Today’s Cyber-security Landscape

What every MSP needs to know.

Richard Parker,
Tech Data Cloud,
Business Development Manager

Richard is a 20+ year veteran in the IT Distribution Channel. He works with vendor partners and MSP to assist with their journey to the cloud.

It seems like everyone is offering cloud services of every flavor these days, with new players joining the market every day. Over the past 10 years, we've seen cloud-based storage, email migration; remote monitoring, online productivity, and cloud security take center stage. Managed Service Providers (MSPs) are trusted with securing organizations' networks. However, many do not fully understand their own customers' priorities when it comes to security.

As the IT industry continues to evolve, more security threats are emerging each day and we are seeing our private and personal data at risk of data breaches. Is the cloud secure? Companies that allow employees to use their network to visit social media websites are opening themselves up to cybersecurity risks.

With more enterprises moving their business technology systems to the cloud—and moving away from on-premises—it only makes sense that security delivered as cloud services would follow suit. Yes, the on-premises security market is still growing, but we are seeing accelerating growth of cloud-based security services. According to Business Wire, the global Managed Security Services (MSS) market is estimated to grow from $14.32 billion in 2014 to $31.86 billion by 2019.

Cloud-based security is indeed taking off. For most partners, it's about ease of deployment and management. There's no need to maintain on-premises equipment for customer websites that require expertise to operate—updating security software and keeping logs, while monitoring intrusion detection, prevision systems and firewalls requires skills that are increasingly more difficult to hire. Cloud security solutions are removing that burden and, therefore, lowering operating costs.

Security is and should be a top priority for enterprises and end users. Continue to read how top security vendors are positioning themselves to assist MSPs to help them keep ahead of threats and keep their customer's information safe.

www.ExperienceTechDataCloud.com

Barracuda

David McAlister
Sr. Manager
Distribution Channel Sales

David McAlister has been with Barracuda for seven years. David's team is focused on taking care of all Barracuda partners and recruiting new partners to the company.

"We're in the golden age of network security. Not long ago, a customer's network security might have been limited to a firewall, email security, or an entry-level web security solution.

Barracuda's product line has grown from an increased need for security, and the need to secure all points of entry into a customer's network. This includes next-generation firewalls, enhanced email security with encryption, web security, secure VPN connections, and protection for web facing assets via a web application firewall.

We call this solution the "Total Threat Protection," a family of network security products with multiple deployment options, including traditional hardware appliances, virtual appliances and cloud (including AWS & Azure), which are all manageable via our Cloud Control Center."

https://www.barracuda.com/

BROCADE

Jess Bennett
Sr. National Account Manager

Jess has over 20 years of IT experience, helping Strategic Solution Providers build technology practices focused on business outcomes.

"The need to keep information secure will become a $170 billion business in the next four years, and it's easy to understand why.

Last Summer, the U.S. Federal Government had a security breach that exposed the personal information, such as finger prints and financial information, of anyone who submitted to a background check in the last 15 years. Last year, a group hacked the extramarital affairs website, Ashley Madison, exposing personal details of members to the public.

There are two types of IT security managers today: Those that have been hacked, and those that don't yet realize they've been hacked. The legacy network infrastructure, based on architecture that hasn't changed in 20 years, cannot keep up. IT security starts with updating the network to multi-vendor solutions with technology from this century. Gartner has recognized Brocade as a visionary in the future of the Software-Defined Network, with our MLX product line ready for deployment. Many vendors offer security or network performance, but Brocade can do both."

https://www.brocade.com

Thomas Soricelli
Distribution Account Manager

Thomas Soricelli has spent the majority of his career in the technology industry, and over 15 years with Symantec. His focus has ranged from the consumer business unit to managing one of the largest distributors.

Symantec is the global overall market leader in endpoint security, email security, data loss prevention and SSL certificates

"Symantec sees more threats and protects more customers from the next generation of attacks. We are dedicated to developing industry-leading technologies and focused on providing the very best security products. We create simple and easy programs that provide enhanced incentives for partners selling Symantec products, and we have a new cloud program coming soon."

"Last year, we saw 317 million new malware variants, with targeted attacks and zero-day threats at an all-time high. Organizations are struggling to keep up with the rapidly evolving threats. Symantec Endpoint Protection, backed by industry-leading security intelligence, is designed to protect against advanced threats with powerful, layered protection."

www.symantec.com

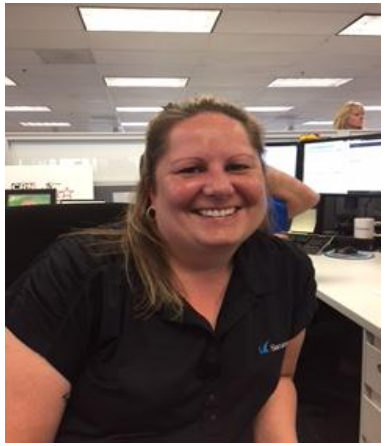
Lamon Gormon,
Service Provider Manager

Lamon help managed service providers (MSPs) develop successful lines of business focused on managed security services. Through eight years of industry experience, he focuses on both MSPs and those just making the business transformation.

“Security is often the “anchor” that many transitioning to the managed service provider (MSP) model build their managed service offerings around. Security is often a top priority for small and medium-sized businesses (SMBs) today, thanks to the rampant spread of Ransomware. Today, building your offering around security is the fastest way start your transition. In most cases, VARs are already selling security, installing it and fixing it when something breaks, so it is a natural progression to create a managed service around it. Trend Micro is not only a leader in the security space, but also has a very mature MSP program.

The Trend Micro MSP program is perfect for those who are just transitioning to the MSP model (or those who have already transitioned) as we provide a flexible pay-as-you-go monthly licensing model, aggregate pricing, and tools specifically for MSPs. Specifically, we provide a cloud-based eco-system of tools for instant licensing and multi-tenant product management. This combination allows our MSP partners to improve operational processes, which increases their productivity and profitability.”

Want to learn more how Trend Micro can help you make the transition? www.trendmicro.com



Cynthia Klocke,
Distribution Sales Rep

A five year veteran of Barracuda Networks, Cynthia bring her knowledge of Inside Channel, Renewals and Channel Development to the Barracuda team at Tech Data.

"As customers migrate to the cloud, it's important that their security solutions go with them. Our newest key initiative at Barracuda is supporting our customers transitioning to the cloud, especially those moving to Office 365. Barracuda Essentials provides critical multi-layer security, archiving, and backup for Office 365. The program allows organizations to prepare, migrate, and operate faster, safer, and more efficiently in Office 365. Barracuda Essentials gives customers peace of mind and complete protection of their email, data, and cloud infrastructures.

The modern network includes a combination of local servers, remote devices, and cloud-hosted applications. If you use cloud-based platforms such as Office 365, Salesforce, Amazon Web Services (AWS), and Microsoft Azure, you need to ensure that all of your critical applications and devices are available when needed and secured. Barracuda Next-Generation Firewalls are purpose-built for the modern, distributed network in which performance and availability is as important as security. Unlike traditional port-based firewalls, our firewalls are application-aware, enabling you to regulate application usage and intelligently prioritize network traffic.

https://www.barracuda.com/

Jeff Confarotta
Director, Channel Sales

Daron Benbenisti
Partner Executive

Micro Focus is one company operating two product portfolios, namely Micro Focus and SUSE. The Micro Focus portfolio is a grouping of the Attachmate, Novell, NetIQ, Borland, and Micro Focus products, and the SUSE portfolio encompasses value-added commercial open-source solutions for enterprise customers.

Micro Focus' access management products provide customers with convenient system access, single sign-on, multi-factor authentication, least privileged access, and access review from any device anywhere in the world. CloudAccess is our integrated identity and access management (IAM) solution that provides simple single sign-on and account management. We make it easier for organizations to secure and manage access to important applications—cloud-based, internal web-based, and even mobile apps.

www.microfocus.com

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest privately-owned cybersecuirty company. We operate in 200 countries and territories and have 37 offices in 32 countries. Nearly 3,300 highly-qualified specialists work for Kaspersky Lab.

A survey from Kaspersky Lab has found that almost three quarters (73%) of companies are relying on standard endpoint security-class solutions to protect their virtual environments, which could lead to reduced performance and overload systems. A third of businesses (34%) remain unaware that specialized security products exist. In using endpoint security-class solutions on virtual machines, a number of issues can arise. For example, anti-malware scanning and updating databases on multiple machines simultaneously can have a negative effect on the quality of service, overload infrastructure, or even lead to service failure.

"We believe that everyone – from home computer users to large corporations and governments – should be able to protect what matters to them most. Whether its privacy, family, finances, customers, business success, or critical infrastructure, we've made it our mission to secure it all. We succeed in this by delivering security expertise, working closely with international organizations, and law enforcement agencies to fight cybercriminals, as well as developing technologies, solutions, and services that help you stay safe from all the cyberthreats out there."

Eugene Kaspersky, Chairman and CEO of Kaspersky Lab

Alex Paunic
Distribution Account Manager
Intel Security

Based in St. Petersburg, Florida, Alex is responsible for building accelerated growth through sales, marketing, and operational support at Tech Data. His team focuses on enabling Tech Data representatives and partners to embrace the threat defense lifecycle solution methodology.

***Intel Security is poised to do things no one else can do**. We are the one player in the industry that covers the entire IT environment: the endpoint, the network, and the data center, with the right level of management and analytics capabilities to bring it all together.*

Our customers and partners can expect Intel Security to address the rapidly evolving threat landscape with a portfolio of products and services that can meet their security needs, from device to datacenter.

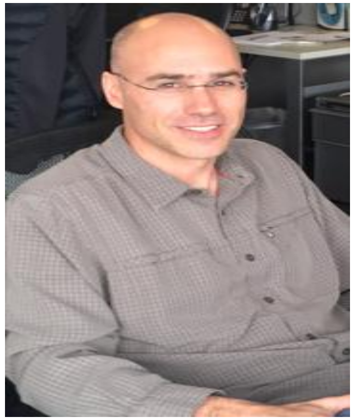
Our valued partners have the opportunity to work with us to provide comprehensive end-to-end solutions for their companies and their customers.

*Whether it's securing nodes and big data with our enterprise solutions, or protecting employees personal devices at home, we can be your **one** security partner, truly protecting your professional and personal lives.*

Wherever you are, whenever you connect, and whichever device you use, Intel Security is there.

Questions? Contact your TD Catalyst Team at 1.800.237.8931 ext.73519 or IntelSecurity@techdata.com

WEBROOT



Phillip Seigenfield
Distribution Manager

Phillip Seigenfeld is responsible for all channel distribution in North America. Seigenfeld brings over 18 years of technology industry and sales experience. He has been with Webroot for 12 years, holding numerous positions and is well versed in security and cloud solutions.

“In the twelve years I’ve worked for Webroot the increase in cyberthreats, malware, and security breaches has been dramatic. Our threat intelligence researchers detect 25,000 new malicious URLS, 100,000 new malicious IPs, and 101,000 new malware and PUAs on a daily basis. With threats like crypto-ransomware becoming more sophisticated, 2016 is going to be a busy year.

Webroot’s next-generation endpoint security solutions (the SecureAnywhere line of products), powered by our Threat Intelligence Platform, monitor behaviors, not signatures. This allows us to identify threats as they occur, and continually process and analyze the information to create predictive behavioral determinations on malware instantly and with high accuracy. In this rapidly changing landscape, Webroot offers its partners a powerful, cloud-based solution against real-time threats, with less than 1MB presence, agent user performance won’t be impacted.”

www.webroot.com

TechData Cloud

Benjamin David,
Distribution Account Manager

Benjamin David is responsible for Check Point's SMB and Enterprise Security channels focusing on the recruitment and enablement of security partners in the Check Point STARS program.

"In 2016, networks will be more vulnerable than ever. With the growth of the Internet of Things (IoT), cloud, and mobile technologies, IT environments are more open and less controlled. Malware is evolving fast and it's targeting these open environments with new threats, new techniques, new actors, and new targets. The biggest challenge for businesses will be how to make the best possible decision for the business, without compromising security.

Most security technologies work retroactively, remediating after malware has hit the network. Check Point believes in security that is proactive, focusing on preventing network attacks before they happen. With a suite of security products designed for the network, mobile, and cloud environments, Check Point is a recognized leader in the Gartner Magic Quadrant and in independent testing from NSS Labs."

http://info.techdata.com/checkpoint-c

Tech Data's Security Solutions cover all endpoints and everything in between. We've closed the loop on security technologies and will provide you with the tools and services you need to make your security business the most profitable. There's a newfound preoccupation with security and it's not too surprising. Companies are facing increased threats from cyber attacks, lost devices, and the loss of confidential or proprietary data such as bank account numbers, credit card information, and customer and employee records. Whether it's due to a malware attack, a server crash, or a stolen mobile device, lost information can be highly detrimental, if not fatal.

NEXT STEPS

Contact our Tech Data specialists and get ready to have new conversations with your customers to create and deliver a strong foundation you need to ensure success.

☎ 800-237-8931

✉ tdcloud@techdata.com

@tech_data

🖥 www.techdata.com

Tech Data
TD Cloud