



VMsources Group Inc.

Intelligent Information Security

A Comprehensive Approach
to security for Organizations

Agenda

- The Challenges
- “Where's the Beef?”
- Identify the Challenges
- Intelligent Information Security: Prevention, Remediation, Training (PRT)
 - **Prevention** – Preventing issues before they happen , utilizing active technologies to stop hackers before they hit gold
 - **Remediation** -- Being able to recover quickly & quietly when events do happen
 - **Training** – Educating users to avoid malware
- Secure Cloud Computing
 - VMsources Secure Multicloud

The Challenges



Ransomware

Network and security flaws allow Ransomware to spread through an Organization like fire



Theft

Hackers are using new attack vectors to steal Organizational data and demand payments



Identity Verification

Organizations encourage bad security by using obsolete policies and authentication methods



Phishing

Lack of active filters subject users to sophisticated phishing emails on a daily basis

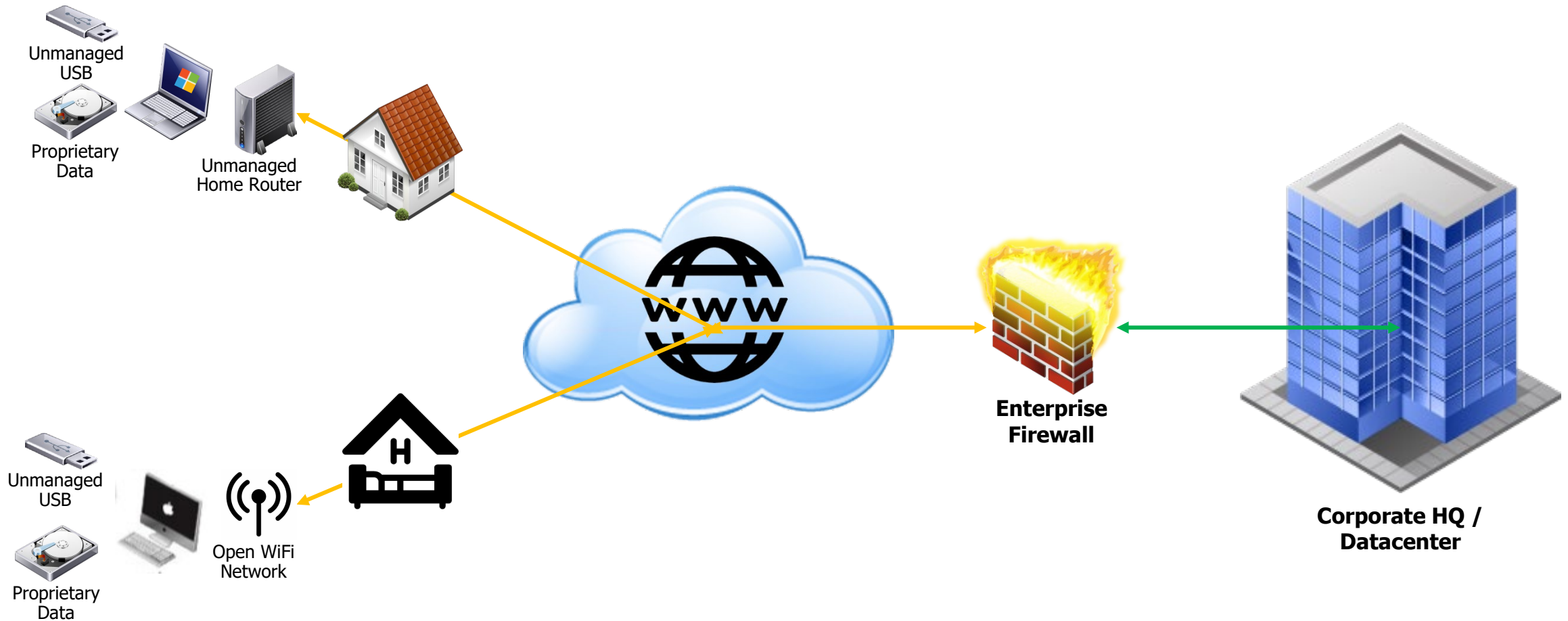


Business Continuity

Many Organizations are unprepared to rapidly remediate Ransomware or failover in a disaster

Where's the beef?

The "*beef*" is your organization's proprietary data and work product, and it needs to be protected and secure



Ransomware

Networking is often the problem

- Ransomware is becoming more sophisticated.
 - Increased use of VPNs for remote users from unsecured networks has opened the door
 - Brute-force password and remote code execution are common vectors
 - Lack of network segmentation allows propagation.
- Recent front-page events like the Pipeline shutdown were the result of an insecure VPN
 - This event could have been prevented by following the recommendations we are going to present here



Theft

New challenges for your Organization

- Hackers used to disrupt Business Continuity and seek ransom payment
- Now hackers also steal Organizational data and seek ransom payment(s) to not release the data
 - Obviously, there's no guarantee that they won't keep coming back



Digital Identity

A username and a password are not enough anymore!

- Bad password policies leave Organizations vulnerable
 - Password policies should comply with: [NIST Digital Identity Guidelines 800-63-3](#)
- Brute-force attacks without additional verification allow hackers directly onto proprietary systems
- Users often leave workstations unlocked
- It is common practice to share user accounts and passwords in order “to get it done”



Phishing

It's not all about deploying payloads anymore

- Hackers are developing more sophisticated Phishing attacks all the time
- It used to be all about delivering a Ransomware payload
- Now, Phishing attacks often identify key players in an organization for specifically target attacks:
 - Phishing from "customer" to AR at your Organization: "Please send future ACH transfers to this new address"
 - Phishing from "employee" to payroll at your Organization: "I changed banks, please send my paycheck..."
 - Phishing from "court" to payroll at your Organization: "John Q. Public is in default, direct 50% of paycheck to..."



Business Continuity

Read All About It...

- Ransomware events are likely to occur, even with the best protections in place
- The key is in being able to recover quickly & quietly, without having to pay ransom
- Avoid significant disruptions to Business Continuity
- Don't let you or your Organization become headline news!



Staying Safe

A Simple, affordable Protection plan

1. Use MFA to prevent false logins
2. Comply with the 3-2-1 Rule
 1. Three copies of backups
 2. On at least two different destinations
 3. At least one copy is remote or in the Cloud
3. Verify passwords, especially local device and service passwords
 1. Comply with: [NIST Digital Identity Guidelines 800-63-3](#)
4. Use Endpoint protection
 1. We recommend Microsoft Defender Endpoint at minimum

"Insanity is doing the same thing over and over and expecting different results."
-Albert Einstein

Intelligent Information Security -- PRT

Prevention, Remediation, Training

TPR – The foundations of Business Continuity

There is an opportunity for success



Training

Educate your users and continually test their awareness to emerging threats using SET



Prevention

Actively use technology you already own to avoid Ransomware and data exfiltration/theft



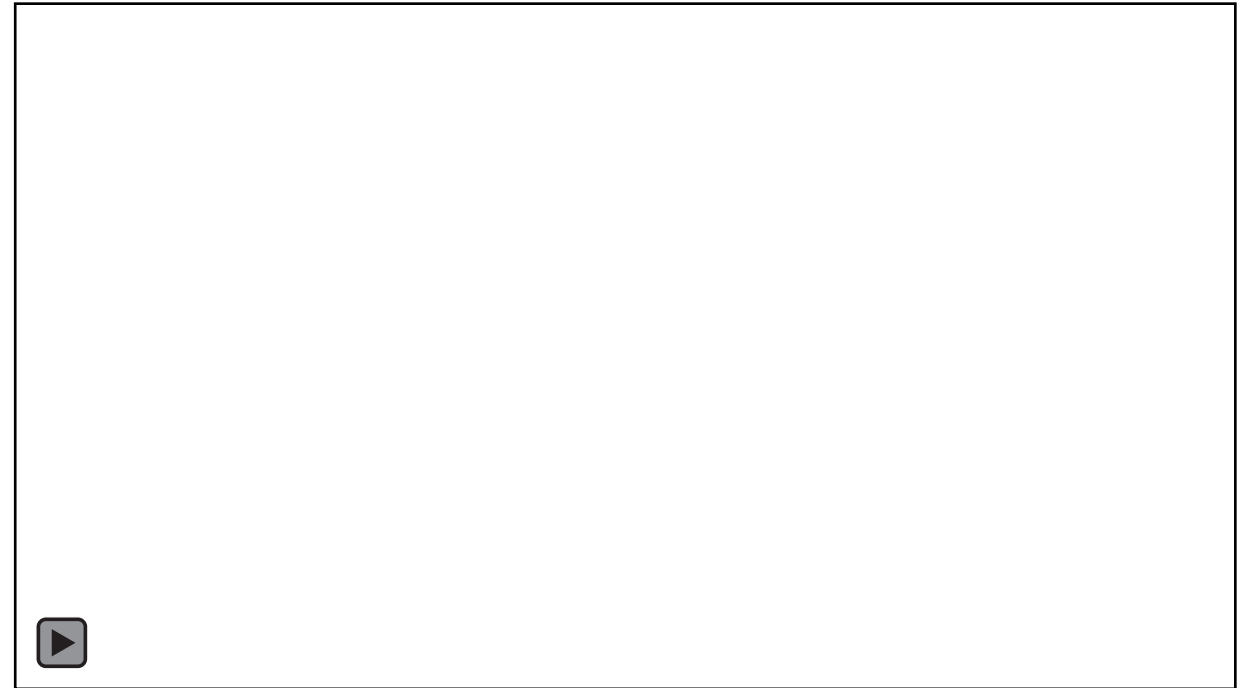
Remediation

Be able to recover quickly and quietly when Ransomware happens and other losses occur

Be successful - Know who's on first

Understanding all the components is the key to preventing incidents

- Perform Social Engineering Toolkit (SET) tests
- Do Network Penetration Testing
- Use Network Segmentation
- Deploy policies based on current guidelines
- Require 2FA
- Implement a true DMZ
- Use best-of-breed Endpoint Protection
- Keep firmware up-to-date
- Train your users



SECURITY

Prevention

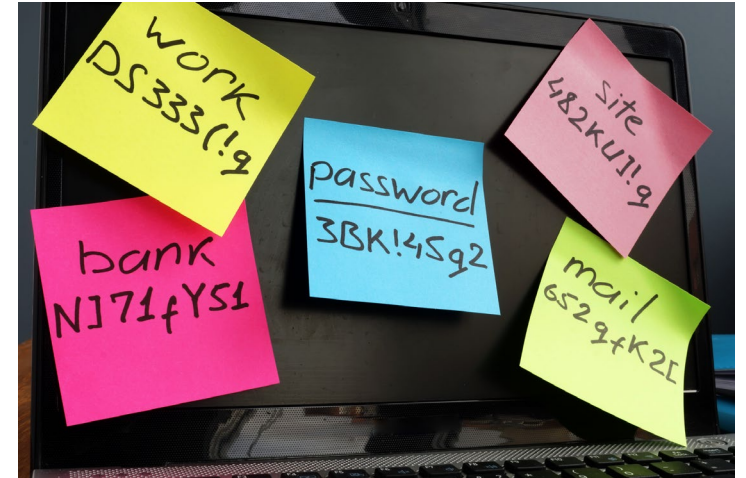
Active measures to improve security

Identity

Smart and logical policies for your users

There's more to Password Policy than you think!

- Use intelligent password policy
 - Most password policy is based on dogma, and some is counter-productive
 - How many users have written down their password in plaintext (on a Post-it even!)
 - How many people store sensitive information (passwords) in un-encrypted documents (*.docx, *.xlsx)
 - How often are passwords shared by users on your Organization (“Hey, Bob, login as me with the password 1234Mainstreet#!”)



NIST Digital Identity Guidelines [800-63-3](#)

The DO's

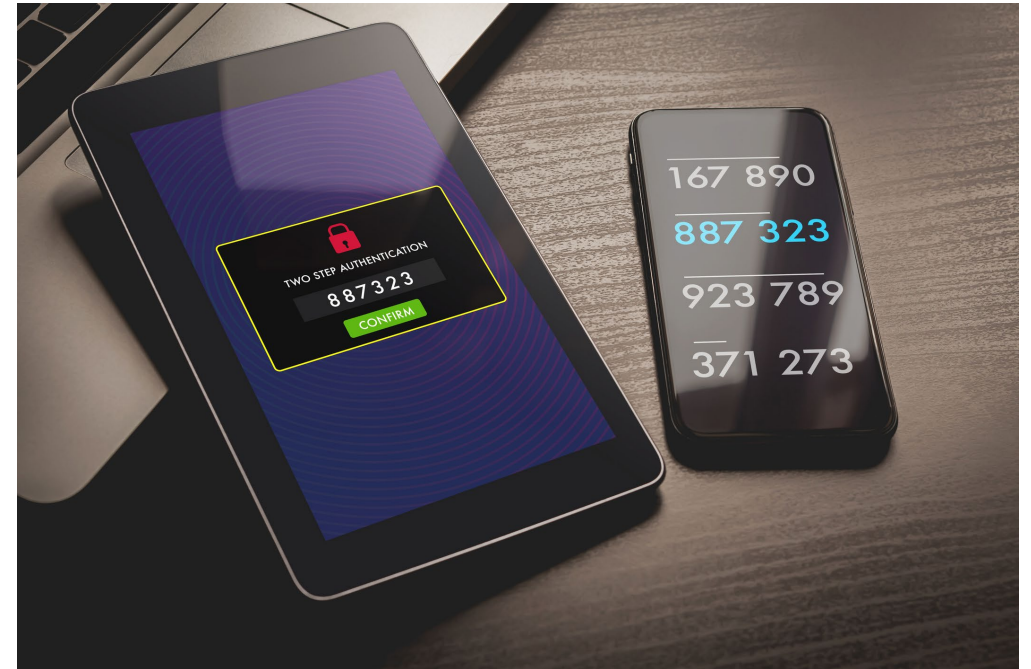
- **DO allow use of passphrases**
- **DO allow the use of cut & paste for passwords**
- **DO favor users, not administrators**
- **DO enforce password length**
- **DO create a banned-list and compare passwords to known-bad passwords**
- **DO enforce timeout for inactivity**
- **DO allow users to see their passwords in plain text**

The DO NOT's

- **DO NOT require numbers, special characters or enforce composition rules**
- **DO NOT use hints or questions**
- **DO NOT enforce password aging**

Deploy two-factor Authentication (2FA)

- 2FA helps to make sure only authorized users access sensitive data
 - The addition of phone, SMS, or other second-factor drastically reduces the possibility of unauthorized access
- 2FA is the standard in improving security



File Sharing

Needs to be usable and secure

- Windows file servers should be permissions-based
 - Each user entitles to only certain files based on Active Directory
- Avoid users leveraging Public Cloud services or email to transfer files from `work` to personal computer resources
- Users data **MUST** be readily available or users will circumvent normal security procedures with USB Drives, email or Public Cloud file sharing



FILE SHARING

INTERNET SECURITY AND NETWORKING

VMsources MSP and Consulting

What VMsources can do for your Organization




- VMsources can assist in the deployment and adoption of 2FA for your Organization
- VMsources can assist with updating Active Directory Password and Security Policy
 - NIST Recommendations based on [NIST Digital Identity Guidelines 800-63-3](#)
 - Group Policy and Security Policy to inhibit Ransomware
- VMsources can help to deploy and validate permissions-based file-shares and file sharing
- VMsources can deploy secure Linux-based filesharing services

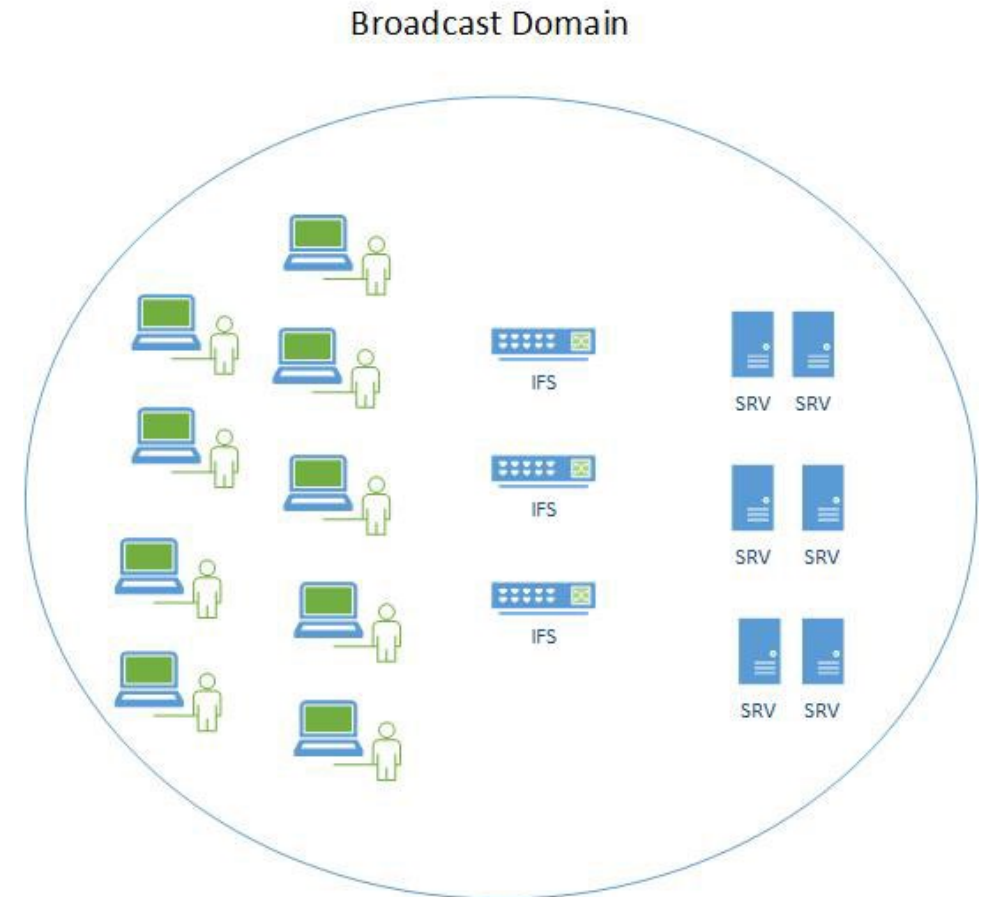
Network

Network segmentation and firewalling
means Security

Understanding a Broadcast Domain

Lack of Network Segmentation often gives Ransomware the foothold it needs

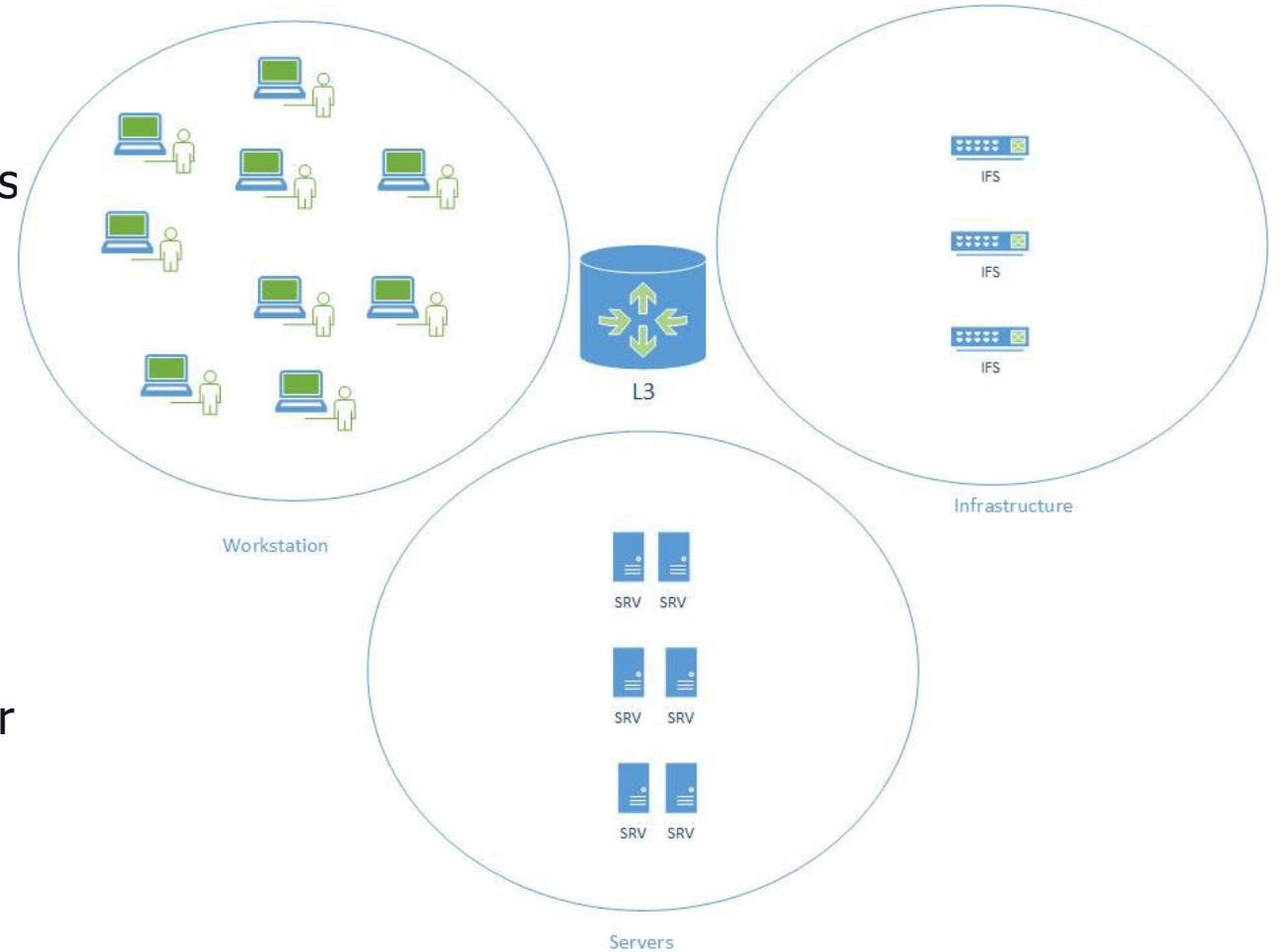
- Broadcast Domains are unrelated to Active Directory
- People often use the terms: "Network," "Subnet," "VLAN" interchangeably to refer to the concept of Broadcast Domain
- Refer to a contiguous Network Segment where all hosts can "talk" to each other without restriction
- Within a Broadcast Domain, Malware, Ransomware and Exploits can spread easily
 - Workstations 
 - Servers 
 - AD, Mail (Exchange), SQL, Terminal Server, Citrix
 - Infrastructure 
 - VMware, Backup, Edge (L3)



Network Segmentation

Network Segmentation alone is a huge step forward

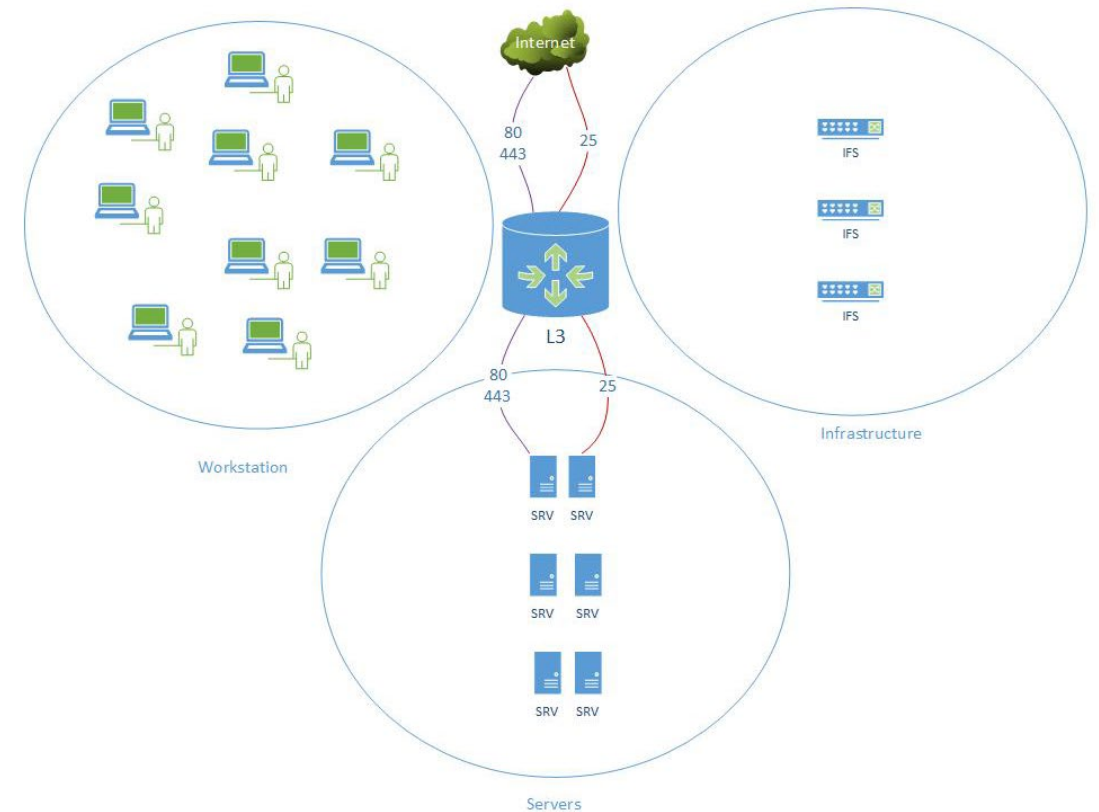
- Network segmentation means moving different categories of system to unique Broadcast Domains
 - Workstation Network
 - Server Network
 - Infrastructure Network
- Communication (AKA: "traffic") can not pass between different Broadcast Domains unless passing a Firewall
- Routers/Firewalls (L3) inspect traffic and permit or deny based on factors such as:
 - Source/Destination
 - Application (Email, SQL, Web)



Port Forwarding (NAT) can be dangerous

Firewalls and Routers can only do so much for security without a DMZ

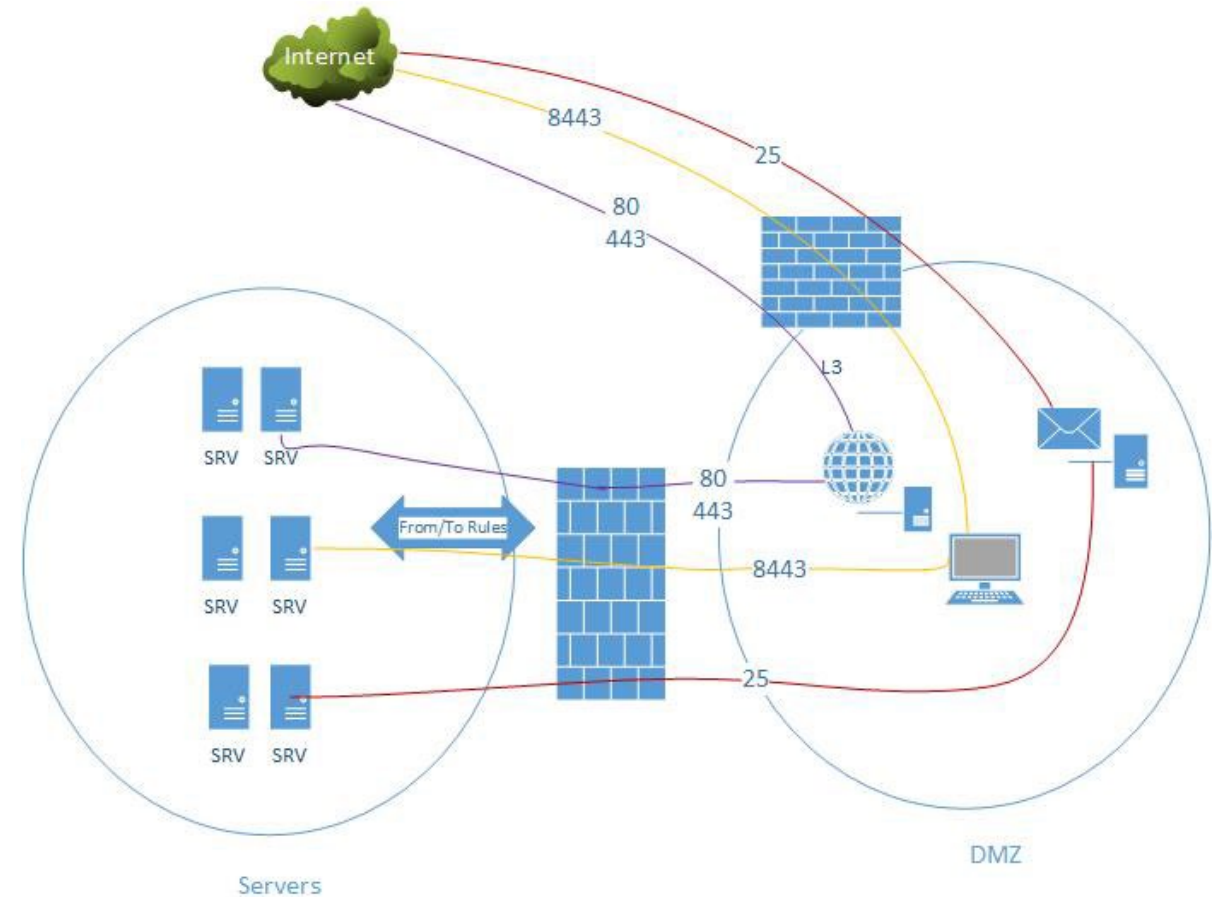
- Applications announce what they are supposed to be using "Ports"
- Port Forwarding is directing certain types of traffic such as Web or Email to the correct Server
- Hackers are able to announce incorrect Ports to introduce exploits
- Port Forwarding from the Internet to any general-purpose Broadcast Domain is a bad idea
 - Remote-code execution vulnerabilities could allow hackers to reach any other system within the Broadcast Domain



True DMZ

Network Segmentation with a true DMZ is the best network policy to prevent propagation of Ransomware

- A true DMZ (Demilitarized Zone) is a dedicated Broadcast Domain containing Internet-facing servers and/or dedicated proxy-servers
 - Web servers often exist entirely in a DMZ
 - Mail servers (such as Exchange) often place an Internet-facing proxy in the DMZ
 - Virtual Desktop Infrastructure (VDI) should have a Secure Gateway server in the DMZ
- DMZ entities should NOT be a member of Active Directory



Stateful Firewall with active ruleset

- Geo-IP Blocking
 - Block countries or entire continents which are not relevant to your Organizations
- Domain Name Service (DNS) Blocking
 - Active DNS Blocklists prevent users from going to known bad addresses
- Content Filtering
 - Limit or prevent traffic based on content type as appropriate for your Organizations
- Secure Delivery
 - Prevent access to addresses which do not have HTTPS/SSL secured by a Trusted Certificate Authority (CA)



VMsources MSP and Consulting

What VMsources can do for your Organization

- VMsources can help create VLANs and then implement Network Segmentation with unique Broadcast Domains for:
 - Desktops
 - Servers
 - Infrastructure
- VMsources can help move Web-facing servers into a true DMZ and/or create secure non-AD proxy Servers
- VMsources can help to remove critical IT Infrastructure (such as: Backup Servers, VMware and Hyper-V) from the main AD domain
- VMsources can help deploy Virtual Firewall technology to implement active protection and Geo-IP blocking

A person's hands are shown holding a glowing Earth globe. The globe is illuminated from the right, creating a bright orange and yellow glow on its right side, while the left side is in shadow. The background is dark with scattered white stars and a soft, out-of-focus light source on the right. The overall mood is one of care and responsibility.

Remediation

Addressing Business Continuity when bad things happen (and they will happen)

Things are going to happen

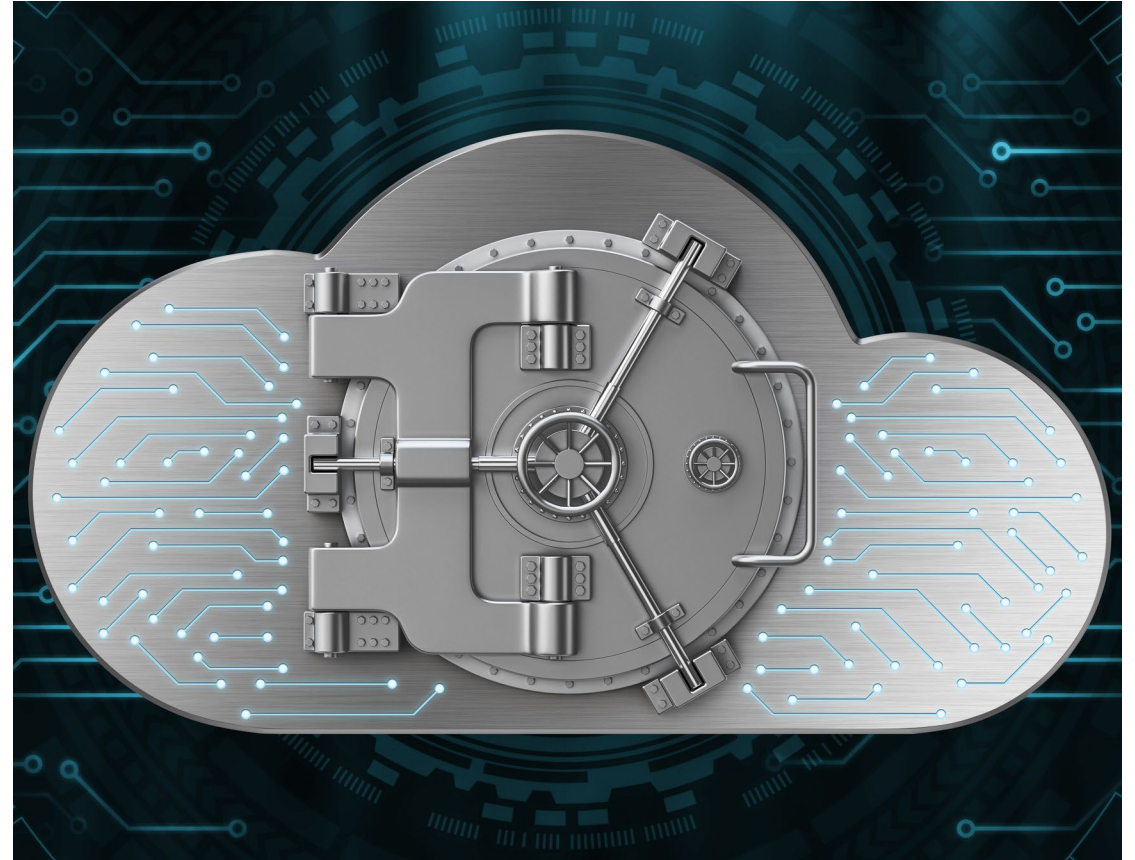
Don't let your Organization be the next headline news

- No matter what you do, something is likely to slip through the cracks.
- Being able to failover to a DRaaS facility or recover quickly from backups is the threshold by which you will be judged.
- Set the standards in advance, there's no such thing as a zero-downtime event!
 - The media has taught us that outages of days and huge ransom payments are the NORM!
 - **Be the hero if you can be fully online in 24 hours or less without paying ransom.**
- Common Thresholds:
 - Organizations with DRaaS can expect to failover fully in about 4 hours
 - Organizations protected by Immutable Backups can expect to recover over a period of about 24 hours
- SUCCESS = Rapid failover and/or recovery
- FAILURE = Extended disruption, loss of data, exfiltration, and paying ransom

Hardened Backups

Existing Backup systems can improve

- A huge problem is Organizations which join Backup Servers and VMware vSphere servers to the AD Domain
 - This effectively allows Ransomware to encrypt the backup files and VMs directly!
- Here are some recommendations:
 - **GOOD:** Do NOT join your Backup Server or Repository to AD Domain
 - **BETTER:** Follow 3-2-1 Rule
 - **BEST:** Combine the two suggestions above with or Immutable Backup technology



Disaster Recovery as a Service (DRaaS)

DRaaS is the way when rapid recovery is the goal

- Deploy an effective Disaster Recovery plan
 - DR or DRaaS should address both physical disasters and logical ones
 - DRaaS maintains a current copy (Replica) of all mission-critical systems at a DR site
 - Understand how far back a replica can be restored (in case of ransomware)
- Test that plan to understand the implications
 - Public IP addresses, DNS, Active Directory and more can all present unanticipated challenges
- Understand the costs of testing and failover
 - Some providers charge exorbitant prices for running any form of failover including testing



VMsources MSP and Consulting

What VMsources can do for your Organization

- VMsources knows and understands Backups and DRaaS better than anyone else.
- We'll build a white-glove DRaaS plan specifically for your Organization.
 - We're happy to respond to RFPs through normal purchasing channels as well.
- We can assist your Organization with hardening existing technologies.
- We can deploy Veeam Immutable Repositories at your location or in our Cloud to protect against Ransomware.
- We'll help you write an IT Business Continuity Plan that will:
 - Establish realistic expectation for events and recovery
 - Spell out "Who's on first" by diagraming every component of the Backup and/or DRaaS systems and what it does.
 - Provide easy-to-follow flowcharts



Training

Educate Users to prevent Ransomware attacks

Training

Knowledge is the key to user success

- Live events with team-building exercises are most effective
 - Mandatory training will help users understand the threats and avoid common mistakes
 - Understanding the challenges will make users sympathetic to new requirements
 - Team building will improve participation in security initiatives
- Webinars can work, but we know they are a drag!
- Recorded sessions are least effective
- Consider the following:
 - In-person group training (with remote participants).
 - The people in the room get the ball rolling and stimulate questions from the remote participants
 - Lunch & Learn
 - A small investment by your Organization will develop a positive attitude about the presentation



Target Training Audience

Your entire Organization

- The audience for IT Awareness Training is your entire Organization, even the techies and administrators who are already knowledgeable.
 - The Techies will affirm the topics covered to their colleagues, creating confidence.
 - The administrators will share real-world experiences and challenges.
 - The bosses and supervisors presence will confirm the importance of the topic.
 - Team-building will establish enthusiasm and cooperation.

Training Agenda

- Email security
 - What Phishing looks like today.
 - Testimonial + Q&A.
 - How SET is being deployed to improve security.
- 2FA
 - Why it's important?
 - How it works for your Organization.
 - What's protected by 2FA and what's not?
- Filesharing
 - The correct way to share files with colleagues, external recipients, even yourself
- Passwords
 - What is a good password?
 - When can we share a password?
- Sensitive Information
 - What is sensitive information?
 - How to use Microsoft Office to protect sensitive information.
 - How to share sensitive information with authorized people.
- Ransomware avoidance
 - Common ways Ransomware finds its way into systems and across firewalls.

Secure Cloud

Multicloud Powered by VMware and Proxmox
VE



Call to action – Secure Cloud

Powered by VMware vCloud with vSAN

- About **half the cost** of Amazon and other Big Clouds
 - Compare for yourself at: <https://calculator.s3.amazonaws.com/index.html>
 - Fixed and **guaranteed 36-month TCO** (No Big Cloud will do that for you)
 - Control the ever-increasing cost of IT
- True **Secure Cloud**
 - You get the flexibility you need with the security you require
 - Multi-tier protection from Ransomware
 - Dedicated Secure Cloud resources are guaranteed to you
- **Concierge Secure Cloud Management**
 - We'll manage the migration process to the Secure Cloud
 - We'll make sure updates get applied
 - We'll allow you to turn your attention to higher value matters



Secure Cloud

What we do to protect YOU from Ransomware



Veeam 3-2-1-1-0 Rule

3 Three different copies of data

2 Two different media

1 One offsite copy

veeam

1 Of which is: offline air-gapped or immutable

0 No errors after automated backup testing & recoverability verification

- True **3-2-1 Rule** Backup Compliance
 - Local backups provide fast access to data and are the first component of the 3-2-1 Rule
 - Remote backups provide the second component of the 3-2-1 Rule
 - Veeam Replicas provide the third component of the 3-2-1 Rule
- We use only **Veeam Immutable repository** technology
 - Tested and proven by [Cohasset Associates](#) meeting the requirements for non-rewritable, non-erasable storage as specified by SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d) – **WORM Equivalency**
- Backup Repositories exist on **dedicated SAN and Networks**

Secure Cloud

What we do to protect VMsources from Ransomware

- VMsources edge systems use **DUO Multifactor Authentication**
- VMsources uses **strong, randomized passwords** for Infrastructure Systems
 - 24 random characters or longer
- VMsources **complies with [NIST Digital Identity Guidelines 800-63-3](#)** Digital Identity Guidelines
- VMsources uses **dedicated Business Continuity domain** for Backup and Infrastructure Systems
- VMsources **always encrypts passwords** and all sensitive and proprietary data



Secure Cloud

Certification & Compliance

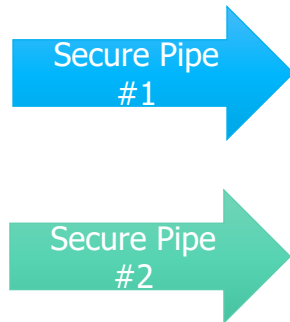
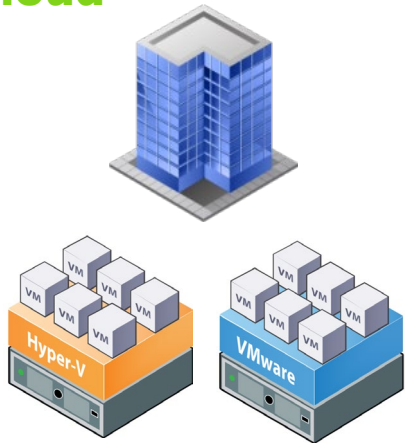
- AICPA Audited
 - SOC 1
 - SOC 2
- ISO 27001 Certified
- HIPAA Compliant
- PCI DSS Compliant



Secure Cloud

Integration with both Public and Private Clouds

On-site Private Cloud



Secure Cloud



Public Clouds



SSL - Secure

SSL - Secure

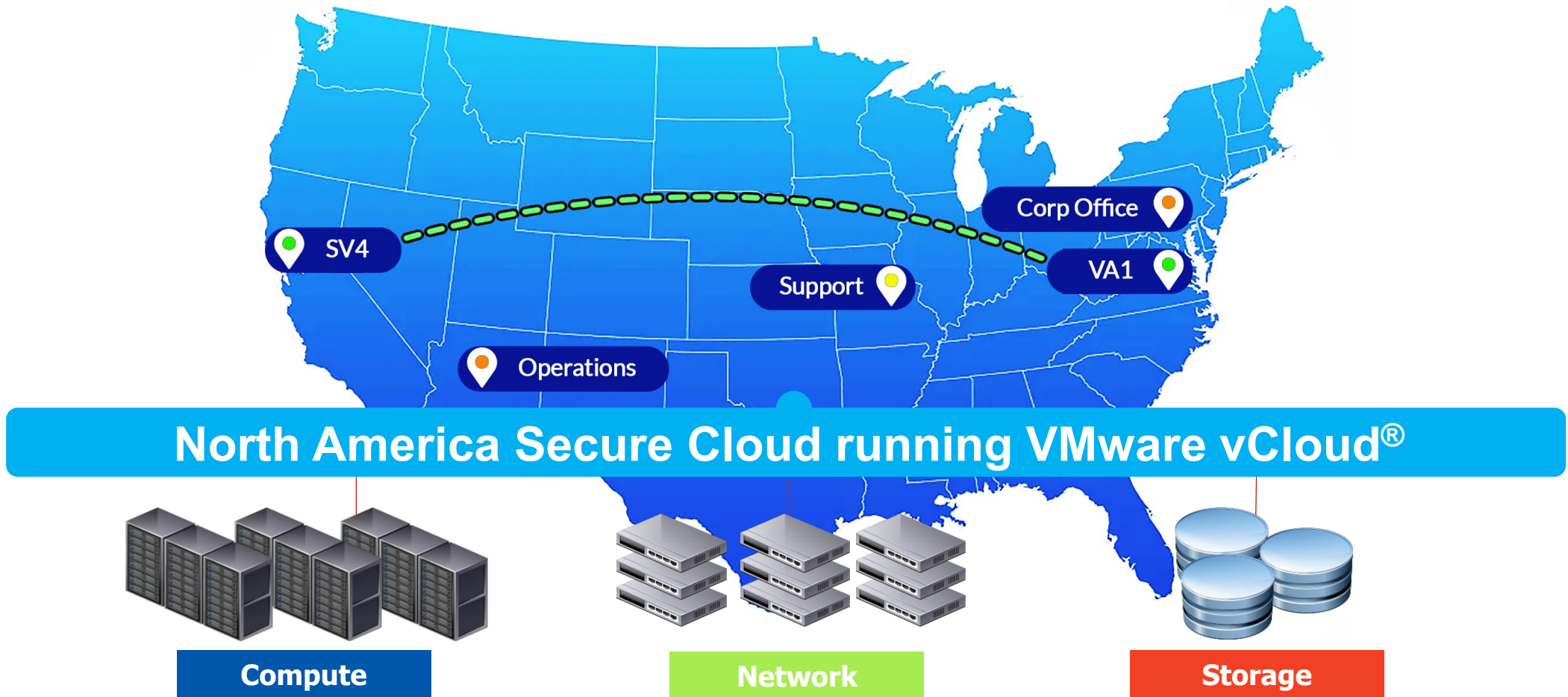
SSL - Secure

User Portals Workloads Security

Three icons in a row: 'User Portals' with two computer monitors, 'Workloads' with 'APP OS' and 'VM' icons, and 'Security' with a padlock and a shield.

Secure Cloud Geo-Scale Diversity

Multiple Locations Guarantee Broad Network Access



Secure Cloud

Why Choose VMsources Secure Cloud?

- All Clouds will provide the resources you need
- **Only VMsources** provides a pathway from your on-site Private Cloud to the Secure Cloud
- **Only VMsources** provides complimentary knowledge transfer when migrating to the Secure Cloud
- **Only VMsources** offers unlimited Tier 4 support tickets / sessions
- **Only VMsources** offers guaranteed TCO
- **Only VMsources** backs the 3-2-1 Rule with **certification** of your protection

Secure Cloud Glossary

- Secure Cloud RAM
 - The RAM (or vRAM) allocated to your powered-on VMs
- Secure Cloud vDisk
 - Super-fast vSAN SSD Virtual Disk for production VMs or Replicas
- Veeam Backup SaaS
 - Veeam Backup and Replication (Enterprise Plus Edition) Software as a Service
- Veeam Immutable Repo
 - A primary backup target for incremental backups, permitting fast restores and further offloads to alternate location(s) or Cloud(s).
 - Veeam Immutable Repositories are tested and proven by [Cohasset Associates](#) meeting the requirements for non-rewritable, non-erasable storage as specified by SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d) – **WORM Equivalency**
- Wasabi S3 Immutable Repository
 - Optional S3 Object storage in alternate Cloud Location

Secure Cloud Glossary

- Grandfather-Son (GFS) Backup
 - Long-term retention of full backups on a schedule (Weekly, Monthly, Yearly)
- Incremental Backup
 - One full backup supplemented on a schedule with backups containing the differences
- Replication
 - Stored on a Cloud Datastore, a Replica provides a ready-to-run copy of a Virtual Machine in an alternate location.



VMSOURCES

Cloud & Infrastructure

Simplicity is elegance

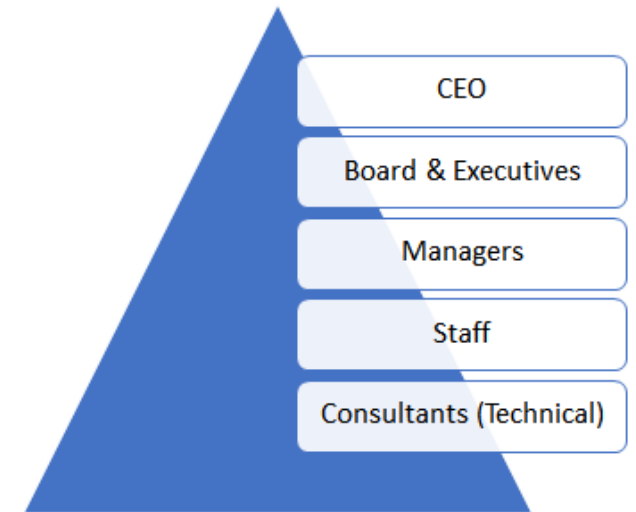
VMsources is a customer-facing MSP specializing in Private Cloud, Infrastructure, and Network.

It is VMsources mission to act as the client's advocate at every stage of the project, from concept to completion.

VMsources Group Inc.



Traditional IT Organization





About Us

We are proud to bring the best technical guidance to the top of a traditional organizational structure.




VMsources Group Inc.

 John Borhek

 +1 215 764 6442 X1001

 john@vmsources.com

 <https://vmsources.com/>