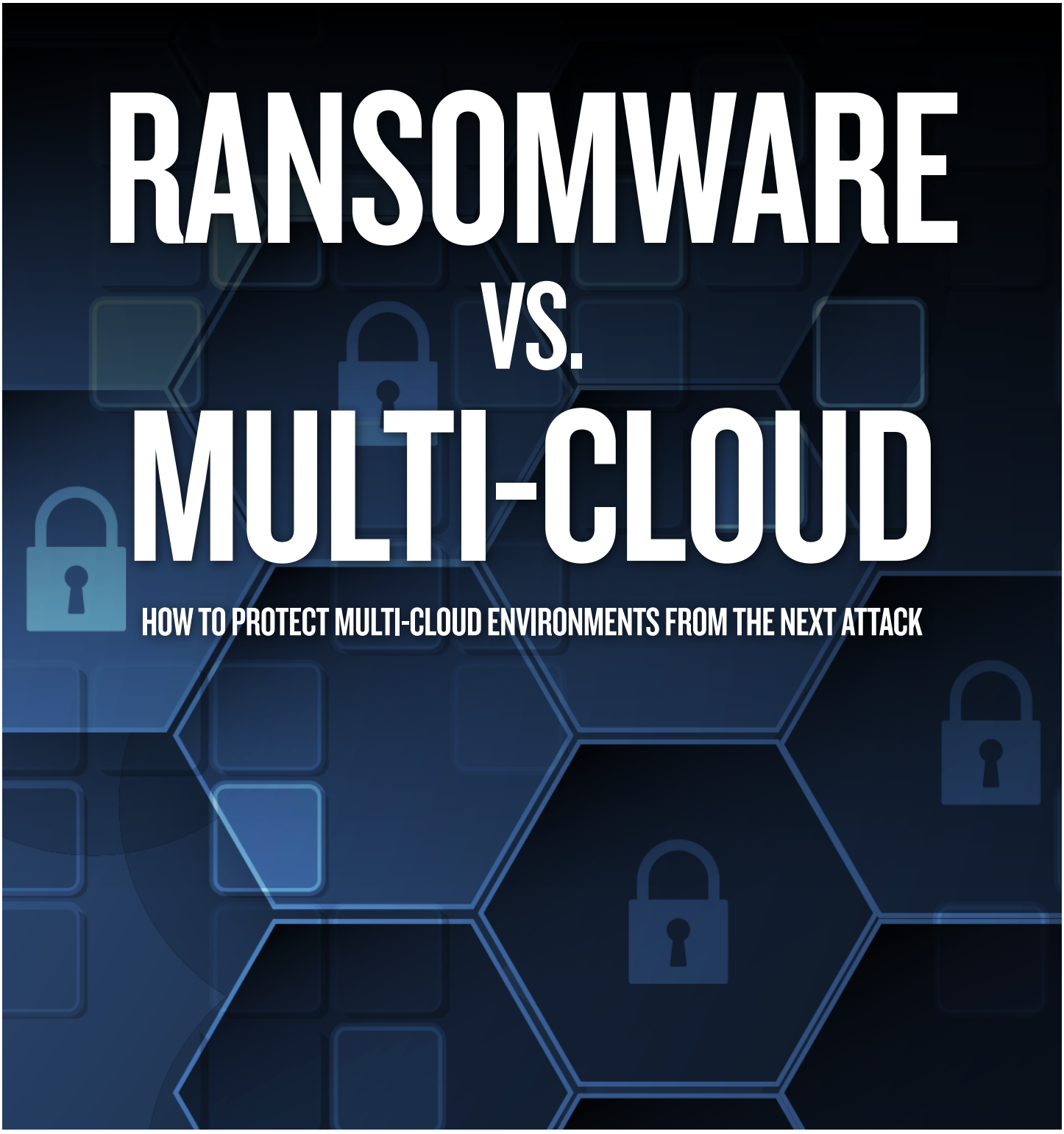

ebook

An SC Media publication

Sponsored by

vmware®

A growing attack surface

Ransomware gangs are doubling down on attacks against multi-cloud environments. Bob Violino explores the threat and offers guidance for a more ironclad defense.

The scale and economics of the cloud are a boon for today's enterprises, enabling them to move applications and data out of on-premises data centers and into multi-cloud environments as needed. The public cloud is delivering unprecedented flexibility at a time when agility is nearly essential to business success.

But the trend comes with a dark side. The multi-cloud environment has greatly expanded threat surfaces, putting organizations at greater risk of devastating attacks such as ransomware.

This report explores how companies can move beyond segmentation inside the data center and traditional next-generation firewalls at the perimeter, to build a defense that more effectively meets the special demands of a multi-cloud environment.

OUR EXPERTS: Ransomware vs. multi-cloud

Andrew Topp: Director, cloud and infrastructure, West Monroe

Bruce Young: Head of cybersecurity operations, Harrisburg University of Science and Technology

Matthew Rogers: Global chief information security officer, Syntax

Christopher Rence: President and CEO, Rimage

Mandy Andress: Chief information security officer, Elastic

Multi-cloud defined

Multi-cloud is a model of cloud computing where an organization utilizes a combination of clouds, which can be two or more public clouds, two or more private clouds, or a combination of both public and private clouds.

It is the superset of multiple public cloud, hybrid, on-premises, and edge. A multi-cloud deployment model relies on the use of more than one public cloud service provider for computing or storage resources, independent of the use of other private cloud or on-premises infrastructure. A multi-cloud deployment that includes private cloud or on-premises infrastructure is considered a hybrid multi-cloud.

A multi-cloud strategy not only provides more flexibility for which cloud services an enterprise chooses to use, it also reduces dependence on a single cloud hosting provider.

There are several reasons to adopt a multi-cloud platform, including:

Provider-specific services: Organizations can choose from different cloud providers to best fit specific application and infrastructure requirements to their own unique business needs.

Enhanced scalability: An enterprise can quickly scale to multiple cloud providers as demand increases.

Containers and microservices: Organizations that utilize microservices when developing containerized applications with Kubernetes may find that some services are only available from a specific cloud provider. Multi-cloud Kubernetes deployments are increasingly popular as new services come onto the market, hosted by a variety of cloud providers.

Reduced latency: Dispersed organizations can reduce latency by choosing local public cloud vendors based on each facility location. This also facilitates multi-cloud networking, since all major cloud providers are connected to each other with fast, low-latency connectivity.

Regulatory and governance mandates: Some organizations may need to use

multiple cloud storage providers to adhere to government regulations and data sovereignty laws that require certain types of data to reside within specific geographies.

Reduced footprint and lower costs: Most organizations that employ multi-cloud capabilities use the public cloud for infrastructure, avoiding the need to build and maintain their own datacenter and in effect building a virtual data center in the cloud without needing a physical piece of hardware. This saves money and physical space, because the company does not have to invest in or store their own hardware. It also saves time, because the public cloud service provider manages, maintains and updates the data center.

Bruce Young: Head of cybersecurity operations, Harrisburg University of Science and Technology

Bargaining power: Opting for multiple cloud services provides benefits beyond spreading the risk of failure across several vendors.

By adopting a multi-cloud strategy, businesses can pick and choose the provider offering the best price for a given service, thus helping ensure that all providers continue to competitively price their offerings.

With those benefits in mind, companies are rapidly expanding their multi-cloud footprint. Attackers have taken notice and are increasingly targeting multi-cloud vulnerabilities with ransomware.

The growing ransomware threat

Ransomware is a threat to any environment, whether it's on-premises, single-cloud or multi-cloud, says Andrew Topp, director of cloud and infrastructure at consulting firm West Monroe.

"If an attacker gains entry and obtains access to a privileged credential, they can move freely within the environment to exfiltrate data, destroy backups, and encrypt data to hold an organization at ransom," Topp says. "If there are Windows systems running in the cloud, or if an attacker gains access to cloud systems or cloud management portals using their compromised credentials, then those services can be attacked like traditional on-premises systems."

Although ransomware might be a threat regardless of the computing environment, expanding the number of cloud services in use can significantly increase risk.

"Most organizations utilize more than one cloud environment," says Bruce Young, who heads the Cybersecurity Operations and Control Management operation at Harrisburg University of Science and Technology. And the use of multi-cloud environments "means that data and systems are distributed and ultimately more exposed to be compromised by ransomware," he says.

Deploying multi-cloud environments means security controls must exist consistently across those environments, Young says. "If the deployment of security controls is inconsistent, gaps exist that may lead to a security breach," he says.

Bad actors not only attack cloud environments, but use the cloud to conduct malicious activity, Young says. "The cloud service design is for easy system provisioning," he says. "All you need is a stolen credit card number. Bad actors can then use the computing resources to launch phishing campaigns, attack computer systems, crack passwords, or create advanced persistent threats [against] compromised systems."

Cyber criminals will use compromised cloud environments to perform the same nefarious activities to launch ransomware

attacks on other organizations, Young says.

"Most organizations recognize the digital transformation to the cloud, utilizing multiple cloud service providers creating multi-cloud environments," Young says. "The digital transformation produces a very distributed and easily accessible computing environment. However, if organizations do not include cyber security architecture into the design of a cloud environment, gaps will exist, exposing systems and information to compromise."

Christopher Rence: President and CEO, Rimage

A big risk with using multiple cloud services is that organizations can lose sight of the importance of protecting data.

"Many organizations that migrate their onsite data storage facilities to the cloud quickly fall prey to the age-old adage, 'out of sight, out of mind,'" says Matthew Rogers, global CISO at enterprise software provider Syntax. In multi-cloud environments, lots of assumptions are made, such as "the data is safe because it's not hosted here, or it's safer because it is somewhere else," he says.

What's particularly concerning is that in a multi-cloud environment, many companies simply don't have a handle on where their applications and data are at a given time.

Recently, Christopher Rence, former security and risk executive at a financial services firm and now president and CEO of optical disc hardware maker Rimage, met with a large company to discuss its multi-cloud strategy.

"In general, they did not have one," Rence says, and this presents all kinds of potential security issues. "They need to understand what they have, who can add and subtract apps or services, and how they are connected into their environment," he says. "It was a very eye-opening discussion, and they are not alone as they made the assumption that the cloud provides layers of security and process by default."

Building a multi-cloud defense

To better protect themselves against ransomware in a multi-cloud environment, organizations need to move beyond tactics such as segmentation inside the data center and relying on traditional next-generation firewalls at the perimeter.

Organizations that use multiple cloud environments must create a security architecture that ensures the protection of systems and data not only on premises but in the cloud, as well, Young says.

"Building a defense for a multi-cloud environment, an organization starts with identifying the current security controls implemented to protect the data and systems of the on-premises [infrastructure], and then recognizes the security controls required to operate in a cloud environment," Young says.

The cloud environment security architecture includes an understanding of the "boundary of responsibility," Young says.

> "Implementing a public key infrastructure environment is essential, including key management, to ensure the security of the data in the cloud."
>
> *– Bruce Young: Head of cybersecurity operations, Harrisburg University of Science and Technology*

"The boundary of responsibility defines the security controls implemented by the cloud service provider and the security controls that are the responsibility of the customer/consumer," he says.

One particular security control that is critical when using a cloud environment is encryption, for data at rest and in transit, Young says. "Implementing a public key infrastructure environment is essential, including key management, to ensure the security of the data in the cloud," he says.

Andrew Topp: Director, cloud and infrastructure, West Monroe

In general, defending against ransomware requires a defense-in-depth cyber security strategy, and that includes the cloud. "A defense-in-depth approach is designed to meet the organization's cyber security requirements," Young says. "The organization identifies cyber security requirements by performing a risk assessment."

However, there are specific security controls that defend against ransomware, Young says. This includes:

- Multi-factor authentication (MFA)
- Firewall
- Network detection and response (NDR)
- Endpoint detection and response (EDR)
- Security incident and event management (SIEM), and
- Cloud access security brokers (CASBs).

"Access control is a critical security function for an organization utilizing cloud services or defending an on-premises environment, including any user access exposed to the internet," Young says. "Using MFA as a user access control is an additional security control layer to defend against a ransomware attack launched through an advanced persistent threat."

Firewall functionality now includes intrusion detection and prevention, application-layer functionality, the ability to receive online threat notifications; and the ability to identify malicious web content sites and proxy systems, in addition to the traditional firewall services, Young says.

A key component of network security, Network Detection & Response (NDR) comprises a varying set of complementary network security technologies that together seek to automatically monitor, detect, analyze, and respond to sophisticated cyber threats.

Often including network traffic analysis, IDS/IPS, and advanced threat analysis, NDR solutions give security teams real-time visibility and awareness over network traffic and the ability to respond quickly to perceived threats.

EDR, unlike traditional anti-virus software, provides the capability to detect and respond to malware including ransomware. But a significant difference between EDR and traditional anti-virus software is that EDR is heuristics-based as opposed to signature-based. "Heuristics means that the underlying technology is developed based on mathematical algorithms and machine learning," Young says. "Most EDR solutions can detect malware, APT [advanced persistent threat] attacks, and zero-day vulnerabilities."

> "Segmentation between environments in the cloud using different accounts, authentication realms, and connectivity can also significantly limit the scope of a compromise."
>
> *– Andrew Topp: Director, cloud and infrastructure, West Monroe*

A SIEM application has become a critical component for any organization's defense-in-depth security strategy, Young says.

Most SIEM solutions offer two significant functions, centralized log collection for networked devices and an event correlation

engine, he says. A SIEM provides the ability to configure alerts and notifications of detected events and malicious system activities from other security controls.

CASB is the security control that bridges the gap between the on-premises environment and cloud services. "Usually that gap is the internet, but it also may include private circuits an organization has directly with a cloud service provider," Young says.

Segmenting clouds

If cloud environments represent "production" or "product" environments, companies should consider segmenting them at the credential and connectivity level from other environments, Topp says.

Using separate authentication domains or not providing persistent connectivity between on-premises and the cloud environments means that the scope of the damage will be naturally limited," Topp says. "Segmentation between environments in the cloud using different accounts, authentication realms, and connectivity can also significantly limit the scope of a compromise.

Organizations should ensure that administrative accounts for cloud management portals are not synchronized from an on-premises Active Directory or other identification environment, Topp says. West Monroe has seen many instances where an easily compromised administrator account from an external authentication domain is used to manipulate an otherwise disconnected cloud environment.

"Along the same lines, do not exclude 'trusted' network ranges from MFA [multi-factor authentication] or other compliance requirements for administrative accounts," Topp says. "Attackers are not above logging into cloud environments from a bastion in the client's physical office, allowing them to bypass MFA when such exclusions are in place."

Micro-segmentation or virtual containerization is an effective way to understand the data flows through cloud environments, says Mandy Andress, chief information security officer of Elastic, a provider of online search tools. "It allows teams to divide their cloud environment or data center into distinct security segments and isolate workloads from one another, and then define security controls that limit network traffic between each unique segment," she says.

At a policy level, organizations should reinforce with employees the danger of configuring "permissive" privileges or connectivity to cloud systems during development or troubleshooting work, Topp says.

"It's far easier for a cloud system to be exposed to the internet inappropriately," Topp says. "Inadvertently exposed systems can act as the entry point for an attacker, who may pivot from environment to environment if connectivity and permissions allow. Where possible, segment roles so that a single user cannot both provision a new system or service and allow connectivity to it."

> "Understanding your shared-responsibility model is extremely important when it comes to ransomware defense, especially in the context of multi-cloud environments where responsibilities can vary across service providers."
>
> *– Mandy Andress: Chief information security officer, Elastic*

At all times, organizations need to guard against being complacent about ransomware protection and watch for the early warning signs.

"Ransomware is a sub-component of an attacker's campaign on an entity," Rogers says. "This means that it is not the beginning of an attack, it's the end. Ransomware is

the completion of the event in most cases. There are typically alarms and indications of cybersecurity problems long before ransomware events start."

Organizations will always have security events to deal with, Rogers says, "but the time it takes a team to respond will determine if you can contain the blast radius to a few systems or thousands. An aware, accountable security organization should be proactive and respond quickly to indicators and alarms."

Mandy Andress: Chief information security officer, Elastic

A shared responsibility

Organizations that use cloud services understand — or should — that security is a shared responsibility of the customer and the cloud provider. Defending against ransomware and other threats requires a clear understanding of what their responsibilities are as opposed to those of the service providers.

"Understanding your shared-responsibility model is extremely important when it comes to ransomware defense, especially in the context of multi-cloud environments where responsibilities can vary across service providers," Andress says. "If you lack clarity around your specific responsibilities — which can often happen within organizations that are new to using cloud environments — your defensive posture can weaken because you'll likely overlook a critical security gap that could allow malicious actors into your environment."

While cloud providers "certainly bear the brunt of infrastructure security responsibility, they're not responsible for protecting data within the cloud," Rogers says. "This may sound illogical to the companies using cloud providers, but the cloud shared responsibility model delineates security obligations between both parties."

In this model, cloud providers are responsible for securing cloud infrastructure, including hardware, software, networking, and facilities, Rogers says. "Cloud customers, on the other hand, are responsible for securing the data they put in the cloud, which includes endpoints, accounts, and access management."

When using cloud service providers, "it is essential to understand the concept of boundary of responsibility," Young says. "The boundary of responsibility regarding security controls defines which controls are implemented by the [cloud providers] and which rules should be implemented by the organization."

The boundary is also determined by the type of cloud service. "Each type of service will define different levels of responsibility for security controls," Young says. "The organization consuming cloud services must understand the contractual agreement of the [providers'] security controls to ensure it meets compliance requirements."

To ensure the protection to defend against ransomware, organizations need to understand how or if the security controls are implemented, and who is responsible for the administration of the security controls.

"Many organizations assume that migrating to the cloud shifts the burden for backup and disaster recovery to that cloud provider," Topp says. "However, that is often not the case, and the misunderstanding can often cost time during a recovery or even lead to lost data due to incomplete backups."

For infrastructure-as-a-service (IaaS) virtual machines, "the migrated systems may be much easier to protect using readily available regional replication and cloud backup offerings, but that functionality is not automatically in place and the provider

typically has no native obligation for providing backup" Topp says.

Also, it's the customer's responsibility to bring a recovered system back online. "The troubleshooting and administrative effort of recovering from an attack or disaster will fall to the customer, not the provider, and plans need to be in place that cover the cloud IaaS environment like it's a piece of traditional infrastructure," Topp says.

Platform-as-a-service (PaaS) services have varying levels of backup and disaster recovery available, Topp says. "There are some where customers need to configure replication or schedule backups," he says. "Others include automatic replication between regions or automatic backups on a set schedule. Customers need to understand what schedules and options are available to be sure that either the default configurations or the functionality offered will meet recovery time and point objectives during recovery."

Companies also need to understand the interaction between these services and others, Topp adds. "For example, if a set of IaaS Windows VMs are encrypted and must be recovered to an alternate cloud region, what does that mean for an unimpacted PaaS database those servers rely on?" he says. "Can it be accessed cross region without impactful performance penalties? Understanding the dependencies between different tiers of services is critical during the recovery process."

Software-as-a-service (SaaS) offerings shift most backup and recovery burden to the provider, Topp says. "Customers can ensure configurations are correct for backup frequency, the duration backups are kept, and the ability for end users to self-service," he says.

Security for the modern digital business

Cybersecurity programs are nothing like they were even a few years ago, before the broad moves to the cloud that many organizations have experienced. Operating multiple cloud services has become commonplace — and a security risk.

"The bad actors are always looking for [opportunities] that they can exploit," Rence says. "With all the remote workers leveraging different paths to your network, these vulnerabilities exist."

Sticking with legacy tools might not protect organizations against attacks such as ransomware. That doesn't mean everything needs to be changed, but enterprises do need to step up their security efforts.

"Organizations need to get better at basic security hygiene and understanding how to leverage the existing security capabilities that are built into their operating systems or provided within their cloud environments," Andress says. "Security teams don't always have to rely on various external tools and technologies to effectively defend their environments."

They do need to rethink how they provide security, however, so they can protect their organizations against attacks such as ransomware and thrive in a cloud-based business environment. ■

For more information about ebooks from SC Media, *please contact Bill Brenner, VP, content strategy, at bill.brenner@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

Sponsor

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control.

With VMware Cross-Cloud™ services and our global ecosystem of partners, we deliver the smartest path to cloud, edge and app modernization. Customers gain multi-cloud autonomy and consistent operations while creating a more secure, frictionless experience for their distributed workforce.

As the trusted foundation to accelerate innovation, VMware gives businesses the freedom and flexibility they need to build the future.

More information is available at www.vmware.com

Masthead

EDITORIAL
VP, CONTENT STRATEGY
Bill Brenner
bill.brenner@cyberriskalliance.com
PROJECTS MANAGER
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER
Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
VP, SALES
Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*

The Strongest Defense

for Your Multi-Cloud Network

Workloads protected by VMware are safest.
Public Cloud. Private Cloud. **Any Cloud.**

LEARN MORE

SE Labs
INTELLIGENCE-LED TESTING
BEST
Network Detection & Response
WINNER 2021
VMware
vmware

SE Labs
AAA
AUGUST 2021
Network Detection & Response
VMware NSX Network Detection and Response

Industry's First and Best
AAA-certified Advanced NDR

vmware®