# TABLE OF CONTENTS

- From the Desk of Tracy Holtz ................................................................. 3
- We Spy Some New SPI Tool 2.0 Updates .................................................. 4
- The Passage Program is Now Available ..................................................... 5
- Professional Services for the Expanding Threatscape ............................... 7
- Top Security Resources and Thought Leadership for 2022! ......................... 10
- Join the Cybersecurity Fight With CompTIA ............................................. 12
- Follow the Data: Finding Adjacent Sales Opportunities in Your Customer Base .......................... 14
- How to Protect Business Systems With the Right Cloud Security .......... 16
- MSP Corner: 8 Lessons Learned From the Nextgen + MSP Conference .... 18
- Vendor Spotlight: Introducing Our Newest Vendor, Ciena! ..................... 22
- The Holtz Story Podcast ........................................................................... 24
- Listen to the Latest 30 Minutes With a Hacker Episodes! ......................... 26
- Digital Security Practice Builder Takes on MSP .................................... 27

Navigate the Journey to
Better Cybersecurity with ConnectWise

Tools and tactics you used in the past won’t be enough to keep today’s cyberthreats at bay. Continuing to keep the status quo will make things worse in the future. ConnectWise offers software to bring your cybersecurity up to speed. Build a profitable cybersecurity practice by upgrading your offerings with ConnectWise solutions.

**ConnectWise Identify**
Managing security is all about knowing and mitigating risks. Based on the globally adopted NIST Cybersecurity Framework, ConnectWise Identify enables you to proactively pinpoint critical risks that leave your clients vulnerable to cybersecurity incidents. Visit ConnectWise.com/IdentifyTrial-TechData to start your free trial today!

**Perch Co-Managed Threat Detection**
Prevention alone can’t stop all threats. Perch helps you detect what you can’t stop with co-managed threat detection and response. Leveraging the Perch SOC and the Perch application means you can add staff—and expertise—without adding headcount.

Contact Tech Data to learn more about ConnectWise Solutions
**Email:** ConnectWiseTD@techdata.com
FROM THE DESK OF TRACY HOLTZ

Tracy Holtz, Vice President, Security Solutions, Americas, Tech Data

Welcome to 2022! As we look back at 2021, it was another exciting year for Tech Data with the merger being finalized and our security business delivering strong year-over-year growth. 2021 proved to be another year of record cyberattacks and threats – with the shift from employees solely working from home to companies moving to hybrid work environments or returning to office. Another area attack vectors increased was around the volume of internet of things (IoT) expansion in 2021.

As I reflect on all the challenges, the effects of the SolarWinds attack, Log4j, and supply chain attacks such as the Colonial Pipeline compromise were the most noteworthy. The continued growth of ransomware created mainstream headlines throughout 2021 too. Modern ransomware attacks appear to circumvent traditional cyber protection, which creates opportunity for all of us to identify new risk barriers.

My projection for 2022 is the number of threats will continue to reach profound rates well above 2021 attacks, with AI taking priority to defend and protect against threats. Remote work IT infrastructure will be top priority for a company's security refresh and business upgrade budgets as well.

At Tech Data, we will continue to focus on bringing new technologies, services, and enablement for your security business. I can't thank you enough for your partnership and look forward to an amazing 2022 together!

All my best,

Tracy
WE SPY SOME NEW SPI TOOL 2.0 UPDATES

In December, we launched the new 2.0 version of our popular Solutions Product Inventory (SPI) Tool. This is a global resource our partners can leverage to help them recommend solutions that solve their customer’s IT security challenges. The tool was originally launched in 2018 before being updated as an online, web-based tool in 2020. This new upgrade to the 2.0 version is significant, providing:

- **Country specific contact information** to get questions answered and assist our global partners in providing products and services to customers.
- **Improved searchability** throughout the tool.
- **Improved user interface.**
- **Mobile friendly** making it easy to search from a smartphone or tablet.
- **Various multi-vendor solutions** developed by us in partnership with our vendors.

What’s Next?

With the merger of SYNNEX and Tech Data, partners can expect several more updates in 2022, including:

- In the first quarter of 2022, all legacy SYNNEX vendors will be integrated into the tool – more than doubling the security vendors our partners can leverage.
- The tool will be expanding its information catalog to cover solutions in IoT as well as Cloud. These additional areas will be targeted for the second quarter of 2022.
“Analysts estimate that by 2025, roughly 3.5 million global cybersecurity jobs will be unfilled.”

– Cybersecurity Jobs Report 2021, Cybersecurity Ventures

The increasing threatscape has created a significant market demand for cybersecurity personnel. So why are there so many job vacancies? Employers cite two main reasons: a hands-on skills gap with existing cybersecurity applicants and a limited pool of qualified personnel, which has created a demand gap between job requirements and responsibilities.

Additionally, employers often have an unrealistic expectation that graduates from cybersecurity programs will be fully qualified, with entry-level job postings requiring 1-2 years of work experience or asking for a specific number of years’ experience in certain skills or programs that have not even existed for the duration of the request.

How do you find job-ready candidates for security positions within your organization? Delivered through the Cyber Range, the Passage Program is a new professional service designed to bridge the skills gap for upcoming and established cybersecurity professionals, providing job readiness skillsets for:

• Individuals entering the field of cybersecurity, through the Placement Initiative.
• Existing cybersecurity personnel, through the Upskill Initiative.

The Placement Initiative relieves the financial and time burden of finding job-ready personnel for your organization. This initiative supports new cybersecurity talent through job-readiness training and hands-on skills development. Tech Data partners looking to hire qualified and job-ready candidates for internal cybersecurity roles should reach out to the Passage Program team.

Many organizations find it increasingly difficult to develop newly hired talent and retain tenured personnel while managing the requirements of day-to-day security operations. The Upskill Initiative is designed to develop participants in their current job role by providing the knowledge, resources and skills needed to succeed. As a Tech Data partner, you can utilize this professional service to develop your own internal security operations center (SOC), security assessment teams or resell this experience to end-user customers with internal security practices.

How does the Passage Program develop qualified individuals? While not an accrediting body, the Passage Program's Placement Initiative and Upskill Initiative develop today's cybersecurity professionals through hands-on experience, professional consulting and job-readiness assessments. Both initiatives focus on critical, entry-level cybersecurity jobs and are focused on delivering the cybersecurity professionals needed in today's workplace.

SOC Analyst 1 / Tier 1 Analyst
The SOC Analyst 1 is a critical job in the defensive cybersecurity arena. A core member of the SOC, the SOC Analyst 1 is responsible for the monitoring and investigation of security alerts and incidents.

The Passage Program will provide job-readiness and skills development through training and assessments on the following topics:

• Data search procedures
• Fundamentals of Windows
• Identification and recognition of vulnerabilities
THE PASSAGE PROGRAM IS NOW AVAILABLE CONTINUED

- Interpretation of collected information and logs
- Malware identification
- Report writing
- Utilization of protocol analyzers
- Reconnaissance and information gathering
- Remediation guidance
- Report writing
- Vulnerability analysis

Junior Penetration Tester

A Junior Penetration Tester is considered the primary entry role in offensive cybersecurity. Junior Penetration Testers are responsible for the reconnaissance, enumeration, analysis and reporting of security vulnerabilities.

The Passage Program will provide job-readiness and skills development through training and assessments on the following topics:

- Enumeration
- Introduction to exploitation
- Post-exploitation and engagement clean up
- Pre-engagement analysis
- Remediation guidance
- Vulnerability analysis

Overall, the Cyber Range Passage Program helps partners bridge the cybersecurity skills gap. By utilizing the Passage Program Placement Initiative, partners can expand their internal security departments and eliminate the constraints of onboarding new hires. Additionally, partners will have the confidence that they're hiring qualified and job-ready candidates. For partners looking to develop their existing cybersecurity professionals or resell the service to their customers, the Passage Program Upskill Initiative can support this need.

If you are interested in learning more about the Passage Program, please visit our website or email us at securityservices@techdata.com.
The threatscape continues to grow as bad actors evolve their strategies, targeting the critical systems of businesses of all sizes. Tech Data offers very effective and specialized security services that your customers need to keep their companies safe from these cyber threats.

Our security offerings are intended for our partners to sell to their customers. These offerings address a range of unique cybersecurity needs. Partners can grow their security practice through these professional services while driving higher-margin solutions and expanding their customer portfolio.

**Assessment Services**

Tech Data’s Assessment Services identify security weaknesses and vulnerabilities with clear recommendations for your customer. From these services, partners can build a roadmap to deliver required products and services chosen specifically for customers.

- **Penetration Testing**: Our engineers can demonstrate the ways your customers’ data may be at risk and identify vulnerabilities that should be addressed immediately.

- **Vulnerability Assessments**: These assessments identify common misconfigurations that attackers exploit. Vulnerabilities are evaluated and scored based on their prioritization and likelihood of being exploited.

- **Security Maturity Assessment**: We’ll help you reveal potential flaws in your customer’s infrastructure and compile a report for you to give to them with a summary of events and a customized action plan.

**Compliance and Implementation Services**

We can help you deliver compliance gap assessments that encompasses governance, risk and compliance services across many of the industry-wide regulatory companies. This includes the Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), Payment Card Industry Data Security Standard (PCI-DSS), National Institute of Standards and Technology (NIST) 800-171, International Organization for Standardization (ISO) 270001, North American Electric Reliability Corporation critical infrastructure protection (NERC-CIP), Service Organization Control (SOC) 1&2, General Data Protection Regulation (GDPR) and more. For a complete list of regulatory compliance services we offer, view our data sheet.

**Incident Response Services**

In today’s information climate, you must be prepared to counter a cyberattack before damage is caused. However, if you’re just launching your cybersecurity practice or want to build on an existing practice, Tech Data can help with our Incident Response services.

- **Incident Response Plan**: A detailed Incident Response Plan describes the steps every team member must take to respond to an incident alert. Our security consultants can help create or build a customized Incident Response Plan, tailored specifically to your customer’s business, that can help their IT team take action and respond to cyber threats that may impact their business.

- **Incident Response Readiness Review**: Having an Incident Response (IR) Plan doesn’t mean your customer’s IT team is fully prepared to handle any type of cyber incident that may impact your customer’s business. How often do they test their IR Plan? Is their IR Plan updated regularly to incorporate the changes in their environment? Our security consultants review your customer’s IR Plans and make recommendations to required remediation steps to improve your customer’s security posture. If your customer hasn’t performed an incident response readiness review in more than a year, this is a great place to start.

- **Incident Response Emergency Service**: Despite the best preparation and planning, breaches can happen. Our IR Emergency responders will provide rapid remediation assistance with engagement able to begin within a few hours of signing a statement of work.

**Managed Security Services**

Managed security service providers (MSSPs) can help your customers gain security expertise while reducing the workload of their in-house IT team. We offer a range of managed security services for partners to leverage.

- **SOC-as-a-Service (SOCAaS)**: Security Operations Center (SOC)-as-a-Service provides organizations with a cybersecurity bench of experts dedicated to fully
monitoring threats across an organization, which are then analyzed and addressed with the best solution for the organization. Identified and confirmed cyber threats are immediately escalated to your customer via alerts, which contain all the details of the threat and the recommended remediation steps to block or contain the identified threat.

- **Firewall:** Managed firewall services allow companies to focus on their core business instead of dedicating time to the management and upgrades of a firewall. This service includes Add, Move, Delete, and Change requests, along with updating and maintaining your customer’s firewalls.

- **ISAO Threat Feed:** Information Sharing and Analysis Organizations (ISAO) allow companies, local governments, and security professionals to form communities that collaborate, share intelligence, and deliver training and conferences to take place under the veil of mutual non-disclosure agreements.

If you’re interested in learning more about any of our professional services, please reach out to your security sales rep or email us at securityservices@techdata.

---

Symantec Integrated Cyber Defense

All the essential security solutions working together to protect your business.

Learn More at: https://shop.techdata.com/vendorpartners/symantec
DON’T PAY THE RANSOM.

Ransomware protection can be as easy as 1-2-3. Secure your email, web apps, and data with Barracuda.

For more information, contact barracuda@techdata.com
# TOP SECURITY RESOURCES AND THOUGHT LEADERSHIP FOR 2022!

Our featured resources dive into industry trends and highlight how Tech Data can help partners offer technologies, services and solutions to their customers. Our resource content is updated frequently, so be sure to bookmark the Resources page of our Security Solutions site.

Here are a handful of our latest digital assets and resources:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Essentials Series</td>
<td>The Cyber Essentials Series serves as an introduction to the tools and resources that can be utilized at the Cyber Range. These free, instructor-led courses provide participants with the cybersecurity knowledge needed to better understand system vulnerabilities and how to strengthen cybersecurity postures.</td>
</tr>
<tr>
<td>Cybersecurity Decyphered Videos</td>
<td>Global Vice President of Cybersecurity, Alex Ryals, shares his unique perspectives on the cybersecurity market through his YouTube channel, Cybersecurity Decyphered.</td>
</tr>
<tr>
<td>CyberTalk Webinar Series</td>
<td>#TDCyberTalk is a webinar series from our Security Solutions Business Development team. This group is a vendor agnostic team of security experts that provide a unique point of view on all-things security technology. The goal of this webinar series is to help you create new revenue streams for your business.</td>
</tr>
<tr>
<td>Cyber Range eBook</td>
<td>This Cyber Range e-book will showcase why you need a resource that lets your team practice the skills needed to combat network exploits in the real world.</td>
</tr>
<tr>
<td>How Zero Trust Helps Instill “Real” Trust</td>
<td>Now’s the precise time to take a new look at your customer’s legacy security infrastructure and multiple point products to help them re-think their security strategy.</td>
</tr>
<tr>
<td>Secure Access Service Edge: Breaking It Down</td>
<td>Follow us on social media to stay up to date on events, resources and news!</td>
</tr>
</tbody>
</table>

Follow us on social media to stay up to date on events, resources and news!
SonicWall Delivers Choice, Flexibility as Part of Cloud Evolution

SonicWall's growing virtual, cloud and hybrid offerings leverage the best of the company's Boundless Cybersecurity approach to provide deployment choices to the customer while solving real-world use cases faced by SMBs, enterprises, governments and MSSPs.

Every day, SonicWall secures real-world hybrid environments using a cohesive mix of virtual, cloud and on-premises offerings, including SonicWall NSv virtual firewalls, Cloud Edge Secure Access zero-trust security, Cloud App Security to protect SaaS applications and appliance-free SMA virtual private networks (VPN).

For more information on how SonicWall can deliver a comprehensive cloud solution for your business, please email SonicWall@TechData.com

TREND MICRO™ WORRY-FREE™ WITH CO-MANAGED XDR

MSPs, rest easy. Security posture across your customer base is monitored 24/7 by security and threat intelligence experts.

• Increase protection for your customers
• Expand your business
• Lower operating costs
• FREE 75-user NFR license of Trend Micro™ Worry-Free™ XDR

Trend Micro Team
trendmicro@techdata.com
(727) 539-7429 ext. 5545035

For more information, please email trendmicro@techdata.com or (727) 539-7429 ext. 5545035.
JOIN THE CYBERSECURITY FIGHT WITH COMPTIA

CompTIA members get exclusive access to some of the tech industry’s most valuable resources in the fight against cybercriminals — including pertinent insights from CompTIA research, content, programs, and guidelines from the Cybersecurity Advisory Council and Cybersecurity Community. CompTIA members can also expect the latest threat intelligence and remediation advice from the CompTIA Information Sharing and Analysis Organization (ISAO). These resources have all been developed to help members better secure themselves as well as their customers’ businesses.

Here’s a look at some of CompTIA’s most recent work:

- **2021 MSP Trends in Cybersecurity** Learn the trends and cybersecurity principles guiding MSPs today, so you can stay ahead of the curve.
- **A CEO’s Guide to Addressing Cybersecurity Concerns** Make sure your customer is asking his or her team the right questions for a better understanding of their organization’s cyber posture.
- **State of Cybersecurity 2021** The latest cyber research report from CompTIA explores cybersecurity policy, processes, people and products.
- **The Cost of a Cybersecurity Breach** Today’s cyber stats don’t paint a pretty picture. It’s time to convince your SMB customers to join the fight against cybercriminals.
- **Information Security Risk Assessment Guide** Talk to your customers about why a security risk assessment is critical to their protection — and yours.

Click here for more information on membership opportunities

INTRODUCING CYBERShark 2.0!

**CYBERShark 2.0 is the ONLY SOCaaS that includes EDR and SOAR at NO ADDITIONAL COST!**

30 day **FREE POC’S for all your clients!**

VISIT WWW.CYBERSHARKINC.COM OR CALL (800)988-8599 FOR MORE INFORMATION.
Endpoint Security
Extensible, Cloud-based
EPP and EDR

Essential technology for your
customers’ zero-trust environments.

Contact us to learn more:
Phone: 800-237-8931 ext. 5545033 *   Email: sewatchguard@techdata.com
Customer demands are driving organizations to digitally transform, and converging technology trends between analytics, AI, IoT and cloud, have been underway for some time with data at the center of it all. The pandemic has only accelerated these trends and forced business leaders who had not already done so, to formalize their digital transformation (DX) and data initiatives.

Incident Response Services

A recent Forrester study shows that data-driven companies are 58% more likely to beat revenue goals than non-data-driven companies and 162% more likely to significantly outperform laggards. However, in an increasingly online world with more people, applications and connected things generating staggering amounts of data, implementing processes and streamlined procedures that foster cross-company data sharing requires investment and commitment from business leaders and teams across the organization.

According to IDC, 32% of new technology investments will be driven by DX. If your customer has a formal DX initiative underway, it’s a good place to start inquiring about their goals and who across the organization establishes their data policies.

Data governance best practices include the orchestration of people, processes and technology to enable an organization to leverage their data as a strategic asset. Ensuring one’s data is secure throughout its life cycle is essential. Effective data governance is especially crucial for sensitive data, such as protected health information and personally identifiable information that is subject to privacy regulations.

While it’s a challenge for clients to become a data-driven business, understanding where your customers are within their data maturity journey is the key to uncovering opportunities to help. Tech Data has built a data and IoT practice to serve partners who want to accelerate their client’s evolution along the data maturity journey.

This data journey requires simplification and expertise. We stress to our partners that they shouldn’t miss out on this opportunity to serve their clients regardless of where they are in their journey.

Analysts continue to project substantial growth and spend across all four areas of the journey. We’ve also wrapped our value stack around these stages to help you capture market opportunity. The Data & IoT consultants are part of the broader NextGen organization to ensure we look across emerging trends and vertical nuances. This allows us to assist our partners with successfully navigating today’s technology landscape and to solve for ecosystem complexities with next-gen solutions including cloud, data, IoT and security.

Our Data & IoT solutions consultants engage with our partner ecosystem in the areas of strategy definition, vendor enablement, marketing, aligned services and enablement via our award-winning Practice Builder. Our proprietary methodology shortens the process for channel partners to build data and IoT businesses by reducing resource build-out time and allowing for the quick realization of profits.

We also support value enablement and creation by helping our partners specialize in various areas of data and IoT by
providing credibility with our vertical expertise and programs. Our rich ecosystem of demand generation programs helps to identify the opportunity, delivering on those created opportunities by providing technical support and expertise along the sales journey.

To help reduce your risk, we have developed solutions, highlighted within our Use Case Solutions Catalog, targeted with business outcomes in mind that you can unleash on your clients. All delivered and managed via a cloud platform.

We want our partners to capture a piece of this multi-billion-dollar market opportunity. We welcome you to engage with us in a discussion on where your challenges are and how we can provide our value – all tailored to your needs and the needs of your clients.

We are standing at the ready to capture the data and IoT market opportunity together. Reach out to the IoT team at iot@techdata.com for more information.
HOW TO PROTECT BUSINESS SYSTEMS WITH THE RIGHT CLOUD SECURITY

By: Tracy Holtz, Vice President, Security Solutions, North America, Tech Data

Businesses are implementing new cloud applications at record paces, inviting the risk of security vulnerabilities and threats. Last year, malware was detected in 61% of apps originating in the cloud, including the most popular apps used by enterprises¹. Additionally, 98% of companies indicate they have experienced at least one cloud data breach in the last 18 months, up from 79% in 2020². With the overall security market expected to grow from an average 25.5% CAGR in 2022³, having the right resources in place can help you protect your customers’ business critical systems in the cloud.

As we kick off 2022, many organizations are implementing return to office (RTO) policies or a hybrid model with a balance of RTO and remote work. The shift back to the office is expected to accelerate the adoption of security frameworks such as Secure Access Server Edge (SASE), Security Orchestration, Automation and Response (SOAR), Security Information and Event Management (SIEM) and Extended/Endpoint Detection and Response (XDR/EDR). These market drivers can help you position and improve your security posture.

Tech Data staffs a team of experts with our dedicated cloud security sales team, who are a vendor agnostic, solutions-focused resource – and larger than any other distributor. We also have a team of highly skilled Solution Architects, who have a diverse knowledge of security technology and work closely with partners to recommend the right solutions and provide a true value-add to both the partner and their end user. We’ve also identified several vendors who are driving above-market growth within the Cloud. Included in this list are Fortinet, Trellix, Netskope, Palo Alto Networks, Ruckus, Trend Micro and Zscaler. We work closely with these vendor teams and others to identify and recommend the right solutions to our partners. Many of these solutions can be found on our Cloud Marketplaces, Stellr and StreamOne.

Our enablement tools are another resource for partners to use when working with their customers to recommend and deploy cloud solutions:

• Position new security solutions to your customers by leveraging our SPI (Solutions Product Inventory) Tool. The SPI Tool includes an easy to use keyword search as well as searchability by vendor, product, category, sub-category, MSP readiness, and geographic region.

• The Digital Security Practice Builder (DSPB) provides partners with an assessment of where and how they can drive greater security growth. The program is also dynamic – partners can enter at any time along their journey to receive relevant information.

• Our Cyber Range events provide a way to “touch and feel” cybersecurity, showing how crucial it is to invest appropriately to safeguard systems.

• MSP Evolve is a bi-annual, two-day event designed to provide interactive expertise, guidance and insight partners seek on marketing and sales tools and strategies for their managed service provider (MSP). This event is a cornerstone for partners wanting to grow their cloud security MSP business.

Keep an eye out for our upcoming webinar with Channel Pro that will cover cloud security and what partners should be doing for success. Please reach out to us at securityservices@techdata.com or https://techdata.com/security for additional information.

¹61% of Malware Delivered via Cloud Apps: Report - darkreading.com
²Ermetic Reports Nearly 100% of Companies Experienced a Cloud Data Breach in Past 18 Months - Ermetic
³The Cloud Security Market is Expected to Reach $ 12.73 Billion by 2022 with CAGR of 25.5% - Bloomberg
SMBs: Avoid Being Yet Another Victim of Ransomware

As news headlines demonstrate, ransomware is on a rampage. SMBs face the same threats as everyone else and must be prepared. Having a plan and putting the right security in place means you can stop ransomware—even post-infection. But you need to be ready.

Go to the Fortinet vendor page to learn more at: https://www.techdata.com/vendorpartners/fortinet.
For many managed service providers (MSP), the search is constant to understand how others are finding success. Before the pandemic, many stakeholders at MSPs would glean how to improve performance by meeting with others in similar businesses. These conferences were unbelievably valuable, but these opportunities have dried up over the last year and a half.

Now, in-person gatherings and conferences are slowly starting to happen again. In October, I had the opportunity to attend the Channel Co NexGen conference held in Anaheim, CA. For most of the other attendees and myself, this was our first chance to get together in person since the pandemic. It was a wonderful experience and I could sense a huge need for the attendees to connect to others who are in the same collective boat of running an MSP. Each MSP is unique, but they are the same in many ways – all companies started for distinct reasons, yet they all wish to solve gaps in the marketplace. There were a handful of unique origin stories in which ownership of an MSP – via succession from one owner to another – happened unexpectedly and quickly, and each had incredibly unique challenges to overcome.

The overall theme of the conference was that MSPs are first in the business of customer service; customer service is just being performed by a company who happens to provide IT solutions.

Confucius famously said: “By three methods we may learn wisdom: first, by reflection, which is noblest; second, by imitation, which is easiest; and third, by experience, which is the bitterest.” I want to share a few items of interest to MSP stakeholders in the hopes of acquiring wisdom:

1. **Selling Excellent Service**
   To sell excellent services, we must remember that it’s important for your customers to understand that your service offering is really all about the “service” aspect. That might mean outlining the level of support and availability you will provide, or it might mean translating clearly what service terms mean in an agreement. Plus, if you have a history of accomplishment, show it off: put clients, partners and prospects at ease by discussing success stories and challenges you have overcome with other customers. This will establish you as an experienced solution provider in your field, which leads to peace of mind.

2. **Speak to Your Clients on a Deeper Level**
   Express to them how they can focus on other things or even relax knowing you will be on top of any security or technical issues before they become problems. Giving your clients peace of mind about technology so they can focus on other aspects of their businesses is a massive undertaking and part of the value proposition for your monthly service offering. Many MSPs have found that a quality remote monitoring and management (RMM) tool can help deliver peace of mind to clients. The ability to really understand and utilize your companies’ RMM will pay huge dividends for your business. You can proactively monitor your client’s network environment and provide alerts when things are wrong. You can also set up your remote management and monitoring to automatically resolve routine issues before your client even knows about them.

3. **Break Down the Numbers**
   Once you have provided the service with great execution and your customers have achieved a strong peace of mind, it’s critical that the numbers are explained in detail. It’s easier for most people to digest the cost when it’s presented in terms of monthly payments rather than an annual lump sum. Present the costs of your as-a-service offering in the context of the value and service levels you are delivering and provide the monthly total the customer can expect to be invoiced. There can be a fear of ‘profit guilt,’ where you are nervous to share with the customer that you are making money from the transaction. But anyone who has overcome this understands that it’s acceptable for clients to know that we are providing a service and we are in the business to make a profit. Of course, no one likes hidden fees, so make sure your monthly total is accurate to help establish trust and enable your customers to budget accurately for your service.

4. **Talk About the Results, Not Just the Technology**
   Sometimes, it is tempting to talk about all the bells and whistles of the technology, but what good is it
Are you part of a Supply Chain Attack? Are your customers at risk?

AREA 1 PROTECTS PARTNERS FOR FREE

Preemptive Cloud Email Security • 5 Minute Provisioning • Free Protection for Area 1 Partners • BEC Protection Fraud Protection • Ransomware Protection • Supply Chain Protection • Identify Most Attacked Users + Campaign Origin

Empower your team. Validate cyber defense readiness with RangeForce.

Upskill against real threats in action and learn critical cybersecurity skills with hands-on modules and team-based threat exercises.

Visit Tech Data Team at techdata.com to learn more.
MSP CORNER: 8 LESSONS LEARNED FROM THE NEXTGEN + MSP CONFERENCE CONTINUED

if it doesn’t solve underlying problems? In a sales conversation, do not sell technology, sell the benefits. Most of your customers do not understand business technology and do not have the time to figure it out themselves – they want to see actual results in their businesses. Sell business owners the ability to refocus on their core business and more easily achieve business goals.

Follow Up With a Definition of the Real Costs
Once you have shared the benefits and tangible results from the technology, it’s unbelievably valuable to highlight that the biggest cost of poorly functioning technology is what it costs in people and productivity. Paint a picture to reframe how your services would benefit the client and attach a value to it. Ask tough questions to help tip the balance for your client from the emotional, irrational fears that lead to “no,” towards the logical, rational decisions that lead to the sale.

Establish Yourself as the Trusted Vendor or Partner
If you work in a vertical market, you’re in a great position to sell yourself as a trusted vendor for their niche, which is a big part of your value. Clients want to simplify and focus on their businesses – technology is not their core mission, it’s only a tool. What should relying on you as their one and only vendor mean for your clients? It means they don’t need to worry about technology anymore. Explain the amount of time and energy you will invest to understand every piece of their business and how you will help them choose the best technology to support their business objectives. If issues come up, they only need to make one phone call.

Facilitate the Shift to the Cloud or as-a-service Offerings
Moving your business or your customers business from a rip-and-replace model to an as-a-service model is a challenging proposition. Make sure you have equipped your business to make this transition as smooth as possible for yourself, your business and your clients. You must believe in your own expertise and skills to make a convincing pitch to clients. Technology automation is the key to delivering efficient, profitable managed services. In the future, the most successful solution providers will offer clients more services and manage these services with fewer employees. This should be ingrained in your company culture.

Provide Security-Based Services
Many MSP’s are successfully acting upon this option and moving towards becoming a managed security service provider (MSSP). An MSSP is an external partner who manages and monitors cybersecurity solutions for an organization. Moving into the cloud/security realm might seem daunting at first, but we’re seeing this move is the natural evolution of many MSP companies. Managing more technology with fewer and fewer people is the inevitable path of technology solution providers. Wrapping an MSSP program into your catalog of services might be the ticket for continued robust growth for many years to come.

My hope is that this article will provide some ideas to help you move your business forward profitably!

The Tech Data Security team consists of more than 150+ associates including trained security practitioners, former MSP owners, and industry leaders. Reach out to MSPsecurity@techdata.com today to talk about how to grow your business.

Looking for an on-demand security curriculum to advance your security practice?
Visit Tech Data – Security Practice Builder to register today. Or searching for more solutions to onboard and provide to your customers? The SPI tool has you covered.
Why Trust Microsoft as Your Security Provider?
Microsoft has proven that they’re a trailblazer in IT that takes security seriously.

13 Billion malicious messages blocked in 2020.¹
12 Billion monitored and controlled cloud activities in 2019.²
300 Billion user activities profiled and analyzed over 2019.²

Microsoft 365 improves security and saves customers up to 52% by combining the latest security features under one simple tool:

Identity and Access Management
Threat Management
Information Protection
Unified Endpoint Management
Cloud Access Security Broker

Don’t wait – partner up with a 5-Time Gartner Magic Quadrant leader today!

Explore Microsoft Security

For more information, please reach out to the Microsoft Cloud Team at microsoft@techdata.com

In 2022, we will continue to build our vendor portfolio with new strategic capabilities. In this issue of Security Sentinel, we are excited to announce a new key vendor relationship that delivers cutting edge solutions focused on network automation.

**Ciena** is a networking systems, services and software company that helps their customers create the Adaptive Network™ in response to the constantly changing demands of their end users. By delivering best-in-class networking technology through high-touch consultative relationships, Ciena builds the world's most agile networks with automation, openness and scale.

Ciena knows how to navigate the most complex network virtualization strategies because they’ve done it. The Ciena Virtualized Edge Solution provides one of the most complete, open and proven approaches to navigate the most complex network virtualization strategies. The end goal of the Ciena Virtualized Edge Solution is to offer enterprises the ability to evolve and virtualize their network infrastructure rapidly and successfully, either directly on their own, or indirectly through a preferred service provider or a solution integrator.

We encourage all our partners to take a few minutes to get familiar with Ciena and the solutions they offer that can enhance your security portfolio so you can continue to provide comprehensive solutions to your clients. If you'd like to learn more, contact the team at cienaus@techdata.com.

---

**IBM Security Acquires ReaQta**

Europe's leading AI-based Endpoint Security Provider

**ReaQta Differentiation**

- Automated AI-driven threat detection
- Live-Hypervisor based monitoring
- One-shot learning system

For more information, contact the Tech Data IBM Security Solutions team at ibmsecuritysolutions@techdata.com
Security threats are more dynamic and sophisticated than ever. Static and siloed solutions are simply not enough to keep businesses protected. **Bring your security to life.**

**Trellix** is focused on delivering best in class protection leveraging FireEye and McAfee Enterprise's integrated portfolio. When your security learns and adapts at the speed of dynamic and malicious actors, tomorrow's threats become today's protection.

We call this *living security.*

Learn how Trellix can secure your customers at: [www.trellix.com](http://www.trellix.com)

---

**HARNESS THE POWER OF CYBER RESILIENCE**

Back up, train, protect, block and restore with Carbonite + Webroot. Companies need cyber resilience. Companies need Carbonite + Webroot.

Take full advantage of cross-selling opportunities between Carbonite + Webroot.

Our endpoint and network protection, security awareness training, data backup and disaster recovery solutions help keep businesses moving, no matter what.

---

"THE BACKUP BUNDLE"

- **Carbonite** Endpoint
  - Enterprise protection for the mobile workforce

- **Carbonite** Server
  - Backup and recovery for servers with optional cloud failover

- **Carbonite** Backup for Microsoft 365
  - Complete backup for the entire suite of Microsoft 365 productivity apps

"THE DATA MOBILITY BUNDLE"

- **Carbonite** Availability
  - Keep critical systems online, all the time.

- **Carbonite** Recover
  - Push-button failover for critical workloads hosted in our cloud

- **Carbonite** Migrate
  - Seamless, successful migration from any source to any target

"THE CYBERSECURITY BUNDLE"

- **Webroot** Business Endpoint Protection
  - Stronger and smarter business antivirus with cloud threat intelligence

- **Webroot** DNS Protection
  - Advanced DNS security and visibility into web usage policies

- **Webroot** Security Awareness Training
  - Ongoing cybersecurity education and training for end users

There are a million ways to package our cyber resilience solutions based on your customers needs. **Reach out to us to learn more.**

---

To learn more, please visit [http://tdcontent.techdata.com/techsolutions/security/Carbonite.aspx](http://tdcontent.techdata.com/techsolutions/security/Carbonite.aspx)

To purchase our products, please reach out to your Tech Data Team today at carbonite@techdata.com and webroot@techdata.com.
The Holtz Story podcast has launched more episodes! Hosted by Tracy Holtz, Vice President of Security Solutions in the Americas at Tech Data, she discusses current challenges and trends in cybersecurity with the industry’s leading tech experts.

Recent episodes of The Holtz Story include:

- **Building Security Using SASE and Zero Trust**
  - Sunil Choudrie
  - Product Marketing Lead, Data Loss Prevention and Email Broadcom Software

- **Protecting What’s Now and What’s Next**
  - Frank Lento
  - Managing Director, Global Security Sales Organization and Global Head of the Global Security Sales Partner
  - Cisco

- **Cloud-Based Cybersecurity Trends & Solutions**
  - HoJin Kim
  - Vice President of Worldwide Channels
  - Kayvon Sadeghi
  - Executive Director of Product Marketing
  - SonicWall

- **Protecting Your People, Data and Infrastructure With Zero Trust**
  - Paul Mezzera
  - Vice President of Strategy
  - Saviynt

- **IBM on Security**
  - William “Chip” Crane
  - Cybersecurity Executive Advisor, Public and Federal Markets
  - IBM

- **Evolution of Email Threats**
  - Nishant Taneja
  - Senior Director, Product Marketing
  - Barracuda

- **Ransomware**
  - Corey Nachreiner
  - Chief Security Officer
  - Watchguard

**Upcoming Episodes and How to Listen**
Future episodes are in the works, and will feature leaders from our Security vendor partners, including guests from ConnectWise and Trellix.

The Holtz Story podcast episodes are available on all major streaming outlets:

- [Spotify](https://open.spotify.com/show/5CZQsJhNvKyr7jTnEJjJ86)
- [Stitcher](https://www.stitcher.com/podcast/the-holtz-story)

You can also visit and bookmark [The Holtz Story podcast site](https://theholtzstory.com) to stay current on episodes. Please be sure to subscribe and share with your professional network!
#Ransomware
Are you protected?

Ransomware attacks are more frequent than ever*

Every 2 minutes
Beginning of 2016

Every 40 seconds
End of 2016

Every 14 seconds
End of 2019

Every 11 seconds
In 2021

Be ransomware resilient

Protect and secure client nodes.

Manage security patches and alerts.

Ensure critical systems protection for the backup server.

Test your disaster recovery plan.

Recover from data spillage.

Perform frequent security audits, reviews and training.

Ready to build your own robust ransomware resiliency plan?

Contact your Veritas representatives on our website

LISTEN IN TO THE LATEST 30 MINUTES WITH A HACKER EPISODES!

Have you listened to our 30 Minutes with a Hacker podcast? The Tech Data Security Solutions team launches monthly episodes to dive deep into relevant cybersecurity topics. Podcast episodes focus on recent large-scale ransomware attacks, emerging security technologies and perspectives on cybersecurity trends.

Recent episodes of 30 Minutes with a Hacker discuss security orchestration, the importance of vulnerability assessments and penetration testing, proposed legislation around organizations ‘hacking back’ and deconstructing cyberattacks that made national news, including the Colonial Pipeline breach.

The topics discussed in 30 Minutes with a Hacker pinpoint the changing cybersecurity threatscape. You can listen to episodes and access other cybersecurity resources on our Cyber Range website.

Meet The Hosts

Brett Scott is the Director of the Tech Data Cyber Range and a well-known ethical hacker. As the founder of the National Cyber Warfare Foundation and the Arizona Cyber Warfare Range, he is dedicated to helping advance cybersecurity globally.

Alex Ryals is the Global Vice President of Security Solutions at Tech Data. He’s a security industry leader dedicated to channel security growth. With more than 20 years of experience in deeply technical and analytical positions, he innovates to deliver the best cybersecurity solutions to the channel.

Jade Witte is a Cybersecurity Solutions Development Manager at Tech Data and has more than 25 years of industry experience. He's passionate about the enormous growth and impact of cybercrime, and believes effective cybersecurity is more critical to businesses today than ever before.
### MSP Course

Becoming a Managed Services Provider (MSP) can deliver cash flow stabilization for your organization if it is set up correctly. Rather than living through many common mistakes, we have developed course content for you to leverage from those that have built successful MSP businesses and have shared their insights to remove much of the risk. Even if you are established as an MSP, you should find some useful nuggets to help take your business to the next level.

The digitization of the Tech Data proprietary and award-winning Security Practice Builder program continues to evolve. With more and more businesses moving toward subscription-based models, the time to adopt managed service provider (MSP) solutions is now. Becoming an MSP positions your business to become the trusted advisor for your clients, deepening your relationship and exponentially increasing recurring revenue streams. In response to this demand, we have created a dedicated MSP course.

Unsure where to start? The new MSP strategy videos will guide you. New content launched earlier this month includes strategy videos designed to cover all aspects to consider when planning, building, and executing your MSP business.

Chris DesRosiers, Director of Security Solutions Business Development, and Paul Roatta, Security Strategic Enterprise Consultant, dive into MSP strategy in two videos: “Planning an MSP Business” and “Building an MSP Business.” Both Chris and Paul are uniquely positioned to advise on MSP strategy. Chris has built an $18 million MSP business within a VAR during his career and Paul was the owner of a leading MSP for many years. Stay tuned for video three coming soon to round out the series: “Executing Your MSP Business.”

Exploring which vendors to add to your portfolio? Hear firsthand from the following vendors on their MSP solutions: Check Point, Fluency, Fortinet, and Tripwire. And with more content being added weekly, be sure to bookmark the tool for reference when deciding who to bring on next.

Interested in learning more about cloud security? Today’s market is moving away from on-premises hardware and software. In our Cloud Security Primer video, Paul Roatta discusses cloud security responsibilities, challenges, solutions, and zero trust architecture. Learn how to capitalize on this growing market and increase your monthly recurring revenue.

Digital Security Practice Builder is an on-demand and flexible curriculum. Visit [https://practicebuilder.techdata.com/security/](https://practicebuilder.techdata.com/security/) to register and gain access today.
FLEXIBLE PAYMENT SOLUTIONS TO HELP CUSTOMERS STAY SECURE

The world is changing at a rapid pace. Cyberthreats are becoming more sophisticated. Your customers are panicking. Offering flexible ways to pay can help them acquire the newest cybersecurity technology to protect their business. Ask us how.

financingteam@techdata.com