www.technovera.ae
office@technovera.ae

Business Bay
Churchill Executive Tower 18th floor,
1803
Dubai, United Arab Emirates

GENERAL CATALOGE

THE
TRUE
SOLUTION

Contents

■About

➤ **Vision** 05

➤ **Mission** 05

➤ **CEO Message** 05

■Solutions

➤ **Data Center**

- Server Virtualization 07
- Application Virtualization 09
- Storage Virtualization 10
- Virtual Desktop Infrastructure 11
- Network Virtualization 16
- Backup and Data Recovery 19
- Business Continuity 21
- Storage and Archive 24
- Data Center Monitoring 28

➤ **Network and Data Security**

- Advanced Threat Protection 31
- Information Protection 32
- Endpoint Security 33
- Email Security 34
- Network Security 35

➤ **Consulting and Outsourcing**

➤ **Software Development**

- Blockchain Technology 39
- IOS/Android 40
- Web application 40

■ Academy and Test Center

➤ **Academy** 43

➤ **Partners** 46

➤ **Why Technovera** 47

about us

Vision
Mission
CEO Message

ABOUT TECHNOVERA

Technovera is committed to bringing about change in the field of information technology solutions and equipment. Technovera's impressive growth over the course of its history has been driven by the loyalty and support of customers who want our unconditional services, products and unconditional support to meet their growing needs. Engaging experts, academics and applied professionals along with an unrivaled quality of unique service and support, Technovera Co. gave an unequivocal answer to the location of our customers. Technovera has been able to establish itself in its niche, achieve growth and increase the number of customers thanks to precise planning and mastery of all aspects of working with information technology, as well as appropriate knowledge of the market in the short term.

What is our specialization?

*** Data Center**
- Server Virtualization
- Application Virtualization
- Storage Virtualization
- Desktop Virtualization
- Network Virtualization
- Backup and Recovery
- Business Continuity
- Storage and Archive
- Data Center Monitoring

*** Network and Data Security**
- Advanced Threat Protection
- Information Security
- Workstation Security
- Email Security
- Network Security

*** SOFTWARE DEVELOPMENT**
- BLOCKCHAIN
- WEB/MOBILE APPLICATION DEVELOPMENT

*** CONSULTING & OUTSOURCING**

*** ACADEMY**

Data Center
SOLUTIONS

- SERVER VIRTUALIZATION
- APPLICATION VIRTUALIZATION
- STORAGE VIRTUALIZATION
- VIRTUAL DESKTOP INFRASTRUCTURE
- NETWORK VIRTUALIZATION
- BACKUP AND DATA RECOVERY
- BUSINESS CONTINUITY
- STORAGE AND ARCHIVE
- DATA CENTER MONITORING

SERVER VIRTUALIZATION

Server virtualization is about masking server resources, including the number and identities of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to partition a single physical server into many isolated virtual environments. Virtual environments are sometimes referred to as virtual private servers, but are also known as guests, instances, containers, or emulations.

Classic corporate data centers contain a huge number of servers. Many of them are not functional because the workload is distributed only to some of the servers in the network. This leads to a waste of expensive device resources, requires power, maintenance and cooling. Server virtualization seeks to maximize resource utilization by dividing physical servers into multiple virtual servers, each running a different operating system and applications. Server virtualization causes a virtual server to look like a physical server and act on the same principle, increasing the power of each individual physical machine.

Is server virtualization right for your business?

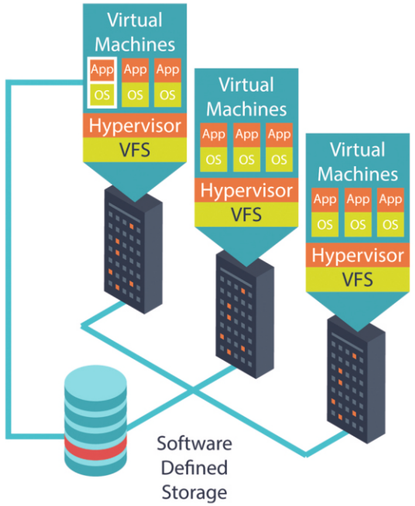
Server virtualization brings multiple operating systems (OS) together on a single server.
Consider this if you're looking to do any of the following:

- Use more apps and OS without breaking the budget for hardware, electricity, and space.
- Reduce the time spent by IT staff installing, repairing, managing and maintaining application servers.
- Add storage virtualization to reduce application downtime and simplify backups.
- Master cloud tasks. Experience with virtual servers will prepare your business to move other business-critical services to the cloud.

VIRTUALIZATION IS A PROCESS THAT INVOLVES MORE THAN JUST PURCHASING AND INSTALLING A PRODUCT. THIS IS A TECHNOLOGICAL JOURNEY. SERVER VIRTUALIZATION CAN BE SEEN AS PART OF THE OVERALL ENTERPRISE IT VIRTUALIZATION.

trend, including storage virtualization, network virtualization, and load balancing management. This trend is a component in the development of autonomous computing, where the server environment will be able to independently organize work based on observed activity. Server virtualization can be used to eliminate server sprawl, make more productive use of server resources, increase server availability, assist in disaster recovery, test and development, and centralize server administration

KEY BENEFITS OF SERVER VIRTUALIZATION:



- Increased server availability
- Lower production costs
- Eliminated server complexity
- Improved application performance
- Faster workload onboarding

APPLICATION VIRTUALIZATION

Application virtualization is the separation of the process of installing an application from the client computer that has access to it. From the user's perspective, the app works just as if it were on the user's device. The user has the ability to move or resize the application window, as well as perform operations using the keyboard and mouse. There may be subtle differences at times, but for the most part, the user should get a flawless user experience.

How Application Virtualization Works

Although there are several ways to virtualize applications, IT staff often use a server-side approach, providing applications for use without having to install them on separate desktops. Instead, administrators implement remote applications on a server in the company's data center or through a Web hosting service, and then bring them to users' desktops. Virtualization software essentially pushes the application as individual pixels from the hosting server to desktops using a remote display protocol such as Microsoft RemoteFX, Citrix HDX or VMware View PCoIP or Blast Extreme. The user can then access the application and use it as if it were installed locally. Any user actions are passed back to the server where they are performed.

PCoIP™

CITRIX™ Ready HDX Technology

Microsoft RemoteFX

TYPES OF STORAGE VIRTUALIZATION

There are two basic storage virtualization methods: file or block. File storage virtualization is a specific use case that applies to network-attached storage (NAS). Using Server Message Block (SMB) or Network File System (NFS) protocols, file storage virtualization breaks the dependency in a conventional NAS array between the data being accessed and the location of physical memory. This allows the NAS to better handle file transfers in the background for better performance. Block virtual storage, or block access virtual storage, is more common in virtual storage systems than file storage virtualization. Block systems separate virtual memory, such as a disk partition, from actual physical blocks of memory in a storage device, such as a hard disk drive (HDD) or solid state memory device. This allows the virtualization management software to collect the capacity of the available blocks of memory and combine them into a shared resource that can be assigned to any number of VMs, bare servers, or containers.

BENEFITS OF STORAGE VIRTUALIZATION

- It is highly scalable
- It allows you to easily add and remove storage without affecting any application
- Easy data migration
- Easy storage management
- Reduced hardware and resource costs
- Improved reliability and performance
- Improved flexibility and scalability

DESKTOP VIRTUALIZATION

The common goal of all our technology developments is to enable you to do more in less time, and today's IT department needs that kind of productivity all the time. Our IT environments are becoming more complex every day. To manage ever-increasing bandwidth requirements, user permissions, network connections, hardware, cloud deployments, applications, and more, the tools we use to manage these systems must give us that ability. Desktop virtualization is the concept of isolating the sample logical operating system (OS) used to access it from the client. There are several different conceptual models of desktop virtualization that can be broadly classified into two categories based on whether a sample operating system is running locally or remotely. It is important to note that not all forms of desktop virtualization technology involve the use of virtual machines (VMs).

TYPES OF DESKTOP VIRTUALIZATION TECHNOLOGIES

Server-based forms of desktop virtualization require users to view and interact with their virtual desktops over the network using the Remote Display Protocol. Since processing takes place in the data center, client devices range from traditional PCs to thin clients, zero clients, smartphones and tablets. Examples of server desktop virtualization technology include: Server virtual machines: Each user connects to a separate VM hosted in the data center. The user can connect to the same VM every time, providing personalization (so-called persistent desktop), or get a new VM every time they log in (non-persistent desktop).

SHARED HOSTING:

Users connect to a shared desktop running on a server. Microsoft Remote Desktop Services, formerly Terminal Services, uses this client-server approach. Users can also connect to individual applications running on the server; this technology is an example of application virtualization.

FIGURE 1: VDI (Virtual Desktop Infrastructure) provides OS desktop functionality to workstations, while Remote Desktop Session Host allows users to access shared applications and desktops.

MANAGEABILITY

* As VDI replaces the PC, deployment, management and maintenance of replacement workstations becomes much easier. Remember, workstations can be laptops, "thin" (or "zero") clients, tablets, mobile devices, and so on. Centralized management software is used to allow IT administrators to manage devices on the network from one central server (data center), meaning that updates, application deployment, and virus control can be centralized rather than handled separately on workstations.

FLEXIBILITY

* Flexibility in maintenance of workstations is one of several benefits of VDI that will positively impact your core software. Routine updates, installations, and more can be done without user intervention. They also don't interfere with end user productivity. Desktops can be easily created virtually by copying images and files and then quickly deployed. End users are not tied to any specific hardware via VDI, so desktop fixes and new desktops can get them back up and running in no time.

ACCESSIBILITY

• With the concept of bring-your-own-device employees, greater worker mobility, the desire to work from home, and more and more employers not worrying about whether their employees are in the office (sitting next to them) or on another continent, accessibility is a key benefit of VDI for such remote, long distance and/or mobile end users. With desktop virtualization, everything is managed and secured in one central location/center/server. IT administrators can do better security, such as protecting files from unauthorized downloads or mass virus updates, and so on.

NETWORK VIRTUALIZATION

Network virtualization (VS) is characterized by the ability to create logical virtual networks that are separate from the underlying network hardware to better integrate and support the network with virtual environments. Organizations have been adopting virtualization technologies at an accelerating pace over the past decade. The VS exposes network connections and services that were traditionally provided by hardware into a logical virtual network that is separate from and independent of the physical network in the hypervisor. In addition to L2-3 services such as switching and routing, the WAN typically bundles virtualized L4-7 services, including firewall and server load balancing. VS solves many of the networking challenges in today's data centers by helping organizations centrally program and deliver the network on demand without physically touching the underlying infrastructure. With VS, organizations can easily deploy, scale, and tune workloads and resources to meet changing data processing needs. With virtualization, companies can take advantage of the efficiency and flexibility of software-based compute and storage resources. While networks have been moving towards more virtualization, only recently, with true automation of control and forwarding planes, as proposed.

software-defined networking (SDN) and network function virtualization (NFV), network virtualization has become more focused.

Applying virtualization to a network When applied to a network, virtualization creates a logical software-implemented representation of hardware and software network resources (switches, routers, etc.). The physical network devices are responsible for forwarding packets, while the virtual network (software) provides intelligent provisioning that makes it easier to deploy and manage network services and underlying network resources. As a result, the WAN can align the network to better support virtualized environments.

VS virtual networks can be used to create virtual networks within a virtualized infrastructure. This allows the aircraft to support complex requirements in shared lease environments. The VS can provide a virtual network in a virtual environment that is truly separate from other network resources. In these cases, the VS may divide the traffic into a zone or storage to ensure that the traffic does not mix with other resources or other data transfers.

Over the past decade, companies and organizations have been rapidly adopting network virtualization (LAN) in an effort to take advantage of the flexibility provided by software compute and storage resources. With software-defined networking (SDN) and network function virtualization (NFV) facilitating the decoupling of control and forwarding planes, more attention has recently been paid to the WAN. For example, after VMware acquired Nicira in 2012, it developed VMware network virtualization.

VMware Network Virtualization and VMware NSX A virtual network built with VMware NSX is a software container that offers logical parts of the network for connected workloads. These logical networks are created and managed in software using the physical network as the packet forwarding plane, allowing for designation of network organization and servers security and connect them to virtual machines (VMs) on the network. As the VM moves from node to node, these services remain attached to it and follow it. VMware says its network virtualization can help data center operators achieve better speed, cost and choice. VMware NSX Data Center is a network virtualization platform that provides networking and security entirely in software, separated from the underlying physical infrastructure. NSX uses software for network functions such as firewall, switching, and routing. This means that multiple users can share the same physical environment using virtual networks that are invisible to each other to increase efficiency and security.

Network virtualization software Network virtualization software allows network administrators to move virtual machines across different domains without changing the network configuration. The software creates a network overlay that can run separate virtual network layers on top of the same physical network.

NSX Data Center Use Cases

• Micro-segmentation

* Reduce the attack surface by micro-segmenting and internally securing applications built on VMs, containers or bare servers in private and public clouds.

• Network Automation

* Gain speed and agility by fully automating networking and security in software, allowing IT and developers to keep up with the speed of business by treating network infrastructure as code.
* Multicloud networking o Streamline networking and security operations by aligning data center, private and public clouds, including AWS and Azure.
* Cloud-native applications o Provide native networking and security for containerizedworkloads, resulting in consistent and automated policy across applications, platforms, sites and clouds.

BENEFITS OF VMWARE NETWORK VIRTUALIZATION

• Flexibility: reduces preparation time from weeks to seconds.

• Cost: Reduces capital and operating costs through automation that eliminates manual configuration and simplifies network equipment requirements.

• Choice: Runs on any hypervisor, any network hardware, and integrates with any cloud management platform. Network virtualization can be classified as external or internal. External network virtualization is the combination of one or more local networks or parts of networks into a single "virtual" network to improve the efficiency of a large network or data center.

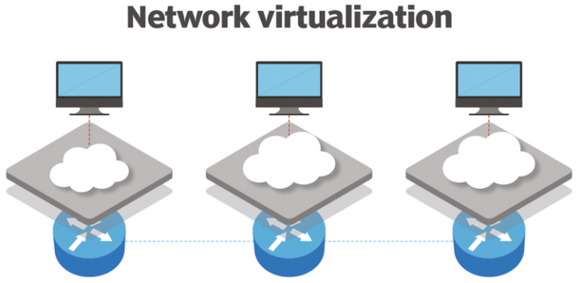
TWO KEY

the components are a virtual local area network (VLAN) and a network switch. Using them together, system administrators can configure systems connected to the same LAN into many different virtual networks. Internal network virtualization is a network that is limited to a single machine and provides network functionality to different VMs using the same system. Also sometimes referred to as a network in a box, it improves the overall efficiency of a single system by isolating individual virtual environments and allowing them to communicate through a virtual network interface. This type is most common on VMware and Parallels workstation versions.

BENEFITS OF VMWARE NETWORK VIRTUALIZATION

• Flexibility: reduces preparation time from weeks to seconds.
• Cost: Reduces capital and operating costs through automation that eliminates manual configuration and simplifies network equipment requirements.
• Choice: Runs on any hypervisor, any network hardware, and integrates with any cloud management platform.

Network virtualization can be classified as external or internal. External network virtualization is the combination of one or more local networks or parts of networks into a single "virtual" network to improve the efficiency of a large network or data center. Its two key components are a virtual local area network (VLAN) and a network switch. Using them together, system administrators can configure systems connected to the same LAN into many different virtual networks. Internal network virtualization is a network that is limited to a single machine and provides network functionality to different VMs using the same system. Also sometimes referred to as a network in a box, it improves the overall efficiency of a single system by isolating individual virtual environments and allowing them to communicate through a virtual network interface. This type is most common on VMware and Parallels workstation versions.



STORAGE VIRTUALIZATION

HAT IS BACKUP AND RESTORE?

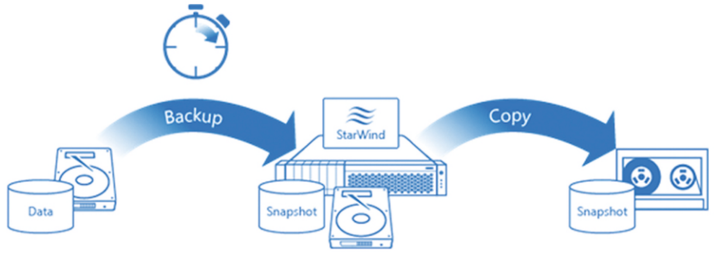
Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations from data loss. This process is sometimes referred to as online recovery. Restoring from a backup usually involves restoring the data to its original location or to another location where it can be used in place of lost or corrupted data.

WHY IS BACKUP AND RECOVERY IMPORTANT?

The purpose of a backup is to create a copy of the data that can be restored if the primary data fails. Primary data failure can be the result of a hardware or software failure, data corruption, and can also be caused by a human, such as a malicious attack (virus or malware) or accidental deletion of data. Backups provide the ability to restore data from an earlier point in time to help businesses recover from an unplanned incident. Storing a copy of the data on a separate medium is critical to protect against loss or corruption of the original data. This additional media can be as simple as an external drive or USB stick, or something more substantial like a disk storage system, a cloud storage container, or a tape drive. The alternate media may be in the same location as the original data or in a remote location. The possibility of weather events may justify storing copies of data in remote locations.

DISK-DISK-TAPE (D2D2T)

Disk-to-disk-to-tape (D2D2T) is an approach to backing up and archiving data in computer storage in which data is first copied to a backup location on a disk storage system and then periodically copied back to a tape storage system. Disk and tape backup systems have their own advantages and disadvantages. For many computer applications, it is important to have data backups on hand after the primary drive becomes inaccessible. In this case, the time to restore data from the tape will be considered unacceptable. Backing up to disk is the best solution because data transfer can be four to five times faster than what is possible with tape. However, tape is a more economical option for data that needs to be stored for a long time. The tape is also portable, making it a good choice for off-site storage. The D2D2T scheme provides the best of both worlds. It allows the administrator to automate daily backups on disk so that he can perform a quick restore and then move the data to tape when he has time. Tape also allows more complete data to be moved offsite for disaster recovery protection and compliance with regulations for long-term data retention at a relatively low cost.



For best results, backups are created on an ongoing and regular basis to minimize the amount of data lost between backups. The more time that passes between backups, the more likely it is that data will be lost when restoring from a backup. Keeping multiple copies of your data gives you the insurance and flexibility to recover to a point unaffected by data corruption or malicious attacks.

STORAGE VIRTUALIZATION

HAT IS BACKUP AND RESTORE?

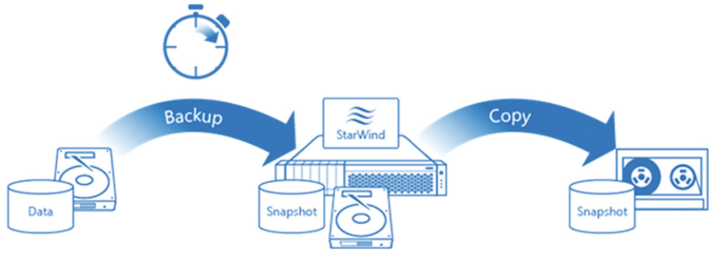
Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations from data loss. This process is sometimes referred to as online recovery. Restoring from a backup usually involves restoring the data to its original location or to another location where it can be used in place of lost or corrupted data.

WHY IS BACKUP AND RECOVERY IMPORTANT?

The purpose of a backup is to create a copy of the data that can be restored if the primary data fails. Primary data failure can be the result of a hardware or software failure, data corruption, and can also be caused by a human, such as a malicious attack (virus or malware) or accidental deletion of data. Backups provide the ability to restore data from an earlier point in time to help businesses recover from an unplanned incident. Storing a copy of the data on a separate medium is critical to protect against loss or corruption of the original data. This additional media can be as simple as an external drive or USB stick, or something more substantial like a disk storage system, a cloud storage container, or a tape drive. The alternate media may be in the same location as the original data or in a remote location. The possibility of weather events may justify storing copies of data in remote locations.

DISK-DISK-TAPE (D2D2T)

Disk-to-disk-to-tape (D2D2T) is an approach to backing up and archiving data in computer storage in which data is first copied to a backup location on a disk storage system and then periodically copied back to a tape storage system. Disk and tape backup systems have their own advantages and disadvantages. For many computer applications, it is important to have data backups on hand after the primary drive becomes inaccessible. In this case, the time to restore data from the tape will be considered unacceptable. Backing up to disk is the best solution because data transfer can be four to five times faster than what is possible with tape. However, tape is a more economical option for data that needs to be stored for a long time. The tape is also portable, making it a good choice for off-site storage. The D2D2T scheme provides the best of both worlds. It allows the administrator to automate daily backups on disk so that he can perform a quick restore and then move the data to tape when he has time. Tape also allows more complete data to be moved offsite for disaster recovery protection and compliance with regulations for long-term data retention at a relatively low cost.



For best results, backups are created on an ongoing and regular basis to minimize the amount of data lost between backups. The more time that passes between backups, the more likely it is that data will be lost when restoring from a backup. Keeping multiple copies of your data gives you the insurance and flexibility to recover to a point unaffected by data corruption or malicious attacks.

Online and Disaster Recovery There are many threats your business faces, and data loss is one of them. Loss of data can lead to several indirect consequences: loss of time, loss of money, loss of business opportunities. To avoid losing data, time and money, your business must recover quickly in the event of a malicious incident. This recovery can take the form of disaster recovery or online recovery. Which one does your business need? Short answer: both. Many organizations rely on data backup for disaster recovery. However, the terms "backup and recovery" and "disaster recovery" have different meanings.

Online restore A backup is designed to bring systems into production by replacing primary data with an earlier copy in the event of data loss or corruption. Data backup includes multiple points in time, up to several years, and can be stored as an archive. The older the data, the less likely it is to be used for recovery. However, many industries have regulatory requirements that require data to be retained for an extended period of time. Backup or archive copies are well suited to meet these requirements.

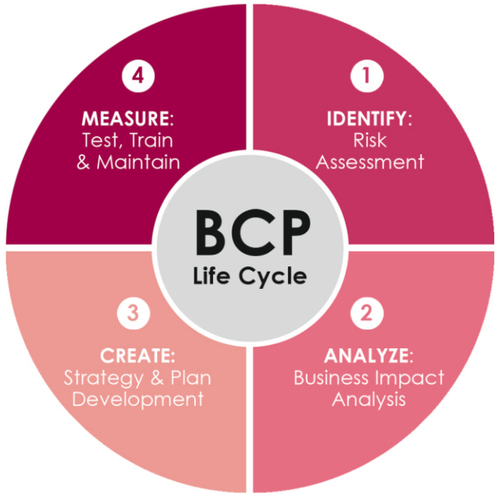
Disaster Recovery A disaster recovery solution is designed to quickly recover an organization from a hardware or site failure by moving to a different copy of the data in a near-consistent state. In the event of a hardware, software or site failure, the applications are put into use at an additional site for a short period to maintain operation. As soon as the primary location comes online again, applications and data are usually migrated back to the primary location. Unlike backups, a disaster recovery solution typically consists of mirrored data, resulting in less data loss (minutes rather than hours or days).

BUSINESS CONTINUITY

Business continuity refers to the ability of an organization to maintain essential functions during and after a disaster. Business continuity planning defines the risk management processes and procedures to prevent disruptions to critical services and restore the full functionality of the organization as quickly and smoothly as possible. The most basic requirement for business continuity is to keep essential functions operational during a disaster and restore them with minimal downtime. The business continuity plan addresses various unpredictable situations such as natural disasters, fires, disease outbreaks, cyberattacks, and other external threats. Business continuity is important for organizations of all sizes, but maintaining full functionality during a disaster may not be practical for all businesses, and may only be appropriate for the largest. According to many experts, the first step in business continuity planning is deciding which functions of the organization are key and allocating the available budget accordingly. Once critical components are identified, failover mechanisms can be created.

Technologies such as disk mirroring allow an organization to maintain up-to-date copies of data in geographically dispersed locations. This allows continuous access to data if one location is disabled. Conducting a business impact analysis (BAA) can identify any potential weaknesses as well as the impact of the incident on various departments. The FDA report provides an organization with information about the most important functions and systems that should be prioritized in terms of business continuity.

The Business Continuity Plan has three key elements: Resilience, recovery, and contingency.



• The company can increase resilience by designing critical functions and infrastructures, taking into account the various possibilities of emergency situations; this may include staff rotation, data redundancy, and maintaining redundant processing capacity. Ensuring resiliency to different scenarios can also help businesses maintain essential on-site and off-site services without interruption.

• Rapid recovery is key to restoring business functions after a disaster. Setting recovery time goals for various systems, networks, or applications can help you prioritize the items that need recovery first. Other recovery strategies include inventorying assets, entering into agreements with third parties to run the company's business, and using refurbished facilities for mission-critical functions.

• The contingency plan provides procedures for various external scenarios and may include a chain of command that allocates responsibilities within the organization. These responsibilities may include replacing equipment, renting office space in an emergency, assessing damages, and hiring third party vendors to assist.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Business Continuity and Disaster Recovery Like a business continuity plan, disaster recovery planning establishes an organization's planned strategies for disaster recovery procedures. However, a disaster recovery plan is just a variation of business continuity planning. Disaster recovery is primarily focused on storing data in a way that is easier to access after an incident. Business continuity takes this into account, but also focuses on the risk management, surveillance, and planning that an organization needs to keep operating during a disruption.

STORAGE AREA NETWORK

Storage Area Networks (SANs) are the most common SAN architecture used by enterprises for mission-critical applications that provide high throughput with low latency. The rapidly growing segment of SAN deployments is optimizing flash-only storage for high performance, consistent low latency, and lower overall cost compared to spinning disk. By storing data in a centralized shared memory, SANs enable organizations to apply consistent methods and tools for security, personal data protection, and disaster recovery. SAN is a block storage that optimizes a high-speed architecture that connects servers to their logical disks (LUNs). LUNs are blocks provided from a shared memory pool to a server as a logical drive. The server partitions and formats these blocks, typically with a file system, so that it can store data on the LUN just as it would on a local disk drive.

SAN USE CASES

SANs are often deployed to support business-critical capacity-driven applications such as:

• **Oracle databases:** These are often critical to business continuity and require superior performance and data availability.

• **Microsoft SQL Server databases:** Like Oracle databases, MS SQL Server databases typically store the most valuable data for an enterprise, so they require the highest performance and data availability.

• **Large virtualization deployments using VMware, KVM, or Microsoft Hyper-V:** These environments often span thousands of virtual machines running a range of operating systems and applications with varying performance requirements. Virtualized environments localize many applications, so the reliability of the infrastructure becomes even more important, as its failure can lead to the failure of several applications.

• **Large virtual desktop infrastructures (VDIs):** These environments serve virtual desktops for a large number of users in an organization. Some VDI environments can easily serve tens of thousands of virtual desktops. By centralizing virtual desktops, organizations can easily manage the security and safety of personal data.

• SAP or other large ERP or CRM environments (Enterprise Resource Planning) or CRM (Customer Relationship

MANAGEMENT SYSTEM): SAN ARCHITECTURES ARE GREAT FOR ENTERPRISE RESOURCE PLANNING AND CUSTOMER RESOURCE MANAGEMENT WORKLOADS.

TYPES OF SAN

THE MOST COMMON SAN PROTOCOLS ARE:

• Fiber Channel Protocol (FCP): The most widely used SAN protocol or block protocol, used in 70-80% of the entire SAND market. FCP uses Fiber Channel transport protocols with built-in SCSI (Small Computer System Interface) commands.

• Internet Small Computer System Interface (iSCSI). The next largest SAN protocol or block protocol, covering approximately 10%-15% of the market. iSCSI bundles SCSI commands in an Ethernet frame and then uses the EtherNet/IP network for transport.

• Fiber Channel over Ethernet (FCoE). FCoE covers less than 5% of the SAN market. This protocol is similar to iSCSI in that it concatenates an FC frame within an Ethernet datagram. Then, like iSCSI, it uses the EtherNet/IP network for transport.

• Non-Volatile Memory Express over Fiber Channel (FC-NVMe). NVMe is an interface protocol for accessing flash memory via the PCI Express (PCIe) bus. Unlike traditional Flash-only architectures that are limited to a single sequential command queue, NVMe supports tens of thousands of parallel queues. Each of them has the ability to support tens of thousands of simultaneous commands.

SAN vs. NAS

Both SAN and Network Attached Storage (NAS) are methods of centralized storage management and sharing with multiple hosts (servers). However, a NAS is based on Ethernet, while a SAN can use Ethernet and Fiber Channel. In addition, while SAN focuses on high performance and low latency, NAS focuses on ease of use, manageability, scalability, and lower total cost of ownership (TCO). Unlike SANs, NAS external storage controllers share the memory and then own the file system. This makes the NAS server look like a Windows or UNIX/Linux server for a memory consuming server. A SAN is typically assembled using three main components: cables, host bus adapters (HBAs), and switches connected to storage fabrics and servers. All switches and storage systems in a SAN must be interconnected, and the physical interconnects must support throughput levels that can adequately handle peak data activity. IT administrators manage storage networks centrally.

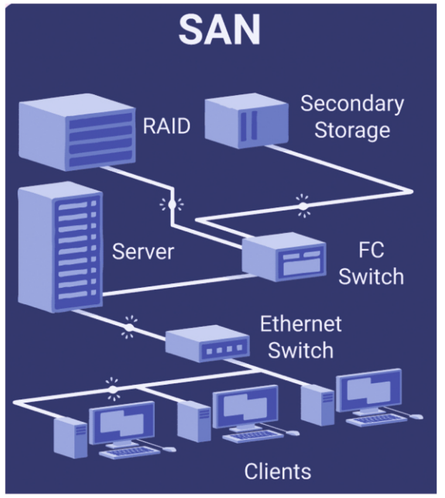
Understanding SAN switches

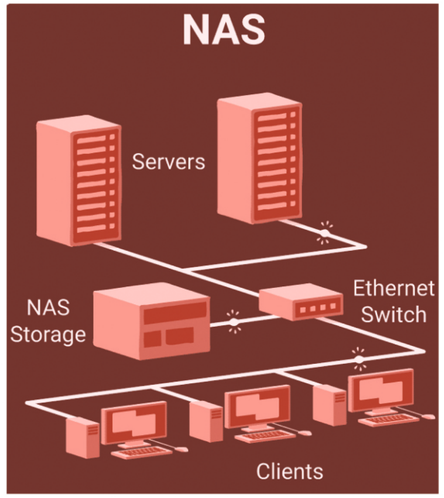
SAN switches connect servers and shared storage pools. The sole job of a SAN switch is to move storage traffic. SAN switches are often Fiber Channel switches that are compatible with the FC protocol on which many SANs are based. The switch examines the data packet and determines its origin and destination. The switch then routes the packet to the correct storage system. FC switches are designed for use in high performance networks.

CONVERGED SAN

SANs are typically kept separate from Ethernet networks. Converged SAN uses a common network infrastructure for network traffic and SAN traffic to eliminate redundant infrastructure and reduce cost and complexity. SANs often use fiber optics, while data networks are usually based on Ethernet.

Converged SANs use the FCoE standard, which integrates the FC payload into Ethernet frames. Converged SANs are almost always based on 10 Gigabit Ethernet, and sometimes several network ports are combined to increase throughput.





DATA CENTER MONITORING

Data center monitoring is the process of monitoring, managing and operating a data center in accordance with operational and organizational requirements. It is the process of using manual and automated tools and methods to ensure that the data center is in the best operating condition. It ensures that key data center functions and services run without any interruptions or failures. Data center monitoring is a broad process that focuses on monitoring the entire data center infrastructure. Typically, data center monitoring is done through automated tools that provide statistical information about the performance/health of the data center. This data is used by data center administrators to detect violations and correct them.

Data center monitoring typically includes:

• Monitoring data center servers and computers for performance, security durability, and more

• Monitoring and managing network operations and resolving network issues as they arise

• Providing comprehensive visibility into all components data center including computers, storage, network and software How does data center monitoring work? Data Center Monitoring gives you the ability to centrally manage all the devices in your data centers. It allows you to connect, collect data, and configure devices using SNMP, HTTPs, and other protocols for IP networks.

• Automatically collect real-time data from all your devices, down to the individual branch level, through a single interface

• Set power and environmental thresholds for collected data and be the first to be alerted to potential problems before they get bigger

• Adjust polling rates to intervals that provide meaningful information while keeping network traffic efficient

• Forward and filter traps to receive only the notifications that matter to you

• Analyze and trend collected data to gain insight into data center operations, including processing capacity predictions

• Give yourself peace of mind about your data center security with door locks and card readers giving access to authorized users and

• Use protocols such as SNMP, HTTPS, Modbus, BACnet, Wiegand, RF, etc. to communicate with data center monitoring software

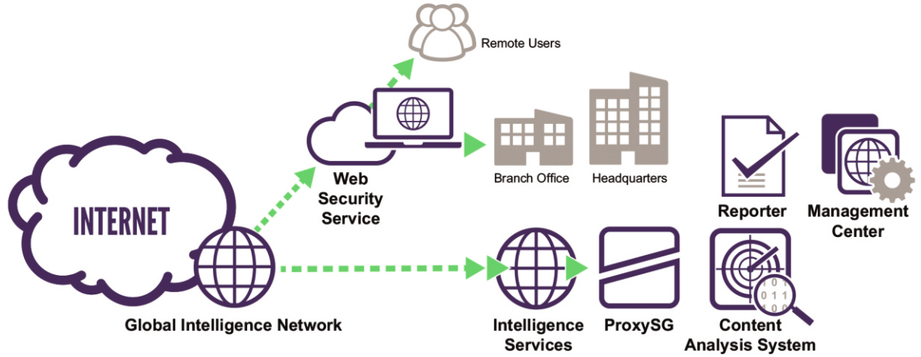
Network Security

ADVANCED THREAT PROTECTION

Gain control with multiple layers of threat prevention, detection, and forensic technology Cybercrime is big business. There may not be a single action that can provide your entire security program. To protect against system failures due to the failure of one element in specific technologies or protection methods, it is necessary to create several redundant and complementary protective systems. This includes the implementation of workstation, email and web gateway security technologies, as well as firewalls and vulnerability assessment solutions. Stay up to date and apply system patches and updates to ensure your security is up to date with the latest security features from Symantec. Threats don't subside. Cybercriminals have added tactics such as cryptojacking and fileless threats to their arsenal while continuing to use proven methods such as ransomware. 50% of the organizations surveyed experienced more cyberattacks than in the previous year, and only 6% reported fewer attacks. Clearly, the risk of advanced threats is real and difficult to combat. Security gaps can increase the likelihood of a breach and the damage these threats can cause to your business. Symantec helps protect your business from cryptojacking, fileless threats, and ransomware.

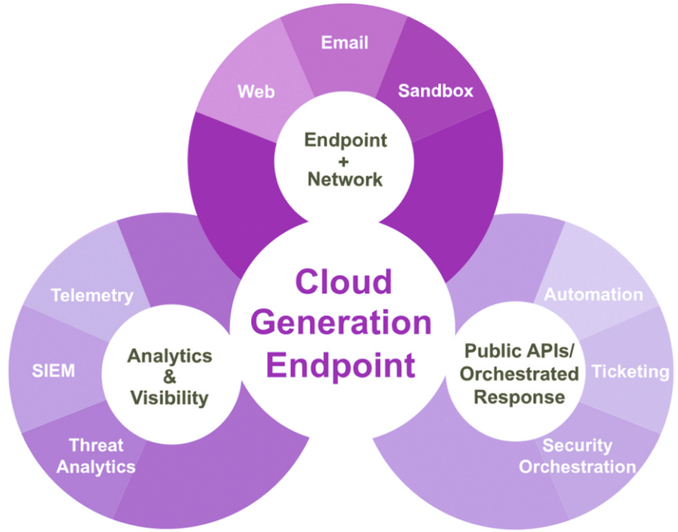
DATA PROTECTION

Protect your important data, wherever it resides Keeping sensitive corporate information safe and secure has never been easier. But today, you are facing a whole new set of data protection challenges. Confidential information leaves the secure area of your corporate network as more employees share files through custom cloud storage services and access those files on their own mobile devices. The number of targeted cyberattacks is on the rise as cybercriminals develop effective new methods to counter traditional security measures and corporate identity theft techniques. As all these factors converge, it becomes increasingly difficult to manage corporate information and protect it from loss and theft. So how do you manage and protect your information in such a complex environment? And what does a complete, successful data protection strategy look like in the face of undermining security perimeters, increasing targeted attacks, and changing user habits and expectations?



WORKSTATION SECURITY

Protect users and critical resources with layered protection Workstations are a prime target for cyberattacks. In 2018, the number of new threats to workstations, mobile malware and the frequency of attacks increased significantly. People now work from everywhere, not just from their corporate headquarters. And the concept of owning employee devices has added billions of devices to an interconnected enterprise system. Today, protecting workstations must consider devices, applications, and networks. Our goal was to help customers reduce the cost and simplify cybersecurity while improving response time and efficiency.



EMAIL SECURITY

PROTECT YOUR EMAIL IN THE CLOUD AND ON SITE

Smart, ubiquitous email protection, whether for on-premises, cloud, or hybrid email systems, starts with a clear understanding of the problem. Email is the most common way for cybercriminals to launch and distribute threats. According to the Symantec™ Internet Security Threat Report 2018, in 2017, there was 1 in every 412 emails containing a malicious attack, 7,710 organizations are attacked every month to compromise corporate email, and spear-phishing is the most widespread the infection vector used by 71 percent of targeted attack groups.

As the number of these attacks grew, so did the level of difficulty. Advanced threats and zero-day vulnerabilities are much more difficult to detect and stop than traditional malware, and standard signature-based anti-malware defenses have proven largely ineffective against them. Attackers now favor spear-phishing scams, especially in the form of corporate email compromise scams. These evasive and dangerous targeted attacks use sophisticated techniques, including domain spoofing and obfuscation of malicious links embedded in email messages. The losses from these attacks now stand at $12.5 billion and have grown by 136% in 17 months. Local messaging isn't going away anytime soon thanks to strict industry regulations, data sovereignty, and company mandates to maintain full control of the email infrastructure. For many organizations, on-premises email security solutions are just as important as they are in the cloud.

NETWORK SECURITY

The traditional network perimeter no longer exists - today the perimeter is where the data resides. Users are everywhere and need fast access to data and cloud applications around the clock. Whether in the cloud or on premises, you need to stop inbound and outbound threats that target end users, information, and key infrastructure. Modern network security must address this new reality while balancing security, performance, complexity, and cost. Security architectures are becoming increasingly overwhelmed as network traffic is merged into the web and cloud applications like Office 365. Your data and your security must go together wherever your employees go. Protect your business with an advanced cloud-based network security service that is highly scalable, performant, cost effective and easy to use. Services Top Level Support Provide your business with a single point of accountability and security expertise when and where you need it. Consulting Services Symantec Consulting Services provides the experience, knowledge, and industry insights to help you better design, design, implement, and optimize security software, people, and processes. Education Services Enhance your product competency and validate your technical knowledge to get the most out of your IT investment with in-depth technical training. Cyber Security Services Expand your team with Symantec to reduce detection and response times, lower costs, and proactively respond to known and emerging threats.

Solutions Consulting and Outsourcing

CONSULTING AND OUTSOURCING

IT services refer to technical knowledge to help organizations create, manage, optimize or access information and business processes. As a small or medium business, you must make the most of today's technology to stay competitive. You have to do it cost-effectively and with little direct information technology experience. Maintaining a dedicated full-time IT department like your larger competitors in the marketplace is too expensive, time-consuming, and inefficient for a small business. As a big business, your business grows and develops, inevitably your IT strategy must evolve with it. These difficulties are solved with the help of a professional technology service provider. Technovera provides consulting, design, implementation, maintenance and support services in the IT field.

Why is it so important?

- Gain time to focus on core business functions
- Leverage economies of scale and purchasing power
- Reduce downtime
- Reduce costs and control operating expenses
- Get resources on demand
- Increase productivity
- Access highly specialized talent
- Bring it to life technological advantage over the competition
- Attract and retain employees
- Gain access to otherwise unavailable supplier support

What services do we offer?

- Infrastructure
- Information security
- Data storage
- Virtualization
- Computing
- Backup and disaster recovery
- Monitoring
- Log management
- Software
- Platforms
- Networks
- Mobile platforms

Software Development

BLOCKCHAIN

In its original form, "blockchain" is a distributed database technology built on a tamper-proof list of timestamped transaction records. Among other things, this technology is used for cryptocurrency.

Its innovative strength lies in the fact that it allows parties to transact with others they do not trust through a computer network where no one is trusted. This is achieved through a combination of peer-to-peer networks, consistency, cryptography, and market mechanisms.

Benefits of blockchain technology

- It's distributed
- High security
- Reduced threat of hacking
- Increased transaction transparency
- No middleman fees
- Various levels of availability
- Faster transactions
- Automatic account reconciliation

SERVICE TECHNOLOGIES IN WEB APPLICATION DEVELOPMENT

Developers can use various technologies to serve the purpose of web application development. These are technologies such as Ajax, ASP .NET, CGI, Java, Perl, PHP, Python, Ruby, Coldfusion, etc. As a rule, agile methods (agile development methodology) and life cycle models such as Scrum, as well as feature-based development, are used.

Mobile Application Development Service Technologies Mobile application development services are typically implemented on Android, iOS, Windows, and Blackberry platforms based on Apache Cordova (Phonegap), Node Js, Xcode, and Genymotion technologies, as well as HTML, Java, C++, C#.

The software development services provided by our company cover the entire product life cycle.

- Software architecture and design
- Implementation
- Testing and quality assurance
- User documentation
- Support

SOLUTIONS SOFTWARE DEVELOPMENT

Academy and Test Center

EDUCATION

The company "Technovera" is an international training center in the field of information technology. We offer high quality, professional and cost-effective professional IT education for corporate clients and individuals.

Guided by our mission to bring innovation to the world, we organize courses for teaching modern

technologies. Why choose Technovera?

- High quality
- Work oriented
- Professional and experienced professors
- Equipped laboratory
- Valid certificate

Seminars

No.	Name of the course	Duration
СЕМИНАРЫ TECHNOVERA		
1	Cisco ISE	40 hours
2	Virtual desktop infrastructure	40 hours
3	Back up	16 hours
4	Blockchain	50 hours
5	Sophos	16 hours

No.	Name of the course	Duration
	HP	
1	HP priolant Server Technology ml\dl\sl	24 hours
2	Accelerated SAN Essentials	40 hours
3	Установка и настройка HP 3PAR StoreServ 1 , 2	40 hours
4	HP data protector v 9.x	32 hours
	Vmware	
5	VMware VCP6 60	6 hours
6	Vmware Vsphere Optimize & Scale V6	40 hours
7	vmware VSAN	16 hours
8	Vmware Horizon view v.7	40 hours
9	Vrealize	24 hours
10	Vmware NSX	32 hours
11	Veeam backup &Recovery	16 hours
	EMC	
12	ISM V 3	40 hours
13	VNX2 Implementation Block Deployment	24 hours
14	Data Domain	32 hours
15	VNX Unity Implementation Configuration	24 hours
16	Networker	32 hours

No.	Name of the course	Duration
	DATA CENTER	
17	TIA-942	24 hours
	Linux	
18	Linux System Administrator (LPIC 1) (для системных администраторов)	50 hours
19	Linux Engineer(LPIC 2) (для инженеров)	50 hours
	Oracle	
20	Oracle Admin Workshop I (семинар для администраторов)	40 hours
	CISCO	
21	CCNA Security	60 hours
22	CCNP ROUTE	50 hours
23	CCIE Security	80 hours
24	CCDA	40 hours
	ITIL	
25	ITIL Foundation	24 hours
	NEW TECNOLOGY	
26	BLOCKCHAIN	

PARTNERS


Symantec


SOPHOS


FORTINET


CITRIX


cisco


Hewlett Packard
Enterprise


veeam


solarwinds


VERITAS


vmware


Quantum


DELL EMC


Pearson
VUE


paloalto
NETWORKS


JUNIPER
NETWORKS


f5


Microsoft


ORACLE


QNAP


gemalto
security to be free


APC
by Schneider Electric


AVAYA


hp


acer


Apacer


Lenovo

www.technoveraco.com
Office@technoveraco.com

REASONS WHY YOU SHOULD CHOOSE US:

1. Our team consists of certified experts
2. We partner with leading companies in the industry
3. We provide you with the answers you need and bring them to life
4. Our experts are broad-based, we can deliver a holistic viewpoint
5. We are dedicated and give the right advice
6. We help you get more out of your investment
7. We see the 'big picture' and can make success sustainable
8. Unparalleled reliability and availability
9. Respectful and professional support
10. Redundant and reliable technicians