An MSP Foundation to Becoming Secure
Page 18

Announcing the Revitalized Security Solutions Website!
Page 9

Further Your Cybersecurity Career - Tech Data Cyber Range is Now Online!
Page 27
# Table of Contents

Welcome to the Fall edition of Security Sentinel.................................................................3
Introducing Remote Home Secure and Incident Response Services............................4
Upgrade Your Business With Tech Data's Digital Security Practice Builder...............7
Join Us Online for Tech Data Security Enforce...............................................................8
Announcing the Revitalized Security Solutions Website!..............................................9
Employee Spotlight: Jamie Buissreth, Supervisor, Security Vendor Management......10
Vendor Spotlight: Discover Saviynt and RangeForce Solutions With Tech Data........12
Employee Spotlight: Ryan Lindeman, Vendor Solutions Representative....................16
An MSP Foundation to Becoming Secure........................................................................18
Get Connected With Tech Data Coaches.........................................................................19
Tune in to On the Clock With a Tech Data Coach.........................................................20
What Partners Are Saying..............................................................................................21
Employee Spotlight: Steve Curtiss, Solutions Practice Consultant, Security..............22
Security: The Foundation of all #MovetoModern Solutions.........................................24
Leverage New Features in the SPI Tool..........................................................................25
Meet the Hackers – The Team Behind the Cyber Range...............................................26
Further Your Cybersecurity Career - Tech Data Cyber Range is Now Online..............27
Employee Spotlight: Tracy Beyer, Senior Manager, Security Solutions......................29

---

**Cisco SecureX**

Help your customers simplify security with the broadest, most integrated platform.

Learn more by reaching out to [technicalboost@techdata.com](mailto:technicalboost@techdata.com)
WELCOME TO THE FALL EDITION
OF SECURITY SENTINEL

We hope you enjoy the many articles and insights we’ve included in these pages as we purposely tried to ensure the content was relevant to our channel and the vendors we support.

Although the world continues to change, the need for cybersecurity solutions has not. Tech Data has seen strong sales in many areas of security, but the highest growth areas are in next-gen firewalls, endpoint security, identity and access management and email security. Plus, as companies are accelerating their investment in the cloud to support remote employees, they realize that the cloud must be secured in much the same way that on-premise resources are.

All this provides an opportunity for you to sell an identity and access management solution that spans both environments comprehensively. It also creates a cloud-based firewall and web-application solution that stands between your on-premise and cloud workloads. We’re expecting to see continued growth in these areas and are excited to watch our partners learn more about these solutions. Don’t forget that you can check out the Tech Data SPI Tool to understand which vendors you can buy from Tech Data in each of these areas.

With many states trying to plan safe ways for students to return to class, I know many of you are also focusing heavily on your SLED business to assist schools in building new technology solutions. My recommendation to you is to ensure you include security in your solution architectures, as schools have a huge need for assistance. In fact, there was a recent breach of five e-learning platforms that exposed over one million online student records because of a misconfiguration in Amazon S3 storage buckets.

Comprehensive security solutions will scan these aforementioned configurations to ensure that cloud workloads are safe and alert the school to potential exposures. Knowing that education is a big topic in our country right now, there is no doubt that hackers will continue targeting our school systems. You can be the partner who steps up to design a solid “defense in depth” strategy for them, and our Tech Data security architects would be glad to participate in those discussions with you if needed.

Another area of cyber space that has seen growth over the last 6 months is managed security services. With threat actors ramping up activity and customer networks more complex and vulnerable than ever, companies are having a difficult time finding qualified security analysts to help them. Their most logical answer is to rely on a local managed security services provider – which could be you.

Tech Data held our latest MSP Evolve workshop in July and had over 50 partners participate for two full days to learn about how to bundle, price and sell managed security solutions. If you missed this great event, you can still watch most of the videos on our Tech Data Digital Security Practice Builder website, so make sure you check it out!

In closing, it’s never too late to start learning about cybersecurity and how you can build and grow your business. Make sure you leverage the Tech Data Digital Security Practice Builder website for over 40 hours of on-demand video content to help you build a strategy, train your sales team, build services, redesign your marketing plan and execute.

Until next time, I hope you all stay safe and find creative ways to keep protecting your customers.

Alex Ryals
Vice President, Security Solutions, Americas, Tech Data
INTRODUCING REMOTE HOME SECURE AND INCIDENT RESPONSE SERVICES

In the first half of 2020, many companies were forced to quickly adapt their workforce to work remotely. The current trends we are seeing from industry-leading Internet companies like Twitter, Facebook and Google are a longer-term or permanent move toward having some percentage of their workforce remain remote.

However, a permanent or long-term remote workforce also expands a company’s attack surface. Threat actors are now turning their focus to home networks. A typical corporate network is well-guarded compared to vulnerable home networks. The average home network is setup with consumer grade network equipment with weak passwords and tend to be completely unmanaged and unpatched by the consumer.

To make matters worse, most households lack appropriate security controls and best practices that are typically implemented in a brick-and-mortar setting. In many cases, company technology is typically shared with other members in the household and many types of software be downloaded to it.

It only takes a simple click of a phishing email campaign before accounts and devices quickly become compromised within the home network.

Hackers recognize the lack of security that is presented by the remote workforce and are taking advantage of the opportunity.

Luckily, Tech Data’s Remote Home Secure Solution can quickly help your customer assess the risk introduced by their remote workforce. This service is delivered by Tech Data’s own security experts who interview, gather data and identify gaps as well as risky behavior, all to find potential weak points introduced by a company’s remote workforce. This service also delivers a comprehensive report which includes an executive summary, detailed findings and risk mitigation recommendations. This service is scoped by the number of remote employees to be assessed, and when its bundled with a Unified Threat Management solution for a company’s executive leader’s home networks for added security and protection, it provides your customer with a complete solution.

Leverage Three New Incident Response Services from Tech Data

Tech Data is also excited to announce that we have three new Incident Response (IR) services that help ensure your customers have the right capabilities in place to respond effectively and recover from cyber threats.

Incident Response Plan Development

The development of a comprehensive incident response plan is a crucial step in minimizing the damage of a security breach. This is because it outlines the steps that need to be followed during an incident, who is responsible for what step and whom to notify and how to resume operations as quickly as possible.

Tech Data’s IR Plan Development can work directly with your customer on your behalf to deliver a cyber resilience policy and playbook which integrates seamlessly with your customer’s people and processes. Plus, it’ll include customized technical and strategic guidance on effectively identifying, containing and neutralizing suspected incidents, which can help your customer to quickly recover and resume their operation with minimal impact.

Incident Response Readiness Review

If your customer is not regularly updating their incident response plan or they are not testing their incident response plan for specific scenarios, then their plan may not function as they expect.

Tech Data’s IR Readiness Review provides your customer with strategic guidance on detecting, containing, eradicating and
remediating suspected incidents and limiting their impact on the business. Since preparation and practice are key to limiting the impact of a security incident, our IR Readiness Assessment can also test for specific scenarios, which is an essential step to building robust incident response plans for your customer.

**Incident Response Emergency**
If your customer has been hacked or has experienced a data security breach that’s caused an interruption in their business or operation, do they know how to effectively address it? Do they have the right security experts on staff that can eradicate and recover from a security incident, while preserving digital forensic evidence? If not, you can now offer them an immediate solution.

Tech Data’s Incident Response Emergency service helps ensure your customers have the right cyber expert capabilities in place to quickly and effectively respond and recover from cyber threats. Our incident responders swiftly engage your customer to provide immediate breach remediation assistance and timely resolutions. Rapid response ensures your customers can successfully contain the overall impact of a security incident.

Tech Data has partnered with various industry-leading cybersecurity firms to deliver our incident response services. These firms, such as IBM X-Force IRIS, Kudelski Security, Foresite MSP, and Abacode Security, all are vetted and specialize in incident response capabilities. Tech Data offers competitive pricing for Enterprise, Mid-Market and Small Business.

Ready to learn more about Remote Home Secure or our Incident Response services? Contact our security team today at securityservices@techdata.com.
The Future is Unpredictable.

Your Customers’ Data Protections Shouldn’t Be.

Discover cutting-edge cybersecurity tools at veritas@techdata.com or call 800-237-8931, ext. 5540408.
The Digital Security Practice Builder is a great resource for developing a security business within your organization. Many of our partners have their marketers get an account to gain access to the customizable content and promotional materials. Other partners encourage their sales teams to sign up and access the robust amount of execution and enablement content. Whatever your reason for signing up, you can take advantage of the following additions and new features that have been recently made to the site:

**The Enablement Course:** View videos covering over 40 security vendors, all to get the most up to date information, identify key differentiators in the market and compare partner programs. We are constantly adding new content to this section to ensure you are getting the most up-to-date information.

**MSP Triangle:** In the upper left corner of many of the marketing and sales execution course videos, you will see a blue triangle with the letters “MSP.” This content is geared towards our partners who want to either become an MSP in the security space or take their technology game to the next level.

**NEW Triangle:** In the upper right corner of many of the videos, you will see a red triangle with the word “NEW” to indicate when new content was added. After a few months, these red triangles will disappear, and as additional videos are added, you will be able to identify the new content easily! In the last month, we have added 21 new videos to the site, and we are about to add two more very soon. So, be sure to check back often.

We are excited to see so many of our partners leveraging this great tool. It truly is a game-changer for many companies. If you aren't registered and haven't checked out the content yourself, you are missing out! Go to practicebuilder.techdata.com/security to get started.
Join us for an exclusive look at the brand new offerings you can showcase to your customers through the state-of-the-art Tech Data Cyber Range. You will also have a chance to connect with our Tech Data security experts and vendor leaders to get your security questions answered.

If you are a part of your company’s security leadership or are an IT security professional, you don’t want to miss out on this exciting event!

Enforce will offer compelling channel and industry trends that will help you gain intelligence around:

- Understanding the rising security opportunities for managed service providers (MSPs)
- How to maximize sales in vertical markets such as healthcare and public-sector
- Knowledge on the latest security solutions and opportunities

REGISTER TODAY

NOV/04 2020
A VIRTUAL EXPERIENCE

The browser is the new endpoint. Act accordingly.

“More than ever, critical business applications are accessed through the internet browser, which wasn’t originally designed with security in mind. Remote browser isolation reduces a vulnerable attack surface by preventing malware from reaching the desktop with minimal impact to the user.”

Alex Ryals, VP, Security Solutions Tech Data.

Why Cyberinc

- Available as Cloud service, appliance or VM
- No agent to install or manage
- Built for MSP - monthly, per user pricing, multi-tenant management and reporting
- Earn high margins through deal registration and new account bonus
- Channel first commitment
ANNOUNCING THE REVITALIZED SECURITY SOLUTIONS WEBSITE

It’s here – our newly refreshed Tech Data Security Solutions website is now live! This new website was designed to enable our partners to discover how they can leverage Tech Data to address their customers’ most critical cybersecurity needs.

The updated site provides partners with the latest information on our broad range of solutions and services as well as our flagship enablement program, the Digital Security Practice Builder. It also features valuable resources including eBooks, brochures, white papers, infographics and the past and current editions of this newsletter, Security Sentinel.

In addition, our new website features a vendor portfolio page that includes our complete line card as well as new vendor microsites for our showcase security vendors:

Vendor microsites highlight promotional programs, contact information and valuable partner resources including solutions briefs, collateral, infographics and white papers. The microsites are refreshed regularly so be sure to bookmark our portfolio page for future updates.

Ready to see it all for yourself? Visit us at techdata.com/security! We encourage you to explore the new site and let us know what you think. For any questions or feedback about the website, contact securitieservices@techdata.com.
EMPLOYEE SPOTLIGHT:
JAMIE BUISSRETH, SUPERVISOR, SECURITY VENDOR MANAGEMENT

Q: What is your job title and describe briefly what you do at Tech Data?

Buissreth: I am a Supervisor within Tech Data’s Security Vendor Management division. I lead a group of individuals who serve in various vendor management, operations and solution building roles. Our overall goal is to optimize the business and uphold our value to vendors and customers.

Q: How does what you do provide value for the company, our customers and/or vendors?

Buissreth: My role allows me to lead and collaborate alongside our vendor representatives. By directing an overarching strategy for businesses and moving forward with positive revenue growth in mind, I help vendors find new ways to drive operational efficiencies.

CONTINUE >
Q: What do you enjoy most about working at Tech Data?

Buissreth: After being with Tech Data for almost 10 years, I most enjoy collaborating with like-minded professionals, many of whom I am fortunate enough to call friends. This dynamic brings new encounters each day and fosters a positive mindset to serve our customers better and grow business.

Q: What is one of your non-work-related goals for the rest of the year?

Buissreth: I strive for greater balance for myself and my family, and much of that includes finding ways to slow down and enjoy moments with those dear to me. On my mission to find this balance, I have found more opportunities to read for pleasure and knowledge. I believe that finding these types of simple joys paves the way for other elements of life to fall into place.

Q: If you could have dinner with anyone from history, who would it be and why?

Buissreth: Irena Sendler, who served as a Polish nurse and social worker during WWII. Born in 1910, she was instrumental in saving 2,500 Jewish children in the Polish underground during the Holocaust. Despite being arrested, she survived the war and lived until the age of 98. A woman like Irena is admirable and could lend tremendous perspective through her experiences and the sheer time she spent on this earth. It helps shape an appreciation for what I have today.

Q: What three items would you need if you were stranded on a deserted island?

Buissreth: A fire starter, water purifier and a signaling device like a flare gun. While I do need to survive, I would like to get back to my suburban life!

---

**EMPLOYEE SPOTLIGHT: JAMIE BUISSRETH, SUPERVISOR, SECURITY VENDOR MANAGEMENT**

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](http://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
1-800-237-8931 x87663 | [ConnectWiseTD@techdata.com](mailto:ConnectWiseTD@techdata.com)
Holtz: We're excited about our new security partnerships with Saviynt and RangeForce. Can you each provide a brief overview of your solutions?

Mozena: Saviynt is a leading identity and access governance platform built for the cloud. It helps customers accelerate cloud initiatives and solve the toughest security and compliance challenges in record time. Saviynt is recognized as a market leader by industry analysts and experts alike, most recently joining the ranks of Inc. Magazine's 5000 fastest-growing U.S. companies.

Our top solution, the Saviynt Intelligent Identity Hub is a software as a service (SaaS) solution that converges Identity Governance and Administration (IGA), granular application access, cloud security and privileged access into the industry’s only enterprise-wide access risk platform. Designed using the principles of Zero Trust, Saviynt's Intelligent Identity solution draws a security perimeter through identity that protects valuable assets while enabling businesses’ agility.

Robison: RangeForce offers an extensive catalog of hands-on training which allows our partners to strengthen their security knowledge as well as resell that same training to their customers.

RangeForce pioneered the concept of combining cloud-based, hands-on training modules, and cyber siege challenges and exercises. Before RangeForce, security pros in IT and DevOps found it nearly impossible to align multiple classes and security exercises with the needs and goals of their team in mind. Many other organizations simply couldn't build a continuous security training program, let alone have any way to assess the readiness of their IT and security teams.

We recently released the 2.0 version of our platform with prebuilt role-based learning paths for SOC, AppSec and DevSecOps teams based on skill level. We also added individual, team and executive reports that offer a clear and accurate picture into existing strengths, weaknesses, gaps and accomplishments against benchmarks.

Holtz: What excites you both about the partnership with Tech Data?

Mozena: Saviynt looked at several options to bring a value-added distributor to our partner strategy and chose Tech Data over all the other options.

We believe that Tech Data's approach to partnering with companies that take a solutions approach to their clients and customers fits best with how we think at Saviynt. As an SaaS offering, an ongoing subscription renewal is critical to our growth and that continued focus on customer success is built into both Saviynt and Tech Data culture.

Robison: We're excited about working with Tech Data to help their partners and customers learn how they can get the most out of exemplary products, while also teaching incident detection techniques across multiple vendor tools. It's a win for everyone: vendors are excited because customers can learn their products in a cloud-based, on-demand training environment, while customers and partners can get more returns on their security teams and investments.
Holtz: Businesses must understand who has access to their data and when that data is accessed to avoid potential risks. How does Saviynt help companies mitigate data risk around data access governance?

Mozena: Saviynt protects structured and unstructured data across hybrid IT systems for internal and external users.

We know data is the core of your business. So you need to be aware of every file that poses a potential risk to your organization - whether it's the structured data locked away in databases and applications, or the largely ignored unstructured data like spreadsheets that so often contain sensitive or business-critical data.

Unstructured data can be in emails, file systems and applications like Dropbox, Box and Microsoft 365. Saviynt’s Data Access Governance (DAG) module enables you to discover, analyze, protect and manage access to all of your data, structured or unstructured, regardless of whether your IT ecosystem is on premises, hybrid or cloud based. Saviynt DAG provides for full visibility into location, ownership and access privileges assigned and used.

Holtz: Emails are one entry point of an attack surface today, however many cybercriminals continue to take a multi-target approach. How does RangeForce help protect partners and enhance their cyber skills to address this?

Robison: The RangeForce cloud platform combines hundreds of beginner and advanced cybersecurity training modules with learning paths that align to the most common security and DevOps roles. Learners are provisioned into a path and immediately start to “develop by doing” and discover the critical skills necessary to defend against an attack.

The training does not stop there though: integrated challenges and team exercises using real security tools help teams learn to work together, coordinating communications and processes so that they can increase the speed of their detection and response process. Finally, you can report on progress, so you have ongoing accountability and visibility into the training your professionals are receiving.

Holtz: Where would you both recommend Solution Providers and MSPs begin to look for opportunities within their clients? Are there certain verticals or markets where you are seeing the most demand?

Mozena: There are many stakeholders who care about access risk across their enterprise. They include, but are not limited to: risk and compliance, internal audit, cybersecurity, finance, HR and digital transformation teams which use DevOps processes to build next-generation business automation.

Due to the breadth of the Saviynt modules delivered on our Intelligent Identity Hub Platform, the client’s initial interest could be a concern about cloud security, or the access risk challenges for a specific critical application. Sometimes it will be the Identity team or more broadly it may be the CISO attempting to gain process efficiency while managing down access risk.
Consistently we see the strongest interest coming from public companies or large private companies with an interest to spin off divisions/business units or the whole company in a public offering. We have more than 200 customers from varied industries. From a public sector perspective, we do have a focus on federal government, not SLED, and are the only IGA product available with FedRamp Moderate certification.

**Robison:** In this past quarter at RangeForce, we’ve seen new customers among medical and technology companies, manufacturers, financial services, and telecom providers. Many are adding training as an essential part of cybersecurity. Accenture’s *Third Annual State of Cyber Resilience Report* reinforces this by saying the speed with which organizations find security breaches is faster for those who provide higher levels of training.

Many large companies have no formal cybersecurity training or a way to benchmark their team’s skillsets and more cyberattacks are successful because of it. Solution providers and MSPs have a great opportunity to change that: with RangeForce, they can stand up a training and cross-train in security programs at a reasonable cost.

The training need is equally important for small security teams too. In some ways, it’s even more important because small IT teams are forced to wear multiple hats. They don’t have the time or budget to be off in an expensive training class: they have a threat and they need to become expert at defending against it in just a few hours. With classes running at 40-60 minutes and covering basic to advanced skills over 2 or 3 modules, RangeForce is a great solution for this need.

**Holtz:** What additional benefits do your respective companies offer Solution Partners/MSPs?

**Mozena:** The Saviynt Global Partner Program offers many benefits, which start with training and sharing best practices.

It’s built with the core idea that Saviynt is a software as a service company. We want our solution partners to make money while representing our products – whether they’re providing advisory, access risk implementation services or a managed outcome for enterprise access governance.

We have seen partners regularly achieve margins between 10% and 30% as a result of these services. The higher margins are typically achieved when the partner is providing thought leadership, delivering on transformative change and when they’ve built trusted relationships across company stakeholders, as opposed to focusing on serving corporate IT.

**Robison:** Let’s start with MSPs because they have a unique model for training. At RangeForce, we have MSPs as customers using the products, and they have had great success in offering these services to their clients just by explaining how it benefits their own security. MSPs can also offer RangeForce’s specialized training to their customer to compliment the MSPs service offering. For example, an MSP might offer detection and containment services for a client, but the client is responsible for accessing and cleaning an infected server or fixing code that is vulnerable to an SQLi attack; RangeForce offers that specialized training that can be packaged and delivered via the MSP.

For solution providers, RangeForce training means service revenue on top of product margin. Not many providers out there can run a red or blue team exercise, build a cybersecurity training program, or optimize a client’s detection processes or response playbooks. RangeForce makes creating and offering these services to clients’ a reality and allows our partners to build new revenue streams.

For further details on RangeForce, Saviynt or any other security vendors at Tech Data, contact our security service team at securityservices@techdata.com.
For MSPs, there’s a new way to spell “win”!

X-D-R

Go beyond EDR with comprehensive detection and response for both endpoints and email (the #1 threat vector)

Trend Micro™ Worry-Free™ XDR is a WIN-WIN!

• Hunts for and finds breaches faster to keep your clients and your reputation safe
• One platform integrated to endpoint and email responds faster with less resources
• Grow with security services by offering additional revenue-generating opportunities

Show your clients what they’ve been missing.

That’s the beauty of Trend Micro Worry-Free XDR

More at www.trendmicro.com/msp

Unknown threats detected and automatically stopped over time by Trend Micro. Created with real data by artist Brendan Dawes.
EMPLOYEE SPOTLIGHT:
RYAN LINDEMAN, VENDOR SOLUTIONS REPRESENTATIVE

Q: What is your job title and describe briefly what you do at Tech Data?

Lindeman: At Tech Data, I am a Vendor Solutions Representative. My focus is to build relationships with channel partners to facilitate and grow SonicWall business in the Western United States Region. Also, I have expertise in SonicWall and Tech Data products, programs, competition, and market strategy to be able to answer inquiries regarding both companies.

Q: How does what you do provide value for the company, our customers and/or vendors?

Lindeman: Being the subject matter expert of SonicWall at Tech Data, I assist our channel partners with anything SonicWall and Tech Data related. This includes knowing the right people at both Tech Data and SonicWall to complete projects. My team and I assist throughout the opportunity, which allows SonicWall partners, Tech Data employees and SonicWall employees to use us as an expert resource for Tech Data and SonicWall procedures.

CONTINUE >
**EMPLOYEE SPOTLIGHT: RYAN LINDEMAN, VENDOR SOLUTIONS REPRESENTATIVE**

**Q:** What do you enjoy most about working at Tech Data?

**Lindeman:** The colleagues I work with every day. Knowing you have a strong group of colleagues working alongside you makes coming into work everyday fun and enjoyable.

**Q:** What is one of your non-work-related goals for the rest of the year?

**Lindeman:** Continuing my training to compete in a 10K race by the end of 2020.

**Q:** If you could have dinner with anyone from history, who would it be and why?

**Lindeman:** If I could have dinner with one person from history, it would have to be Babe Ruth. I would love to know what it was like playing baseball in the early 1900s. As a former college baseball player, I would ask him about players’ lifestyles, fans and the game itself. I would love to hear stories about other players during that era and compare the game it is today to the early 1900s.

**Q:** What three items would you need if you were stranded on a deserted island?

**Lindeman:** My family, satellite TV to watch the University of South Florida football (Go Bulls) and, of course, drinking water.

---

**Artificial intelligence that outsmarts phishing attacks.**

Stop email impersonation attacks with **Barracuda Sentinel**.

Scan to learn more about Barracuda Sentinel. For more information, contact barracuda@techdata.com
John Komer has enjoyed a dedicated 40-year career in the Technology Industry. Prior to joining Tech Data as a Solutions Practice Consultant, he has spent the last 25 dedicated to cybersecurity. John has enjoyed technical roles involving voice and data networks, video, data center, and security technologies, designing, and installing solutions for customers. John has held roles as a system engineer, sales account manager, global account manager and founder of a security consulting company for cybersecurity after the 9/11 WTC attacks to help the Department of Homeland Security.

You always hear when you are on an airplane to put your oxygen mask on first before helping others. In the same belief, you can't help your customers be secure until you are secure yourself.

As you continue to evolve your business to sell security, Tech Data has developed an approach you can take to ensure that your business is just as secure as the solutions you sell your customers. So how can you ensure that your MSP business is secure? Here are a few Tech Data services and teams you can take advantage of yourself to help you and your customers:

1. **Vulnerability Assessments (VA)** help identify weaknesses and risks present in the deployed technology, security processes and users within an organization. External VA, Internal VA and, if necessary, Web Application Assessment and Social Engineering can be conducted for a more in-depth approach.

If budgetary concerns exist, start with an External VA and progress to Internal VA, Web Application Assessment and Social Engineering later. Based on the Vulnerability Assessments outcomes, perform remediation efforts on the prioritized areas outlined in the report/executive summary.

Tech Data Sales Practice Consultants (SPCs) or Business Development Managers (BDMs) can provide potential follow-on solutions or services to meet the gaps identified in the VA. Potential follow-on solutions include MFA, IPS, patching, VPN, policy development (RECON™ Policy), DR/BC, PAM and Security Awareness training. If additional follow-on support is needed, you can also engage the aligned Tech Data Services Representative (SR) for solutions like RECON™ SOC, solution implementation, SIEM tuning and monitoring, as well as IR development/testing.

2. **Penetration Testing (PT)** provides a comprehensive snapshot of the methods threat actors could employ to exploit network vulnerabilities to gain access to critical systems. External PT, Internal PT, and if necessary, Web Application Penetration Test can be conducted for a deeper approach.

If budgetary concerns exist, start with an External PT (least expensive) and move on to Internal PT and Web Application Penetration Test later.

3. **Tech Data Sales Practice Consultants (SPCs)** or Business Development Managers (BDMs) can provide potential follow-on solutions or services to meet the VA and PT’s identified gaps.

Potential follow-on solutions include MFA, IPS, patching, VPN, policy development (RECON™ Policy), DR/BC, PAM and Security Awareness training. If additional follow-on support is needed, you can also engage the aligned Tech Data Services Representative (SR) for solutions like RECON™ SOC, solution implementation, SIEM tuning and monitoring, as well as IR development/testing.

4. Additionally, Tech Data offers many **Training Opportunities**. We are excited to come off two very successful MSP Evolve events helping MSPs transition to full MSSP service delivery organizations.

During the event, we provided great speakers and discussions on how to incorporate security into your MSP practice and evolve your business to adopt a social selling strategy.

For those who couldn't attend, we are hoping to offer a fall class with a specific date to be determined. But until then, much of the material from the last session can be found on our Digital Security Practice Builder website. You will also be able to find resources for strategy, product and service solutions, marketing and sales business development to empower you to drive new business.

Another great resource you have access to is the Tech Data Coaches program. This program is a free resource for all Tech Data partners and you have access to many Tech Data Security team members as part of this resource. Just sign up to access and receive consultative services from some of the experts on the Tech Data’s large support organization!

To help your customers manage their IT budgets while finances are tight, we have finance programs that can turn traditional security HW (i.e. firewalls, IDS, etc.) into a monthly OpEx cost. This can help your partner create a solution that scales with their business, so they only have to pay for what they use. In fact, we have specific programs with SonicWall and Fortinet so partners can pay for that equipment and resell it by the month to their customers as part of a managed services program.

Contact securityservices@techdata.com for additional information.
GET CONNECTED WITH TECH DATA COACHES

Find the right person to help you achieve your desired professional or business outcomes fast. The Tech Data Coaches Community is an online network designed to streamline your and your colleagues’ connections to channel professionals across Tech Data’s ecosystem.

Get matched, schedule meetings, follow thought leadership and grow your connections in minutes! All you have to do is create your free account to get started.

Here are just a few features of our online community:

- **Easy Account Setup:** Share your professional interests and establish your profile in minutes.
- **Community Access:** Favorite, follow and connect with 70+ channel professionals. There are several coaches from our security team who are here to help!
- **Coach Matching:** Receive suggestions on the best connections for you.
- **Pain-Free Scheduling:** View coach availability and request a meeting in seconds.

Fortinet Keeps You Ahead of Ransomware

The Fortinet Security Fabric brings an affordable, broad, integrated and automated approach to security to protect your organization from ransomware. Powered by intelligence from FortiGuard Labs, Fortinet combines market-leading prevention, detection, and mitigation with top-rated threat intelligence to combat today’s most advanced threats. Protection begins with knowing how it works!

Contact the Tech Data Fortinet team to learn how Fortinet delivers comprehensive protection against ransomware:
(727) 539 7429 Ext. 5545031 / fortinet@techdata.com
or go to https://shop.techdata.com/vendorpartners/fortinet
Diana Weber discusses the power of the Agile mindset method and how it motivates teams to collaborate, innovate and grow their decision-making capabilities.

Mark Shaffer demystifies smart cities, how they optimize and raise up communities and municipalities and shares how our partner community can tap-into this unique vertical market.

Adrienne Ambrose sheds light on the importance of strategic account management, building trust among customers, as well as additional best practices and tip.

Jeremy Singh addresses brand marketing, the power behind developing a clean and concise brand and simple tactics you can easily adopt to begin expanding your brand image and influence.

Jade Witte sheds light on the cybersecurity opportunity, common vulnerabilities and risks and market trends.

Tune into more episodes on the Business Insights section of Tech Data’s Authority Blog.
WHAT PARTNERS ARE SAYING

Network Expansion, simple meeting scheduling, time-savings and empowering personal and business outcomes are just a few reasons our reseller partners are excited about this community:

Matt Tinney, Founder & CEO, Windows Management Experts: “The call I had with Tech Data’s public sector consultant provided instant value-add actions I can take towards helping us build our federal government strategy! I now have Tech Data in mind for our strategic direction within SLED as well. What I enjoy most about Tech Data Coaches is the ease of connecting with many resources across all of Tech Data.”

Richard John, Founder, RJO Ventures: “Being involved in the technology sector as a service provider, I’m always looking for ways to learn more and to also develop my individual skills and receive guidance on how to adapt to current trends. The Tech Data Coaches platform was able to connect me with a Google Cloud expert who provided me with excellent feedback on how we could take steps to grow our business with the right solution. Tech Data Coaches makes me feel much more connected to my partners at Tech Data and I’m extremely excited about the ability to connect with subject matter experts in their ecosystem directly!”

Juan Fernandez, Vice President of Managed IT Services, ImageNet Consulting: “As a managed service provider (MSP), we find Tech Data Coaches to be a valuable resource, providing guidance and support when we need it most. What I find most impressive is that Tech Data Coaches is not just for executives – it’s a great go-to reference for people at all levels who seek mentorship or seek input on how to expand their capabilities. I plan to have my entire team – including our marketing department – sign up to use this online coaching platform.”

JOIN OUR COMMUNITY TODAY!
Create your free account at bit.ly/TechDataCoaches.

QUESTIONS?
Contact us at coaches@techdata.com.

remoteworkware
Free your employees to work more securely from anywhere.

See Carbon Black LIVE in the Tech Data Cyber Range at an upcoming event

Strengthen and simplify your security stack with VMware Security Solutions.

Contact vmware@techdata.com to learn more!
EMPLOYEE SPOTLIGHT:
STEVE CURTISS, SOLUTIONS PRACTICE CONSULTANT, SECURITY

Q: What is your job title and briefly describe what you do at Tech Data.

Curtiss: I am a Solutions Practice Consultant in the Security division. With 55% of small businesses closing their doors within six months of a cyberattack, my job is to help our Tech Data partners save these businesses with our wide portfolio of cybersecurity solutions.

Q: How does what you do provide value for the company, our customers and/or vendors?

Curtiss: I train Tech Data partners to speak the language of security to reduce their clients’ cybersecurity risks. At Tech Data, we offer a complimentary, conversation-based, non-technical security maturity assessment that provides a grade (A, B, C or D) and a report on the same phone call. We also have a monthly 30-minutes with a Hacker Podcast that provides fresh insights and strategic solutions to real issues. Our most recent podcast surfaced key security concerns as workers return to work or remain remote.

Boost your security revenue with Microsoft 365

Secure your customers

$720 average revenue

- Licensing sale
- Base security feature deployment
- Supplement on-prem AD with AAD
- Reduce operational cost

Drive assessment

+$310 average revenue

- Cloud security assessment
- Hybrid security assessment (CSAT)
- Implement compliance features
- End-user security readiness

Monetize with services

+$340 average revenue

- Monitoring and alerting
- IAM policy management
- Device policy management
- Threat remediation (P2P)
- Compliance as a service (P2P)

Three-year average revenue per SMB seat from Microsoft 365 Business

Source: The Microsoft 365 Partner Opportunity, A Forrester Total Economic Impact™ Study Commissioned By Microsoft, July 2019

Contact your Tech Data Microsoft Cloud Team
Call 800-237-8931 ext. 5545006
or email Microsoft@techdata.com

Learn More at Bit.ly/TDSecurity
EMPLOYEE SPOTLIGHT: STEVE CURTISS, SOLUTIONS PRACTICE CONSULTANT, SECURITY

Q: What do you enjoy most about working at Tech Data?

Curtiss: I enjoy the collaboration between Tech Data employees and vendors to craft security solutions for our partners. We represent the best in delivering solutions for security, IoT and cloud.

Q: What is one of your non-work-related goals for the rest of the year?

Curtiss: I want to make a difference – either by helping first-responders in some way, lending assistance to the elderly or helping out at a food pantry.

Q: If you could have dinner with anyone from history, who would it be and why?

Curtiss: Maewyn Succat. He was born into a well-to-do British family around 386 A.D. When he was only 16, he was taken hostage by Irish marauders and made an Irish slave for six years, herding sheep and cows. At 22, he escaped, went back to Britain, and then returned to Ireland to inaugurate changes we are still benefitting from globally today. He convinced many to abolish slavery and was the first person in the Western Hemisphere to promote education for the non-ruling classes (the common folk). Most know him by a different name though – Saint Patrick.

Q: What three items would you need with you if stranded on a deserted island?

Curtiss: A guitar, water and the book of Psalms.
Meet the #MovetoModern. It’s dynamic, powerful and always on. It’s where technology meets fast, forward momentum – and it’s all made possible by the integration of cybersecurity.

But how does it prioritize security? Let us break it down for you.

**Pre-Loaded With Third Platform Technologies**
From mobile devices to tablets and laptops, #MovetoModern solutions are pre-loaded with third platform technologies like security, IoT and cloud, and are ready for deployment. Ultimately, our team develops modern solutions with the end-user in mind. Plus, without security built into a modern solution, the end-user can’t meet their goals. What’s more, they risk breaches and cyberthreats. That’s why #MovetoModern solutions are embedded with the most up to date third platform technologies on the market.

**Built to Solve Modern Challenges**
Productivity is the #MovetoModern priority. Regardless of where they’re used, Modern EDGE solutions solve problems with speed and drive measurable outcomes that matter. We know that for today’s modern end-user data is gold. Pulling data from any device and using it effectively is a critical matter. Fear not. All #MovetoModern solutions are integrated with cybersecurity.

**Meeting You Where You Are**
We no longer live in a world dominated by distinct lines. Today, our work and personal lives are blurred. #MovetoModern solutions help the modern workforce meet and achieve their goals wherever they are, at whatever time of day or night. What’s more, the Modern EDGE is intuitive. It drives seamless interactions between people and technology. Plus, modern cybersecurity is built into each solution. Users are free to follow their instincts, discover technology that lets them explore without restrictions and create with confidence.

**Why Move to Modern? And Why Now?**
The #MovetoModern movement is all about giving end-users what they want and need to excel. Research shows that outdated devices are a culprit for slowing down business. The numbers speak for themselves:

- $2,397: Total cost of owning a 4+ year-old PC, enough to replace with one or more newer PCs.
- 61% of SMBs are unable to better secure and protect data on newer PCs.
- < 5 min: Windows 10 PCs boot up in less than 5 minutes, versus waiting 20 minutes for older PCs to boot up and log into key systems.

**Modern Solutions: Why They Help Us Excel**
With modern devices, we’re transforming the anytime, anywhere digital workforce. Enhancements in security, manageability and productivity are revolutionizing the modern workplace. When end-users switch to modern devices, here’s what they can expect to achieve:

- Up to 80% better overall performance than a 4-year-old PC running Windows 108
- Up to 40% faster data analysis than a 4-year-old PC running Windows 109
- Up to 2.1X better multitasking than a 4-year-old PC running Windows 1010

When you #MovetoModern with customers, we want you to deliver a complete and secure solution. Visit our site for a complete rundown of what we can do for you. You’ll find key statistics, our best-in-class vendor lineup, and new solutions to help you move forward with forward-thinking technology that’s smart, first-rate and secure.

CHECK IT OUT
LEVERAGE NEW FEATURES IN THE SPI TOOL

Have you had a chance to become familiar with the Solutions Product Inventory (SPI) Tool yet? The SPI Tool is a global resource that just launched this spring – you can leverage it to position new security solutions and build solutions on the fly, all while enabling you to have deeper conversations with your customers.

The tool is easy to access through the website and includes a simple keyword search as well as vendor, product, category, sub-category, MSP readiness and geographic region search features. We would like to draw your attention to a few new enhancements to the SPI tool:

**Tech Data Professional Services** – By selecting this category, you will discover assessment services, compliance services and implementation services for various vendors that our partners can leverage in expanding capabilities to support their end-user customers.

**Security – Public Sector** – To the left of the geographic region selection is a dropdown list where the user can select products and services Tech Data is authorized to sell into the Public Sector. Many of these security offerings are handled by Tech Data’s recent acquisition of DLT Solutions, a distributor primarily focused in this sector. You will notice, under the NIST 800-53 category and the associated sub-categories, solutions that meet those requirements.

And if you have not checked out the SPI tool, tune into this video where Jade Witte, solutions architect, provides a great overview of the tool.

Leverage the SPI Tool with your customers today! And if you have any further questions, feel free to reach out to us at securityservices@techdata.com.
MEET THE HACKERS – THE TEAM BEHIND THE CYBER RANGE

Beyond being a state-of-the-art, hands-on facility for training, demonstrations, engagement and services, Tech Data has equipped their Cyber Range with an elite team of “white hats,” also known as ethical hackers. This team of cybersecurity professionals possesses a broad range of skills and talents to showcase the many benefits of the range to our partners, vendors, customers and community.

What does it take to run a Cyber Range? You need one-part ingenuity, one-part creativity, equal parts determination and a dash of playfulness. Mix it all together and you end up with Tech Data’s top-notch Cyber Range team. Now, we’d like you to meet the hackers:

Joshua Harp – Tech Data Cyber Range Engineer: Joshua has hands-on experience and in-depth technical knowledge in computer network attack (CNA) and computer network defense (CND). He is a core volunteer with a local non-profit organization that is leading the country to teach practical cybersecurity skills with real-world applications.

As a Field Technical Consultant with the Tech Data security services team, Josh was previously responsible for the design, implementation and follow-through of security assessments, penetration tests and attack simulations. These days, he primarily focuses his skills on our Cyber Range; however, Joshua is still a valued contributor to our Tech Data Security Solutions team.

Outside of work and volunteering, Joshua can be found jamming with the console cowboys in cyberspace.

John Garner – Tech Data Cyber Range Engineer: John has extensive experience defending and protecting company networks. He brings his “blue team” talents and knowledge to the Cyber Range to help develop simulated training environments. These simulations will help drive the cybersecurity industry forward and support the Tech Data security services team.

John has spent the last 5 years working in managed security service provider (MSSP) and security operation center (SOC) environments. In these roles, he worked with a diverse set of network security tools across many enterprise environments, including municipal, education, healthcare and retail. John also dealt with advanced cyber threats, incident response and business continuity. In his most recent role, he helped develop the training curriculum for the SOC.

When not at work, John can be found crushing the online poker tables.

Daniel “Tails” Seth – Security Consultant, Security Solutions: Daniel is a Security Solutions Consultant with the security services group at Tech Data. Daniel’s main job is a penetration tester (also known as a “pen tester”). This service assists customers with identifying gaps in their security, computer systems, networks, applications and human targets. This offensive stance helps customers get an idea of what a bad actor could do and how it may impact a business. Daniel supports the Tech Data Cyber Range by building out technologies and training curriculum that helps Tech Data customers upskill talent in cybersecurity.

Daniel has worked in the IT and cybersecurity industry for many years. Daniel volunteers his spare time with the Arizona Cyber Warfare Range and its foundation, the NICE Cybersecurity Workforce Framework (NCWF). He also enjoys teaching and mentoring others in the security industry, as well as, tracking and learning the new changes in security.

Dylan Hudson – Security Consultant, Security Solutions: Dylan is a Security Consultant for the Security Solutions team. Dylan works as a pen tester. Some of the deliverables he manages as a consultant are external/internal assessments, social engineering and web application testing. Dylan works closely with the Cyber Range engineers to assist with building out technologies, automation and education curriculum.

Dylan has worked in cybersecurity for many years and has hundreds of volunteer hours at the Arizona Cyber Warfare Range, where he learned his penetration testing skills. Dylan also has experience in defensive security by working at an MSSP and for a major airline.

In his free time, Dylan mentors high school students about cybersecurity. Dylan has a passion for cybersecurity and always wants to learn new things; his favorite type of testing is wireless assessments.

This team of highly talented security professionals look forward to working with our partners. They are a group of individuals that are passionate about fostering the mission of the Tech Data Cyber Range which is to enable new cybersecurity talent and significantly improve the skills of existing cybersecurity professionals in the partner channel and the end-user community.

For more information on our Cyber Range, contact us at securityservices@techdata.com or visit cyberrange.techdata.com.
Change is inevitable, but letting it stop you from advancing in your cybersecurity career is not. Our Tech Data Cyber Range team has navigated the recent changes to the cyber-landscape and transitioned several exciting new offerings to an online format that you can participate in from the comfort of your home.

By leveraging the online offerings of the Cyber Range, you will be able to equip yourself with the skills necessary to progress in your career and bring holistic cybersecurity solutions and services to your customers.

Discover how we took our cyber playground, led by a team of elite cybersecurity experts, and converted several of our trainings courses into online offerings just for you.

**Incident Response (IR) Experience**

Hands-on Incident Response experiences enable you to unleash multiple cyberattacks into your customer’s live environment. More than a tabletop exercise, this build-your-own-adventure experience uses our sophisticated threat intelligence platform to help you rehearse a plan of action. Every aspect of your cybersecurity plumbing is tested. At the end of the day, you will see where your gaps are and be better prepared for an attack – with no impact to your work environment.

- Leadership teams walk through a live simulation of a cyberattack and see how you respond.
- Test your own breach runbooks, or we can help you design one.
- Simulation lasts 4-hours and can be performed in the morning or the afternoon.

**Defense-In-Depth (DiD) Training**

DiD is a method in cybersecurity where organizations have multiple layers of security controls in place to protect data and information from cyberattacks. If one of the security controls fail, then another layer within your controls will serve as back up protection and thwart the attack.

Participants who complete this training will come away with a better understanding of:

- How adversaries bypass traditional defense strategies.
- A well-defined framework for protecting their business infrastructure from adversaries.
- How to implement and manage a Defense-in-Depth strategy in their organization and verify it is working properly.

**Zero Trust (ZT)**

ZT is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters. Instead, it must verify anything and everything trying to connect to its systems before granting access.

Participants who complete this training will:

- Become skilled on the core principles of Zero Trust.
- Be able to evaluate and plan for implementing or converting to a Zero Trust framework.
- Be able to monitor and deliver analytics of network/system disturbances.

**Adversarial Review (AR)**

An AR assessment is used to help improve an organization's readiness to withstand attacks from different attack vectors. This training focuses on the strengths and weaknesses within an organization's cybersecurity strategy by reviewing the people, processes and technology which support it.

Participants who complete this training will have a better understanding of:

- Your adversary’s motivations along with tools, techniques and procedures.
- Why uniform policies are needed for your cybersecurity strategy.
- Improving your organization’s readiness to withstand attacks from different attack vectors.
- Your organization’s own cyber resiliency.

These are just a few of the offerings we have made available online for you. To find out how to register for a course, contact us at [securityservices@techdata.com](mailto:securityservices@techdata.com) or visit [cyberrange.techdata.com](http://cyberrange.techdata.com).
When Threats Are Limitless, Your Defenses Must Be Boundless.

SONICWALL

SonicWall.com

© 2020 SonicWall, Inc. All rights reserved.
EMPLOYEE SPOTLIGHT:
TRACY BEYER, SENIOR MANAGER, SECURITY SOLUTIONS

Q: What is your job title and briefly describe what you do at Tech Data.

Beyer: I have worked at Tech Data for over 28 years. My current role is Senior Manager in the security division, where my primary responsibility is to work closely with my team, vendors and partners to ensure business growth and development. All this is with an emphasis on customer service excellence. I am also privileged to launch new security vendors into Tech Data’s ecosystem.

Q: How does what you do provide value for the company, our customers and/or vendors?

Beyer: Every day, my job impacts customers, vendors and Tech Data in numerous ways. So, I strive to create a positive culture for my team and foster new ideas for my vendor community to stimulate growth in revenue and customer base.
**EMPLOYEE SPOTLIGHT: TRACY BEYER, SENIOR MANAGER, SECURITY SOLUTIONS**

**Q:** What do you enjoy most about working at Tech Data?

**Beyer:** I enjoy working closely with my team members to guide their career paths and working with top vendors in the cybersecurity arena.

**Q:** What is one of your non-work-related goals for the rest of the year?

**Beyer:** To find creative ways to be together with my family and friends in a safe environment.

**Q:** If you could have dinner with anyone from history, who would it be and why?

**Beyer:** My grandfather, Dr. Thomas Nicolson. Grandad was a pilot in the Korean War and WWII. After serving his country, he graduated from Auburn University with a doctorate degree in Optometry. He opened his own office in Pinellas Park, Florida, which he operated between 1962 and 1985 and was also Chairman of the Pinellas County LION’s Club. I was lucky enough to work with him while I was in high school and after graduation. Granddad instilled in me a strong work ethic and to accomplish the goals I set in my life.

**Q:** What three items would you need with you if stranded on a deserted island?

**Beyer:** This is easy - my family including my grand dog, my cell phone and sunscreen.

---

**Shift-Left to Proactive Endpoint Security**

Win the battle *before* it begins.

Shift-left means being able to anticipate and stop breaches before they happen, and should an attack get through, run more effective mitigation procedures. McAfee offers the first and only proactive endpoint security solution that uniquely combines three key capabilities:

1. Prioritize threats that matter
2. Predict your ability to protect
3. Prescribe necessary actions to take

Learn how McAfee gives you the intelligence you need to implement a shift-left cybersecurity strategy.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Copyright © 2020 McAfee, LLC.