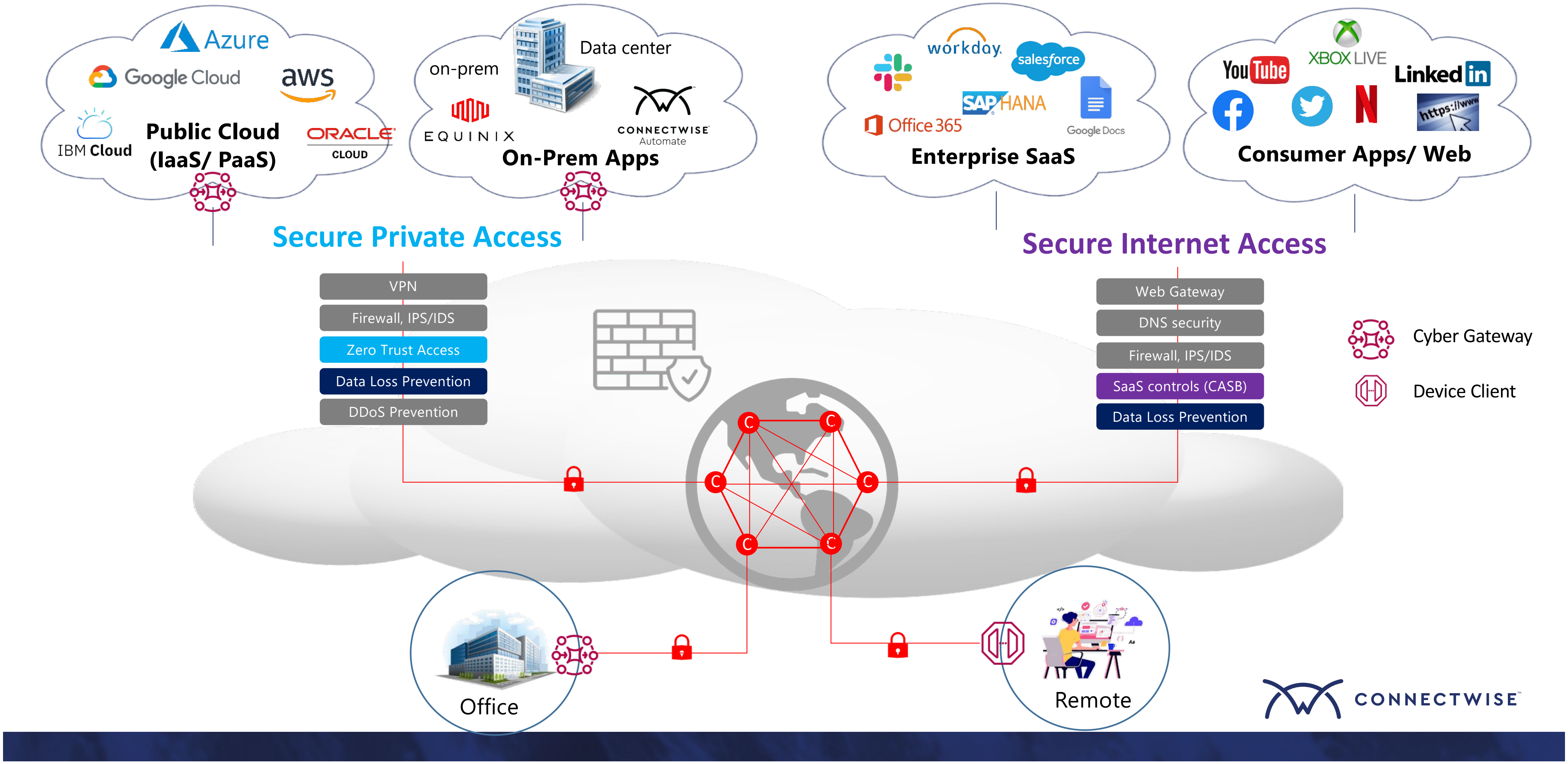
- ✓ MFA / SSO
- ✓ Encryption
- ✓ Identity & Access Management
- ✓ Privileged Access Management
- ✓ Compliance & Risk Reporting

ConnectWise SIEM

- □ SIEM
  (With or Without SOC)
- □ Threat hunting
- □ Threat management
- □ Threat intelligence

Cloud and Onsite Backups

SASE | A New Frontier for MSPs



Public Cloud (IaaS/ PaaS)

On-Prem Apps

Enterprise SaaS

Consumer Apps/ Web

Secure Private Access

- VPN
- Firewall, IPS/IDS
- Zero Trust Access
- Data Loss Prevention
- DDoS Prevention

Secure Internet Access

- Web Gateway
- DNS security
- Firewall, IPS/IDS
- SaaS controls (CASB)
- Data Loss Prevention

Cyber Gateway

Device Client

Office

Remote

Operational Efficiency | SASE by ConnectWise & Exium

CONSOLIDATE & SIMPLIFY

means reducing the number of tools your team manages and improves security, thus maximizing margin and reducing stress

CYBERSECURITY TALENT

is still important, but the impact of a key engineer leaving is minimized with simplified tools that are easier for all to manage

SASE by ConnectWise & Exium

ADD
ZERO-TRUST

CONSOLIDATE
TOOLS

REMOVE
COMPLEXITY

IMPROVE
MARGINS

SINGLE CONSOLE
SINGLE POLICY
SINGLE AGENT

CONNECTWISE™

&

EXIUM

Fully integrated cloud-native
security & networking platform

Gain Operational Efficiencies

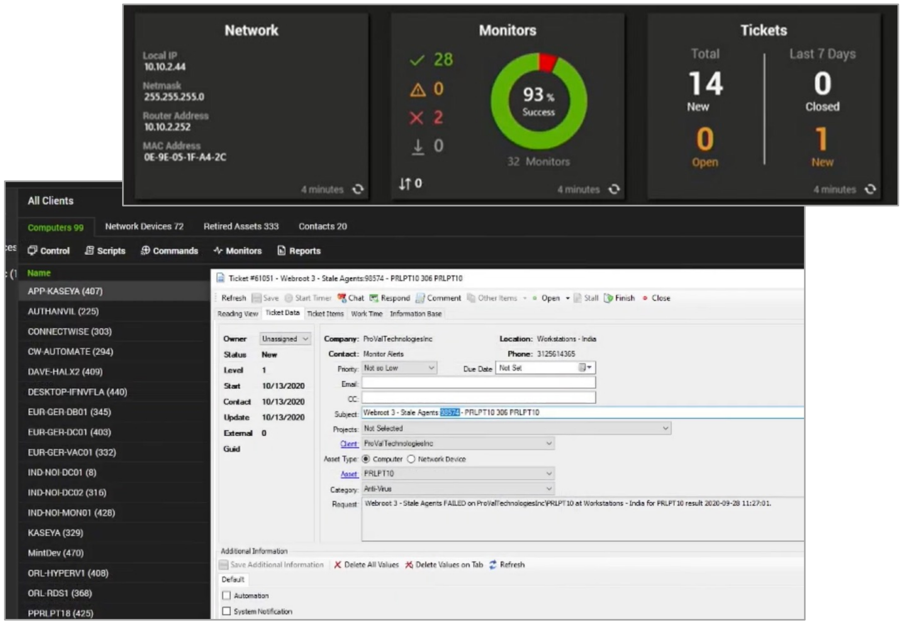
Exium and ConnectWise Integrations

Ordering, Billing, Operational Automation

EXIUM

CONNECTWISE® Automate

- Alerts
- Ticket Creation
- Auto Remediation
- Troubleshooting
- Silent agent deployment



Network

Local IP
10.10.2.44

Netmask
255.255.255.0

Router Address
10.10.2.252

MAC Address
0E-9E-05-1F-A4-2C

Monitors

✓ 28
⚠ 0
✗ 2
↓ 0
↓↑ 0

93 % Success

32 Monitors

Tickets

Total	Last 7 Days
14 New	0 Closed
0 Open	1 New

Computers 99 | Network Devices 72 | Retired Assets 333 | Contacts 20

Name
- APP-KASEYA (407)
- AUTHANVIL (225)
- CONNECTWISE (303)
- CW-AUTOMATE (294)
- DAVE-HALX2 (409)
- DESKTOP-IFNVFLA (440)
- EUR-GER-DB01 (345)
- EUR-GER-DC01 (403)
- EUR-GER-VAC01 (332)
- IND-NOI-DC01 (8)
- IND-NOI-DC02 (316)
- IND-NOI-MON01 (428)
- KASEYA (329)
- MintDev (470)
- ORL-HYPERV1 (408)
- ORL-RDS1 (368)
- PPRLPT18 (425)

Ticket #61051 - Webroot 3 - Stale Agents:98574 - PRLPT10 306 PRLPT10

Owner: Unassigned
Status: New
Level: 1
Start: 10/13/2020
Contact: 10/13/2020
Update: 10/13/2020
External: 0
Guid:

Company: ProValTechnologiesInc
Location: Workstations - India
Contact: Monitor Alerts
Phone: 3125614365
Priority: Not so Low
Due Date: Not Set
Email:
CC:
Subject: Webroot 3 - Stale Agents 98574 - PRLPT10 306 PRLPT10
Projects: Not Selected
Client: ProValTechnologiesInc
Asset Type: ● Computer ○ Network Device
Asset: PRLPT10
Category: Anti-Virus
Request: Webroot 3 - Stale Agents FAILED on ProValTechnologiesInc\PRLPT10 at Workstations - India for PRLPT10 result 2020-09-28 11:27:01.

□ Automation
□ System Notification

ConnectWise Cybersecurity

CONNECTWISE™

ConnectWise Cybersecurity

IT NATION™ SECURE

ConnectWise Cybersecurity

Prevented 6 million MSP attacks over the past year

Our 180 analyst strong SOC reviews over 1.3 million events per second across the MSP landscape

Protecting over 100,000 SMBs and 4 million devices

Industry's most profitable MSPs (17% more profitable)

> 500 unique threat detections across the MSP industry

Cyber Research Unit

Dedicated research team focused completely on MSP threat landscape

ASIO

Industry's only purpose-built platform across BMS, UMM, and Security

Products & Services

MSP tailored cybersecurity solutions and SOC services

Ecosystem

Comprehensive set of products and services covering all MSP relevant security solutions

Partner Program

Award winning partner program supporting your Cybersecurity and BCDR businesses

ConnectWise Cybersecurity Management

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

Identify & Resolve Vulnerabilities

Risk Assessment
Pre-sales tool for endpoint risks & vulnerabilities assessment, including dark web exposure

Vulnerability Management
Continuous endpoint scanning for vulnerability prioritization and management

Identify Assessment
NIST CSF framework-based assessment questionnaire

Secure & Streamline Access

MFA / SSO
Endpoint and application protection through MFA/SSO and Elevated Access

Protect Endpoints & Apps On-Prem/Cloud

EDR
Monitor endpoints to detect, contain & respond to malicious activity

MDR
EDR coupled with 24/7 ConnectWise SOC monitoring & response

SaaS Security
SaaS application monitoring coupled with 24/7 ConnectWise SOC monitoring & response

SASE

Secure Internet Access
Protect endpoints when connecting to networks, Web & SaaS apps

Secure Private Access
Zero-trust network & cloud access for on-prem & remote users

Collect & Analyze Log Data

SIEM
Centralized log collection, analysis, & compliance reporting

Co-Managed SIEM
SIEM solution coupled with 24/7 ConnectWise SOC monitoring & response

Respond & Remediate Cyber Incidents

Incident Response Service
Retainer & on-demand-based 24/7 IR services to respond to worst-case security incidents

Business Continuity & Data Recovery
Backup and recovery services

Co-Managed BCDR
Backup and recovery services coupled with 24/7 ConnectWise NOC management

Compliance & Certification

Get certified against industry regulations, such as SOC, PCI, CMMC, IT security standards like NIST and ISO, and develop plans for security compliance aligned to frameworks like MSP Trustmark.

Cyber Research Unit
ConnectWise SOC
Partner Program
Ecosystem Solutions
IT Nation | Education

#ITNation

Action Items

IT NATION™ SECURE

CONNECTWISE™

CONNECTWISE

CONNECTWISE GUIDE

So, You Want to Start a Cybersecurity Practice

THE ULTIMATE OPERATIONS GUIDE FOR MSP CYBERSECURITY

Are you looking to start or advance your cybersecurity practice?

Get the ultimate operations guide for MSPs

2023 MSP Threat Report

The latest intelligence, insights, and predictions from the ConnectWise Cyber Research Unit (CRU)

- Major MSP-focused hacks in 2022
- Emerging and continuing cyberattack trends
- Top ransomware methods of threat actors
- Action items for MSPs in 2023

Read the Full Study

FORRESTER

The Partner Opportunity For ConnectWise Cybersecurity Management

A Total Economic Impact™ Partner Opportunity Analysis

FEBRUARY 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY CONNECTWISE

Join Today

CONNECTWISE Partner Program

For ConnectWise partners

Scan the QR code to access sales and marketing tools in the Partner Portal

Questions & Next Steps

Learn more about SASE & Zero Trust

www.connectwise.com/sase

www.exium.net

CONNECTWISE™

Join the Partner Program to access everything you need to build, launch, and grow your practice!

www.connectwise.com/partnerprogram

Attend an IT Nation event near you!

www.connectwise.com/theitnation

Don't forget to fill out your

SESSION SURVEY