Welcome to the inaugural issue of our Tech Data Security publication! Our goal is to communicate recent trends in cybersecurity and inform our channel partners about new and upcoming offerings from the Tech Data Security Solutions team. I’m confident that you’ll find the information on these pages to be informative and assist you in building and growing your security practice.

As we close out 2019 and look to an exciting 2020, it’s important that we identify where our customers are struggling when it comes to cybersecurity so that we can develop solutions to these challenges. Our customers are facing threats from all sides with ransomware toward the top of the list, particularly in healthcare. Just a few weeks ago, Wood Ranch Medical in Simi Valley, CA, announced they are closing their doors on Dec. 17, 2019, according to a note posted on its website because of a devastating attack that encrypted all their patient records. While customers feel helpless, this is a great opportunity for our Tech Data partners to offer assistance. With expertise in backup/recovery solutions you can ensure that customers can recover quickly from a ransomware attack that encrypts their data. With a focus on advanced endpoint security, you can arm your customers with a prevention approach that avoids the devastating results of an attack.

Other top security concerns for our customers include Business Email Compromise (BEC) and email phishing attacks, cryptojacking, which uses customer compute devices to mine bitcoins, and advanced exploit kits that provide hackers with full access to a network. The good news is that with training and the right technology, our partners will be more than capable of offering effective solutions to customers so they can minimize the risks in these attacks and even provide other security-managed services to outsource the expertise.

Tech Data is excited to offer many security solutions to our channel. We’re here to assist them in building a security practice, starting with our Security Practice Builder Program. We offer a structured step-by-step program for identifying areas of security to invest in, a selection of security vendors, development of a marketing strategy and building block technologies for developing a security managed service offering.

To enhance our offerings, Tech Data has just launched a Cyber Range in Phoenix, AZ to provide partners with security training opportunities, a facility for demoing vendor security technology and an interactive environment for hosting customer events. For more information about these solution offerings from Tech Data and much more, please reach out to us at securitysolutions@techdata.com.

Alex Ryals

Vice President, Security Solutions, Americas
It’s critical to assess and understand your email security vulnerabilities. Using artificial intelligence and API integration with Office 365, the Barracuda Email Threat Scanner quickly and effectively finds social engineering attacks currently sitting in your mailboxes.

» Start your scan today with Barracuda.
// CHECK OUT THIS IN-DEMAND SOLUTION FROM TECH DATA

With Firewall-as-a-Service (FaaS), you can build managed firewall services around your MSP security practice or portfolio with Tech Data’s FaaS offerings. Increase profitability by managing devices and policies on behalf of their end-user, allowing pay as you grow pricing while their business ramps up. We spoke with Tracy Holtz, Director, Security Solutions at Tech Data, to find out more about this offering.

HOW DOES THE FAAS OFFERING HELP TECH DATA’S PARTNERS?
Holtz: Tech Data offers partners the ability to bundle SIEM and managed firewall solutions together, offering incremental margin potential and scaling with customers’ needs. Plus, Tech Data’s MSSP Practice Builder tracks with Security Practice Builder, helping partners build out MSSP offerings within their business.

DO WE EXPECT TO SEE A LOT OF GROWTH FROM THIS SERVICE?
Holtz: Managed security services continue to be highly demanded in the market since many companies have limited security resources. As threats continue to grow and evolve, we can expect the need for solutions like this to increase.

WHAT MAKES TECH DATA’S FAAS SO POWERFUL?
Holtz: Tech Data partnered with our leading network security vendors to provide advanced, security-focused technologies and threat intelligence tailored to broaden partners’ security service portfolios all while being delivered under a monthly recurring procurement model. End users pay for the seats they need at a low cost and can scale as their business needs change.

91% of malware attacks use DNS.

Bad actors rely on DNS to facilitate their attacks. You rely on DNS to keep your network connected. Don’t let hackers use DNS against you.

Secure the protocol. Secure your network.

Talk to your Tech Data rep

For more information please send an email to bluecatus@techdata.com or call us 1-800-237-8931, ext. 73402.

The Adaptive DNS™ company

Intelligent Networking | Intelligent Automation | Intelligent Security

bluecatnetworks.com
SECURE YOUR CLOUD WITH CONFIDENCE

For additional information on Check Point Solutions, contact one of our specialized solution representatives at Tech Data 800-553-7921, ext. 82380.
TO PAY OR NOT TO PAY…

HOW EASILY COULD YOUR BUSINESS BE HELD TO RANSOM?

Jerry in HR clicks on a ‘CV’ attached to a ‘job application’ email.

Alarmed, Jerry calls Pete in IT, who checks and confirms Jerry’s machine has fallen victim to a ransomware attack.

He quickly discovers that the damage is worse than he’d feared: the company’s main file server has been infected… and his anti-virus software won’t remove it.

Jerry’s company could backup Windows™ PCs and Mac™ to their datacentre storage for inclusion in server protection policies with Veritas Backup Exec & NetBackup.

Jerry could self-service restore to his current machine, a new machine, or his mobile device.

Jerry’s company could backup users’ desktops & laptops direct to public cloud storage.

LET VERITAS HELP YOU PROTECT YOUR BUSINESS

For additional details on how Tech Data and Veritas can partner with you to protect your customers data, contact one of our specialized Tech Data Solution Representatives at (800) 553-7921, ext. 71424 or visit our manufacture store at https://shop.techdata.com/vendorpartners/veritas.
// IS TRANSITIONING FROM AN MSP TO MSSP WORTH THE RISK?

By Jade Witte, Solution Practice Consultant, Security, Tech Data

Most MSPs looking to make the transition to MSSP are talking about the liability risk associated with getting sued if there is a breach with one of their customers. Even investors sue because of the negligence of the organization to secure its infrastructure, it seems even riskier to get into this line of work. So why are companies making the shift?

MSSPs do not take on this liability. Their contracts clearly stipulate they’re not liable for any breaches, loss of intellectual property, ransomware demands, etc. This liability falls on the customer. It’s their business, they are responsible, and most MSSPs are not about to take on that liability themselves.

SO, WHAT ARE COMPANIES TO DO TO PROTECT THEMSELVES?

Get proper cyber insurance and read the fine print. Not all insurance is created equal. Know the loopholes that an insurance company has before you sign. Don’t wait until you try to process your claim to find out you aren’t covered.

Transforming any business carries an inherent risk. Tech Data is in the business of helping our partners be successful; we have a number of programs that help make the transition from MSP to MSSP smoother and less risky and help the business to scale efficiently and rapidly when the big opportunities strike.

Learn more about Tech Data’s security solutions.

MOST HEADLINES ABOUT CYBERATTACKS FEATURE BIG, WELL-KNOWN BUSINESSES.

But the 2018 Verizon Data Breach report found that

58% of all attacks occurred at small businesses.

Your customers may be more vulnerable than they realize. Protect them and grow your business with the Advanced Security features in Microsoft 365.

Learn More
Almost all organizations stand up tools to help with anti-virus, firewall and endpoint security. But that doesn’t mean they’re secure. In fact, the gap between these securities is exactly where the bad guys walk in to do their damage. You can help fill that gap with solutions from Micro Focus, available at Tech Data.

Two areas where you can add quick and effective impact are access management and application security. Micro Focus products in these areas have relatively shorter sales cycles and relatively shorter implementation time frames. This means it’s easy to add as a solution to complement anti-virus, firewall and endpoint solutions.

**APPLICATION SECURITY**

**Fact:** Hackers can break into an application without detection from many anti-virus and firewall products. Application security products help protect against such hacks. Micro Focus provides “Application Security as a Service.”

**The Micro Focus solution:**

- Integrates static, dynamic and mobile application security testing with continuous monitoring for web apps in production.
- Provides easy to use and fast results with regular vulnerability updates.
- Is scalable for application growth - delivered in a flexible cloud, on-premise or hybrid.
- Dedicated technical team support to optimize your services product.

**Micro Focus Application Security products include Fortify-On-Demand and WebInspect.**

**ACCESS MANAGEMENT**

**Professionals want easy access to systems, but security teams must ensure that only authorized users can gain access to systems and sensitive data. Micro Focus provides identity-based access based on the risk of “who” is accessing “what” information from “where.”**

**Micro Focus Access Management products provide:**

- Quick and secure access to the resources end-users need.
- Single sign-on (SSO), which allows for stronger password policy and makes management simpler.
- Access control to IT resources for regulatory compliance.
- Secure access to mobile and BYOD users.
- Authentication methods based on risk- and supports more authentication methods than any other vendor.
- Support for more application types (SaaS, Web, Mobile, Legacy) than any other vendor.

**Micro Focus Access Management products include Access Manager and Advanced Authentication.**

Reach out to microfocus@techdata.com or 727-593-7429, ext. 77732, to learn how you can help your customers fill in their security gaps with these and other Micro Focus solutions.
Centrify’s mission is to stop today’s No. 1 leading cause of breaches – privileged access abuse. Our Privileged Access Management solutions offer the antidote.

Gartner estimates that organizations will spend $137 billion on IT security and risk management in 2019 which equates to a lot of opportunities for you to sell and make commission!

Contact us at centrifyus@techdata.com or 727-593-7429, ext. 73404.
We sat down with Brett Scott, Director, Security Training and Enablement for Tech Data, to discuss the new Tech Data Cyber Range. We learned what inspired this masterpiece of cybersecurity training, what our partners can expect from experiencing the range for themselves, and how it fits into Tech Data’s broader plan to stay a leader in cybersecurity offerings.

SO BRETT, WHAT INSPIRED THE TECH DATA CYBER RANGE?
Scott: I became an employee of Tech Data in November 2016, after Alex Ryals saw me speaking at a conference on cybersecurity for business. I am the founder of The Arizona Cyber Warfare Range/National Cyber Warfare Foundation, which was started in 2012. I was new to distribution and learned the ropes thanks to mentorship from Alex Ryals and Phillip Privett. In September 2018, Alex offered his “big idea” for Tech Data to provide a cyber range similar to the cyber warfare ranges I was operating.

HOW DOES THE CYBER RANGE FIT INTO TECH DATA’S SECURITY OFFERINGS?
Scott: The Tech Data Cyber Range is a mix of our cybersecurity team, our partners, and our vendors. The TDCR is not a “solutions center,” though it shares some attributes. Tech Data and its influences/scale place it into the perfect position to have an impact on the cybersecurity skills gap, the cybersecurity education deficit, and security research on vendor technologies and solutions. The Tech Data Cyber Range has three primary missions:

- One, help solve the cybersecurity skills gap by educating a new cybersecurity workforce and upskilling the existing cybersecurity workforce.
- Two, deliver a premiere environment for partners and vendors to host training, recruiting, and social networking events. The Tech Data Cyber Range is an immersive environment staffed by top-level cybersecurity talent and an exceptional level of cybersecurity knowledge.
- Finally, the third goal is to deliver unmatched environments to demonstrate, test, and assess vendor cybersecurity solutions. The very same capability offers our vendors and partners the perfect place to give end-customers a hands-on understanding of their solutions, how they fit into specific environments, and how they perform during cyber incidents.

The Tech Data Cyber Range drives business outcomes through several methods, generating new cybersecurity talent and upskilling existing talent help to give our partners and vendors an edge in the market by delivering cybersecurity competency rapidly into their respective workforces. Our immersive environment helps attendees to gain hands-on skills while also understanding the “why” of cybersecurity.

WHAT MAKES THIS EXPERIENCE SO UNIQUE?
Scott: Tech Data is the first to deliver a cyber range in distribution, and the exclusive relationship Tech Data has with the National Cyber Warfare Foundation ensures it always stays on the cutting edge of cybersecurity. The hands-on nature of the education our attendees receive helps participants gain high-competency quickly while also providing practical skills they will immediately use in the workforce. Unlike yet another computer lab, the Tech Data Cyber Range is an immersive environment that incorporates the most realistic operational setting for our attendees to develop and hone their skills.

As I mentioned earlier, the immersion also fosters a fundamentally deeper understanding of the “why” of cybersecurity. This immersive environment provides an opportunity to offer partners and vendors a deep and memorable experience. The TDCR’s ability to create, replicate and quickly repeat specific network and operating environments enables our partners and vendors to accurately replicate end customer environments or planned environments to allow everyone to understand exactly how things will work with hands-on access. The possibilities are limitless.
WHAT ARE THE KEY BENEFITS TO TECH DATA PARTNERS?

Scott: Partners will benefit from all three of the missions of the Tech Data Cyber Range. The fast and easy access to well-qualified and experienced cybersecurity talent with hands-on skills gives them a significant advantage in the marketplace and reduces their costs to acquire new cybersecurity talent. The use of the Tech Data Cyber Range event space also serves to capture the mindshare of their end customers by inspiring combinations of technologies and high competence of the Tech Data security solutions team. Their end users will have impactful and memorable experiences inside the Cyber Range, and our immersive environment is brand-able to the partner. The partner may utilize the Tech Data Cyber Range for all its possibilities for a fraction of the cost of building one of their own, saving them millions of dollars.

Leveraging the Tech Data Cyber Range’s ability to replicate operating environments will additionally empower the partner to give their end-users a hands-on experience of their company’s offerings. Tech Data Cyber Range delivers a meaningful capability that drives business outcomes, capable of replicating an end customer’s environment to demonstrate or train them on specific offerings from the partner. We can create the partners “optimal” operation environment where end customers can experience what it would be like to implement the partner’s recommendations.

McAfee MVISION Cloud: Cloud Security That Accelerates Business

McAfee® MVISION Cloud protects data and stops threats in the cloud across SaaS, PaaS, and IaaS from a single, cloud-native enforcement point.

Visibility
Gain visibility into all cloud use and data.

Control
Take control over data and cloud activity from any source.

Protection
Protect against cloud threats and misconfiguration.

Key Use Cases
- Enforce data loss prevention (DLP) policies on data in the cloud, in sync with your endpoint DLP.
- Prevent unauthorized sharing of sensitive data to the wrong people.
- Block sync/download of corporate data to personal devices.
- Detect compromised accounts, insider threats, and malware.
- Encrypt cloud data with keys that only you can access.
- Gain visibility into unsanctioned applications and control their functionality.
- Audit for misconfiguration against industry benchmarks and automatically change settings.

For more information, contact our system engineer specialized in McAfee solutions at (800) 553-7921 Ext. 73079. To view McAfee’s full portfolio, visit McAfee’s website.
Unique to Tech Data, the upcoming Digital Practice Builder has been designed to help our partners identify areas of investment and capitalize on today’s exploding security market. Chris DesRosiers, Director, Security Solutions Sales at Tech Data, answered some key questions on this unique service.

HOW DOES TECH DATA’S DIGITAL PRACTICE BUILDER SET OUR PARTNERS UP FOR SUCCESS?
DesRosiers: The Digital Practice Builder was created to help our partners who’re looking to expand into a new market. This online course moves at their pace, teaching them how they can help solve the cyber crisis and position themselves to best serve their customers.

WHAT CAN PARTNERS EXPECT TO GAIN THROUGH TECH DATA’S DIGITAL PRACTICE BUILDER?
DesRosiers: Our partners will learn the specific methodology to building a security business that covers strategy, vendor selection and enablement, marketing best practices, services and GTM sales execution. They’ll experience an acceleration in creating their security business and start growing their revenue as quickly as possible.

WHAT MAKES TECH DATA’S OFFERINGS STAND OUT FROM THE COMPETITION?
DesRosiers: No one else is giving a voice to newer emerging vendors. Through the RECON Security Suite, MSP Catalog and the Tech Data Cyber Range, we provide the services partners want to offer as well as training delivered by qualified cybersecurity professionals not typically found in VADs.

WHAT IS DRIVING THE NEED FOR THESE OFFERINGS?
DesRosiers: The rise of AI will allow focus on more technical elements of cyber careers. Those cyber professionals replaced by AI tools will likely move on to bigger challenges. At many companies, they’ll be retrained in more technical cyber skills to tackle threats from cloud platforms, IoT connectivity and the ransomware epidemic.

Reach out to securityservices@techdata.com for further updates on its availability.
SLACKERS MAKING SAAS SECURITY SLIPPERY?

UNCHECKED SAAS APPS ARE A RISK.

The explosion of SaaS services and applications—like Office 365 and G Suite—help your business operate with unmatched agility and efficiency. But at what cost to security?

SonicWall Cloud App Security (CAS) helps safeguard your growing SaaS landscape and ensures consistent policies across the cloud applications being used. It delivers real-time threat protection against targeted phishing attacks, business email compromise, zero-day threats, data loss and account takeovers—all managed right from a single console.

Visit SonicWall’s website for more information or contact the SonicWall team at sonicwall@techdata.com or 1-800-237-8931, ext. 71433, option 1.
Data Encryption
Data is encrypted using 256-bit AES encryption at rest and Transport Layer Security

Data Wipe
Erase data remotely with time-based policy triggers/on-demand when a device is lost/stolen.

Legal Hold
Comply with legal hold requirements when facing litigation.

Deep Instinct is the first company to apply deep learning to cybersecurity.

Deep learning is inspired by the brain’s ability to learn. Once a brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct’s artificial deep neural network brain learns to prevent any type of cyber threat, its prediction capabilities become instinctive. As a result, any kind of malware—whether it’s known or new—zero-day, ransomware, or APT attacks from any kind, they’re predicted and prevented in zero-time with unmatched accuracy and speed anywhere in the enterprise. Be it endpoint, network, or mobile – Deep Instinct enables multi-layered protection.

To learn more, visit Deep Instinct’s website.

Contact the Tech Data Deep Instinct team at deepinstinctus@techdata.com or 727-539-7429, ext. 73440 to get started.
// CLOUD PRACTICE BUILDER:
YOUR PATH TO BUSINESS TRANSFORMATION

Rapidly and affordably build a profitable cloud practice without the guesswork, cost, ramp-up time or resources to develop in-house expertise. Tech Data’s Cloud Practice Builder offers quality enablement resources and a simple, step-by-step path to making cloud a strategic part of your business model.

HERE’S HOW IT WORKS:
• Assess Your Cloud Capability: Take the pulse of your business in 5-minutes or less
• Unpack Your Results With a Cloud Concierge: Get direction on next steps from your personalized dashboard
• Follow Your Enablement Path: Complete action-oriented sprints to facilitate your transformation

HEAR WHAT OUR PARTNERS ARE SAYING:
Cloud Practice Builder helped us solidify our strategy and go-to-market approach around cloud in a way that was super simple, which is necessary when you run a business in a channel that is complex and constantly evolving. The program helped us understand gaps in our practice and fill in those gaps.
– JUAN FERNANDEZ, VICE PRESIDENT, MANAGED IT SERVICES, IMAGENET CONSULTING

Cloud Practice Builder arrived in the “nick of time” to prepare us for a major opportunity and introduce us to Tech Data’s professional services that proved vital to the project. Today, we feel confident in our abilities and can compete with much bigger national players in our geography and win!
– TOM TAVARES, VICE PRESIDENT, BUSINESS DEVELOPMENT, MICRO TECHNOLOGY SOLUTIONS, INC.

Prepare to embrace the cloud. Get Started.
Questions? Contact us at cloudpracticebuilder@techdata.com.

YOUR APPS ARE EVERYWHERE.
YOUR APP SECURITY SHOULD BE, TOO.

Learn more at f5.com/security

Contact the Tech Data F5 team at F5@techdata.com to get started.
BUILDING YOUR SECURITY BUSINESS WITH

WatchGuard Passport

WatchGuard Passport is a bundle of WatchGuard’s user-focused security services that introduces an entirely new revenue stream for WatchGuard partners. Sold as a single, per-user license, each service provides persistent, always-on protection that travels with the user and delivers the same level of security on- and off-network. Collectively, the services in the Passport Bundle make it possible to:

1. Authenticate people and enforce strong, multi-factor authentication into VPNs, Cloud applications, endpoints and more!
2. Protect them on the internet, block phishing attempts and enforce web surfing policy anywhere, anytime without requiring a VPN.
3. Keep their endpoints free of malware by detecting and killing threats, and related command and control channels.

Take advantage of the Passport Launch promotion and:
• Get an Instant Rebate on your initial purchase of WatchGuard Passport
• Promo purchases will receive the latest product component at no charge (when available)
• Promotion runs through March 30, 2020

For additional details, contact the Tech Data WatchGuard team at sewatchguard@techdata.com.
// POWERFUL PROTECTIONS YOU CAN TRUST

The estimated cost of an average cyberattack climbed 52%, to $1.1 million worldwide, between 2017 and 2018. Companies that detect a breach in less than 100 days can save $1 million compared to those that take longer.

With Windows 10, security events requiring IT remediation are reduced by up to 33%.

**BREACH SECURITY:** DETECT, INVESTIGATE, AND RESPOND
- **21.5 MILLION** Estimated records stolen in one US government breach
- **256** Average number of days required to identify and contain a malicious attack
- **$21,000 PER DAY** to remediate the average government breach

**CUSTOMERS WANT TO STAY SECURE**
Security is the most compelling reason to upgrade to Windows 10.
- The No. 1 reason why users have already upgraded or want to upgrade is to “get to the most secure version of Windows”
- **21% of businesses** reported that they were impacted by a cybersecurity incident, which affected their operations.

**PERCENT OF BUSINESSES IMPACTED, BY SIZE OF BUSINESS**

<table>
<thead>
<tr>
<th>Size of Business</th>
<th>Percent of Businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (10-49 employees)</td>
<td>19%</td>
</tr>
<tr>
<td>Medium (50-249 employees)</td>
<td>28%</td>
</tr>
<tr>
<td>Large (250+ employees)</td>
<td>41%</td>
</tr>
</tbody>
</table>

**BUSINESSES IMPACTED BY CYBERSECURITY INCIDENTS**
EXPERIENCED THE FOLLOWING MAJOR IMPACTS:
- **54%** Prevented employees from carrying out day-to-day work
- **53%** Prevented the use of resources or services
- **32%** Required additional time for employees to respond to incidents
- **30%** Resulted in additional repair or recovery costs

THE FIGHT AGAINST RANSOMWARE: IT’S TIME TO SUIT UP.

Global ransomware costs are expected to reach $20 billion by 2021. Businesses are attacked by ransomware every 14 seconds.

Don’t let your business be next.

Leverage the StorageCraft Ransomware Recovery Solution:

- **ShadowXafe** - Next-generation data protection
- **Cloud Services** - True DRaaS via a purpose-built cloud
- **OneXafe** - Intelligent data platform unifying data protection with scale-out storage

To get started, visit www.storagecraft.com/ransomware. For more information send an email to storagecraft@techdata.com or contact us at (800) 237-8931, ext. 71458.
Go beyond endpoint detection and response with Trend Micro XDR, which is the first cross-environment detection and response solution to collect and correlate data across email, endpoint, servers, cloud workloads, and networks—enabling visibility and analysis that’s difficult to achieve otherwise.

For more information, contact the Tech Data Trend Micro team at trendmicro@techdata.com or 727-539-7429, ext. 82135.

SUSE, the world’s largest independent open source company, powers digital transformation with agile, enterprise-grade open source solutions.

Collaborating with partners, communities and customers, SUSE delivers and supports enterprise-grade Linux, software-defined infrastructure and application delivery solutions to create, deploy and manage workloads with exceptional service, value and flexibility.

For more information, contact the Tech Data SUSE Team at suse@techdata.com or 727-593-7429, ext. 84344.
DISCOVER WHY FORTINET SECURE SD-WAN IS THE RIGHT CHOICE

Many organizations are in the midst of digital transformation (DX) initiatives, seeking to replace their outdated wide-area network (WAN) infrastructures. The high cost and complexities of reliable wide-area connectivity over traditional carrier-based networks is driving most decision-makers toward some form of software-defined wide-area networking (SD-WAN).

Fortinet is positioned to deliver a Secure SD-WAN solution that includes both networking and security capabilities in a unified solution. Fortinet Secure SD-WAN supports application performance, consolidated management, and advanced protection against threats.

To learn more, visit the Fortinet SD WAN HUB https://partnerportal.fortinet.com/prm/English/c/sd-wan-home

Contact the Tech Data Fortinet team at Uspmfortinet@techdata.com, or 1-800-237-8931 x 64216, option 1, to get started.