Prepared for:

Tempest Fitness

In the following pages you'll find your customized Audit Report. It contains all of the information gathered from your IT environment summarized into one easy to read document. Upon reading, you will have a much better understanding of your IT plan and what you're spending.

YOUR CUSTOMIZED REPORT

Based on our technical analysis of your IT environment, we have customized a selection of 27 audit items spread across three main areas of technology – Infrastructure, Security and Managed Support & Services. A fourth optional area, Telecommunications, may also be represented in your plan.

Each of these areas will give you important insight into the strengths and weaknesses of your IT plan.

YOUR AUDIT SCORE

Using the results of your audit, we calculated your overall audit score. The higher your audit score, the greater efficiency at which you are spending on technology. Our goal is to drive your audit score as close to 100 as possible.

The Comparative Analysis page allows you to easily compare your baseline plan with other plans presented in this document to see qualitative, quantitative and financial results.

HOW TO READ THE REPORT

Each audit item has been color coded to make it easy to visualize your results. Red indicates an audit item that requires immediate attention, yellow indicates an audit item that needs improvement and green indicates an audit item that is satisfactory.

In addition to a Summary page, you will find dedicated pages with color coded summary statements for each individual audit item. Any audit item that isn't satisfactory is described in greater detail and its relative importance is explained in a single page infographic.

Base Plan

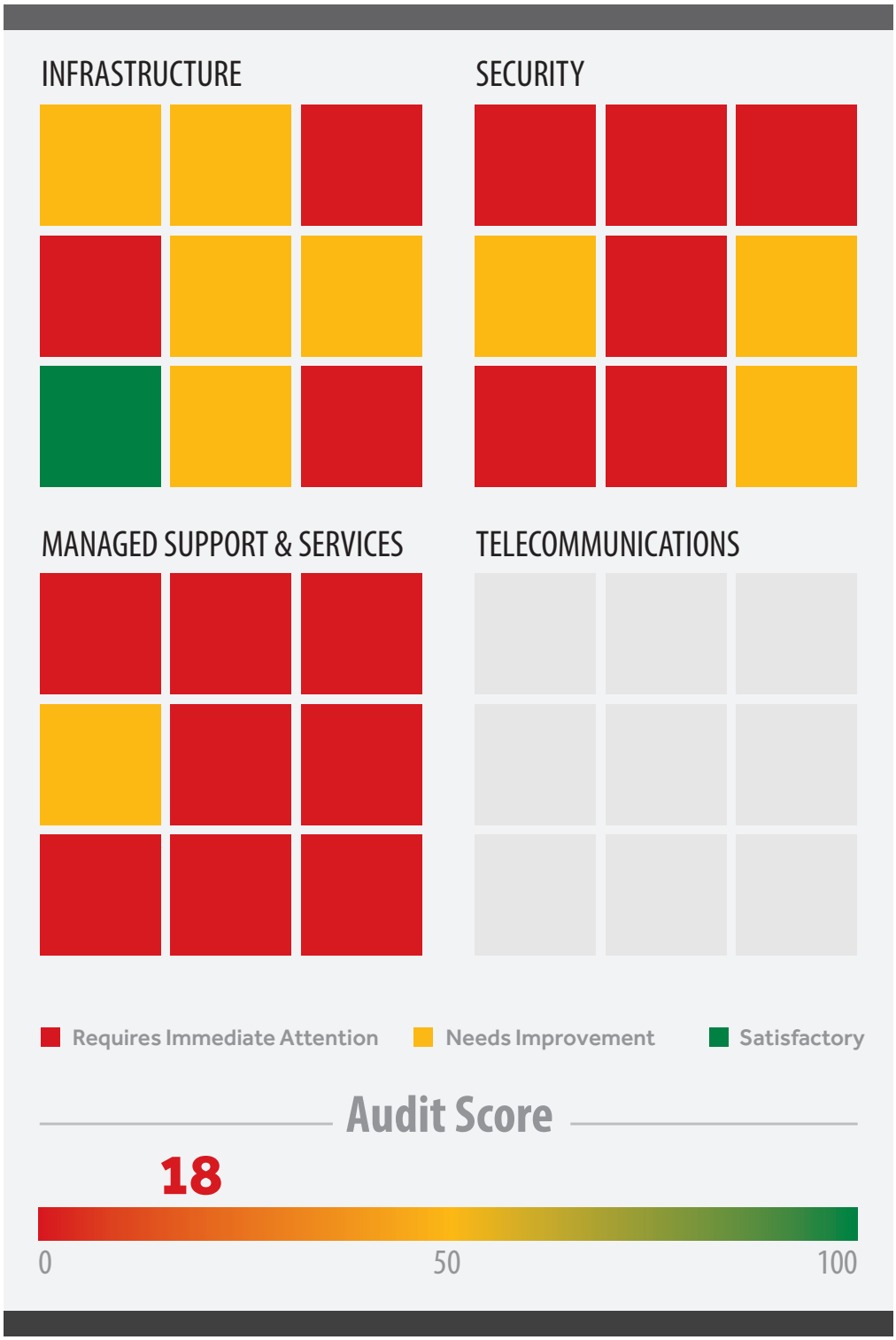
Plan Type: Baseline Plan

Baseline Plan for Tempest Fitness

Summary

Baseline Plan

Baseline Plan for Tempest Fitness



BASE PLAN SUMMARY

The results of each quadrant of your 27 point, base plan audit is summarized here using color coded boxes. Utilizing a weighted scoring system, the results were combined and averaged into an overall audit score. Individual quadrant scores and details for each audit item are shown in subsequent pages. Your base IT monthly expense is shown as a range and has been converted into an "effective" monthly expense based upon your audit score. This helps to level the playing field when comparing plans. If Telecommunications was audited, the results and monthly expense is also shown.

FINANCIAL SUMMARY

Monthly IT Expense
$500.00 - $1,000.00

Effective Monthly IT Expense
Based on the audit score
$2,777.78 - $5,555.56

Telecom Monthly Expense
$500.00

Audit Detail

TECHSPERT data services LLC

INFRASTRUCTURE

Backup & Disaster Recovery	Business Continuity	Server(s)
Online backup service is backing up server(s) on a regular, automated basis.	Business Continuity exists in a variety of services but must be invoked or set up on demand.	The server(s) is over 5 years old, out of warranty or running a non-supported operating system.
Workstations	**Managed Wireless**	**Hosted Exchange Email**
The workstations are over 3 years old, out of warranty or running a non-supported operating system.	Needs Improvement.	Email is in-house using a local Microsoft Exchange Server.
Power Management (UPS)	**WAN Redundancy / Failover**	**Remote Accessibility**
Satisfactory.	Needs Improvement.	Requires immediate attention.

Requires Immediate Attention Needs Improvement Satisfactory

Audit Score

38

0 50 100

INFRASTRUCTURE

Infrastructure is the foundation upon which all of your technology rests. Just like with a house, it's extremely important to verify its integrity before you begin to build on top of it. Poor initial design decisions can lead to downtime, lost sales and ultimately drive up your total cost of ownership. This detailed analysis page represents an overview of the state of your Base Plan Infrastructure. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Infrastructure audit score.

Audit Detail

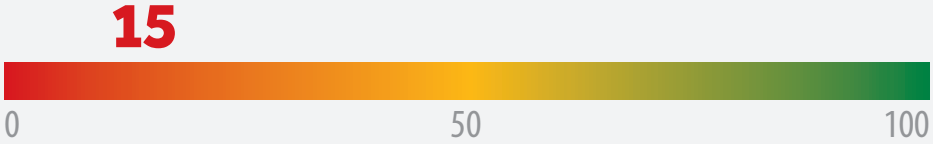
TECHSPERT data services LLC

SECURITY

Internet Security Appliance There is no Internet Security Appliance. ISP provided or residential router is in place.	**Intrusion Detection/Prevention** Requires immediate attention.	**Next Generation Endpoint** Requires immediate attention.
Anti-SPAM and Virus Filter There is a 3rd party Anti-SPAM and Virus filter that is integrated with the Hosted Exchange provider.	**Security Awareness Training** Requires immediate attention.	**Virtual Private Network (VPN)** Needs Improvement.
Two Factor Authentication There is no two factor authentication available for system access.	**Physical Security** There is no physical security and servers are in the open and subject to theft.	**Password Policy** Needs Improvement.

Requires Immediate Attention Needs Improvement Satisfactory

Audit Score



SECURITY

Security is arguably the most important section of your audit report. With so much riding on the security of your infrastructure, you can't afford to have any deficiencies. Fortunately, there's an abundance of security solutions available to help mitigate the risks and protect your data. This detailed analysis page represents an overview of the state of your Base Plan Security. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Security audit score.

Audit Detail

TECHSPERT data services LLC

MANAGED SUPPORT & SERVICES

Virtual CIO Services vCIO services are not provided by current IT consultant.	**Monitoring** There is no monitoring of server(s) and workstations	**Help Desk Support** Remote Help Desk Support is not included and is billed hourly as needed.
Onsite Support Needs Improvement.	**Inventory & Asset Management** Inventory & Asset Management is manual or not included and not reviewed regularly.	**Windows & Application Updates** Windows updates on server(s) and workstations are manual but not all are up to date.
Proactive Maintenance Proactive maintenance of server(s) and workstations is manual and not included in the plan.	**Network Documentation** Requires immediate attention.	**E&O Insurance** Requires immediate attention.

Requires Immediate Attention Needs Improvement Satisfactory

Audit Score

4

0 50 100

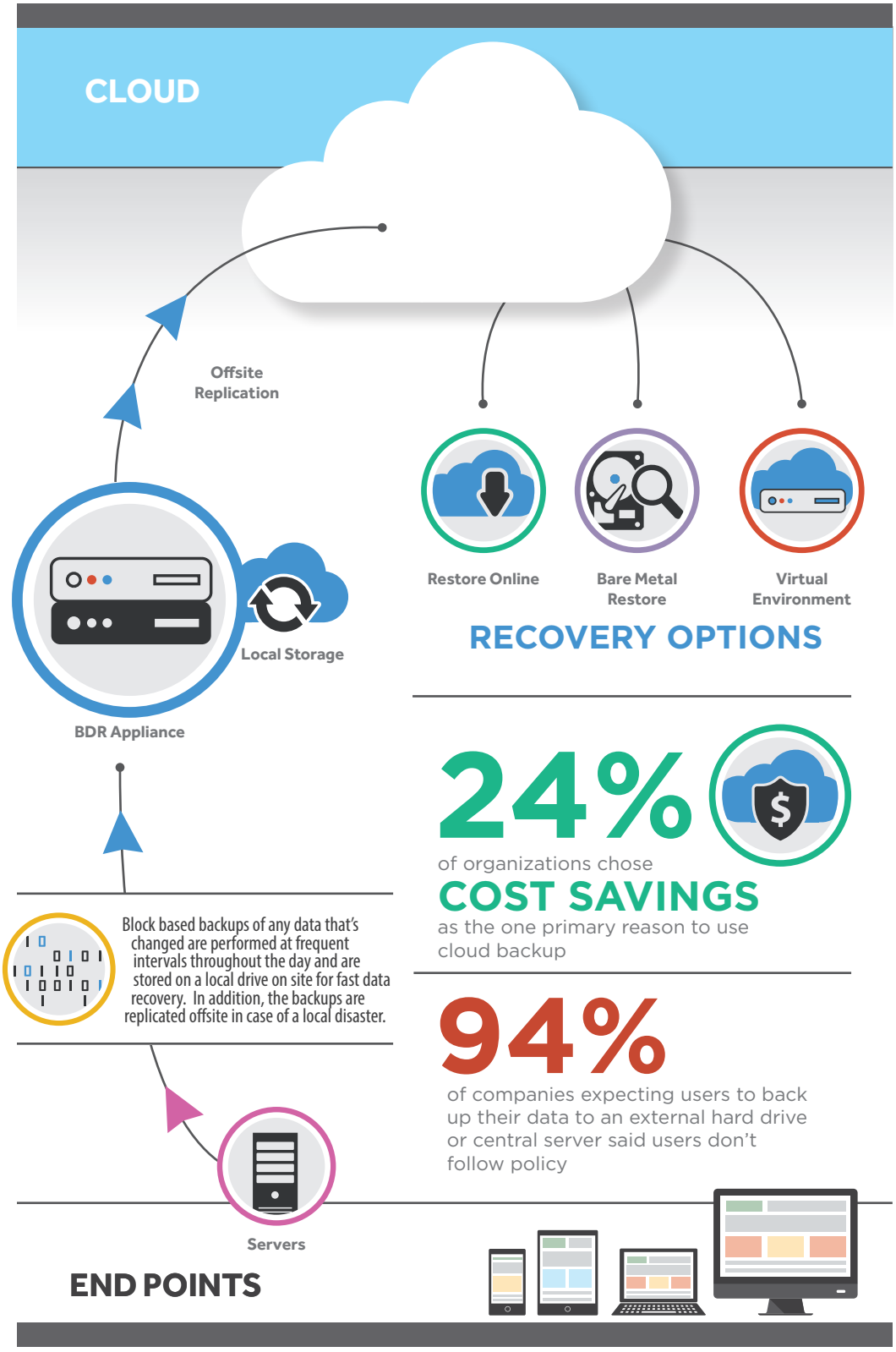
MANAGED SUPPORT & SERVICES

Managed Support & Services is the most efficient way to minimize reactive support and proactively manage your infrastructure. In exchange for a fixed monthly fee, outsourcing support helps improve operations while reducing your overall expense. This detailed analysis page represents an overview of the state of your Base Plan Managed Support & Services. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Managed Support & Services audit score.

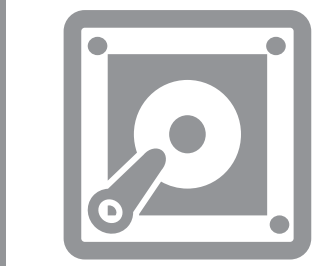
Prepared For: Tempest Fitness
Presented By: Techspert Data Services, LLC

BACKUP & DISASTER RECOVERY

TECHSPERT data services LLC



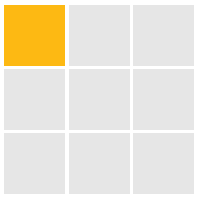
BACKUP & DISASTER RECOVERY



WHY IS THIS IMPORTANT?

Backup & Disaster Recovery (BDR) is one of the most important areas of concern in your IT infrastructure. Everything is working against you ... hackers, viruses, bad weather, hardware malfunction, rogue employees, accidental deletion and the list goes on and on. You need to make sure that your critical data and the servers that they reside on are backed up and highly available with a copy offsite in case of disaster. Traditional tape backups are no longer a viable option and with great BDR offerings available, no small business should ever be down for extended periods of time.

INFRASTRUCTURE

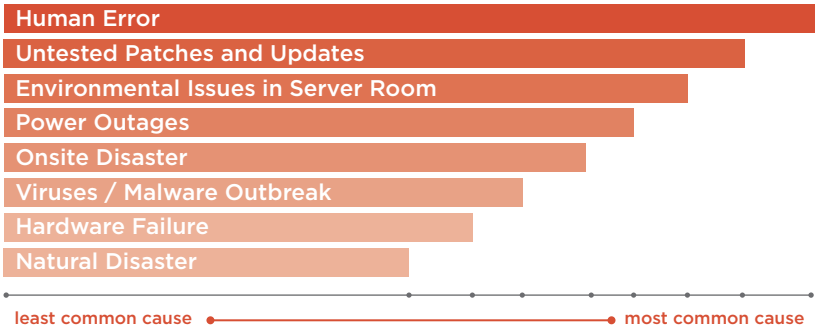


BUSINESS CONTINUITY

TECHSPERT data services LLC

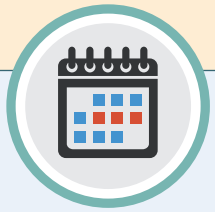
In the absence of business continuity planning, even a minor disruption to critical systems, physical locations or other key resources can halt operations, impact customers or harm the financials of an organization. It's essential for organizations to discuss how an unplanned outage would impact their business and to plan how they need to respond effectively.

Common Causes of System Downtime



48%
of business owners have no business continuity plan in place

84%
of companies experienced one or more instances of system downtime in the previous 12 months



Of those without a business continuity plan:

53%
never recoup the losses incurred by a disaster

51%
fail within 24 months

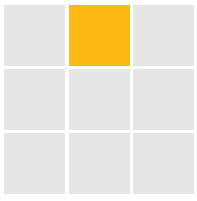
43%
of businesses never reopen after being affected by a disaster

Business Continuity plans differ from Disaster Recovery plans but they are related. Disaster Recovery plans are focused on business recovery following a disaster and help to **mitigate** the negative consequences (such as data loss) of a disaster. In contrast, Business Continuity plans are focused on creating a plan of action to **prevent** the negative consequences of a disaster from occurring at all.

WHY IS THIS IMPORTANT?

There is a big difference between business continuity and backup and disaster recovery. Business Continuity plans help ensure that a business can continue its operations in the event of a natural or man-made disaster. Don't do what 83% of other businesses do and begin planning during a disaster. Be prepared and remember that the best plan is one that works in a variety of scenarios and requires a minimum of change during and after a disaster. With ever increasing cloud computing options, business continuity has become more affordable and easier to implement.

INFRASTRUCTURE

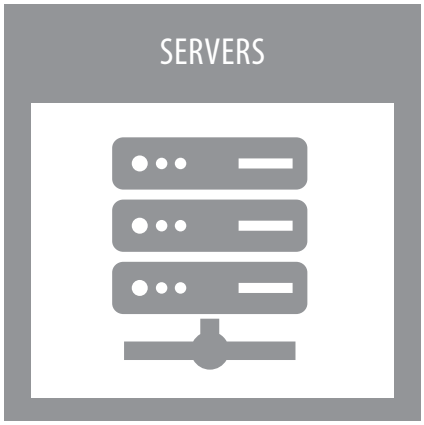


SERVERS

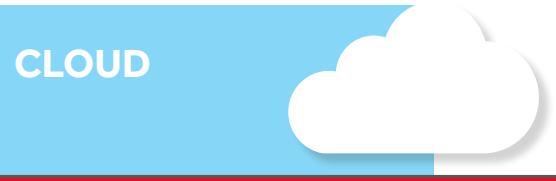
TECHSPERT data services LLC

SERVERS ARE THE FOUNDATIONAL BUILDING BLOCKS OF YOUR IT INFRASTRUCTURE.

Although functions vary, they provide a centralized location for you to store and share your data and enable you to manage security. They can also be utilized to run applications, host your email or to provide specialized functions such as running a database. Whether they are located in your office or in another location such as a data center, the servers need to be properly maintained, patched and secured against unauthorized access.



CLOUD



WINDOWS 2003 SERVER
END OF LIFE
JULY 14, 2015

- No Updates
- No Service Packs
- No Phone Support
- No Web Support

Estimated number of Windows Server 2003 instances running worldwide in 2014: **24 MILLION**

Windows Server 2008 R2

END OF LIFE
JANUARY 14, 2020

Upgrading to a newer server operating system (OS) increases: Performance, Scalability, Availability and Manageability

Migrating to a cloud based server solution improves:
Speed, Resiliency, Cost-Efficiency and Security

Average Server Life Span
3-5 YEARS

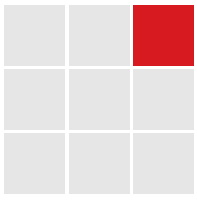
Life cycles are getting shorter due to higher demands from newer technology

END POINTS

WHY IS THIS IMPORTANT?

If your office has server(s) onsite or co-located in a data center, it's important that they run a supported operating system. If not, Microsoft won't release any more security updates or patches and your server could become vulnerable to hackers. In addition, maintaining a valid warranty ensures faster and less costly support from the manufacturer. Owning servers carries a whole host of responsibilities including backup, security, maintenance and, if applicable, adherence to legal and regulatory compliance standards dictated by HIPAA and FINRA.

INFRASTRUCTURE



WORKSTATIONS

TECHSPERT data services LLC

Since 2001, the threat landscape has dramatically changed from unorganized, electronic vandalism to funded, organized theft of personal data, intellectual property and financial information. Protection against these threats begins with modern software and workstations running the latest operating system. Today, many offices allow employees to bring their own devices to the office. While this increases flexibility and productivity and helps lower costs, it also makes your data more vulnerable to attack. Proactively managing all endpoints and ensuring that they are up to date and supported is of paramount importance to your IT infrastructure.

CLOUD

Microsoft Windows xp

WINDOWS XP
END OF LIFE
APRIL8, 2014

Estimated number of machines still running Windows XP

500 MILLION

75 MILLION users have downloaded Windows 10 to their personal computers and tablets in the first month of its release.

Windows 7

WINDOWS 7
END OF LIFE
JANUARY 14, 2020

Windows 7 is 6 TIMES more likely than Windows 8 to be infected by malware

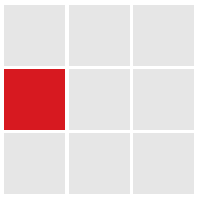
49% of IT professionals plan on upgrading at least some devices to Windows 7 while **7%** plan on upgrading to Windows 8/10

END POINTS

WHY IS THIS IMPORTANT?

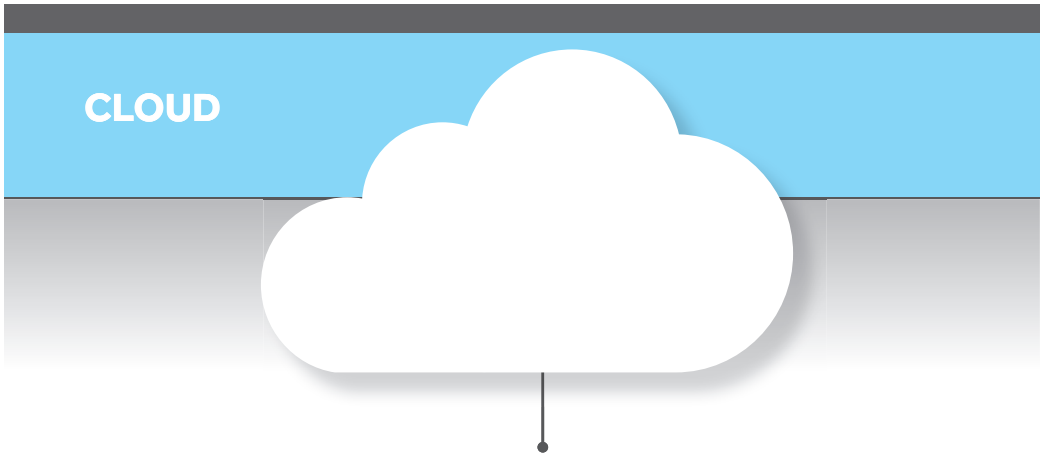
Workstations are the driving force behind technology in your office. It is important that they are running a supported operating system especially if you need to adhere to legal or regulatory compliance guidelines. Maintaining a valid warranty ensures faster and less costly support from the manufacturer. With cloud solutions, offices are able to employ Bring Your Own Device (BYOD) strategies and save money on future upgrades. It's common for end users to not only have a workstation but also a tablet, smartphone and possibly a laptop thereby increasing the threat landscape.

INFRASTRUCTURE



MANAGED WIRELESS

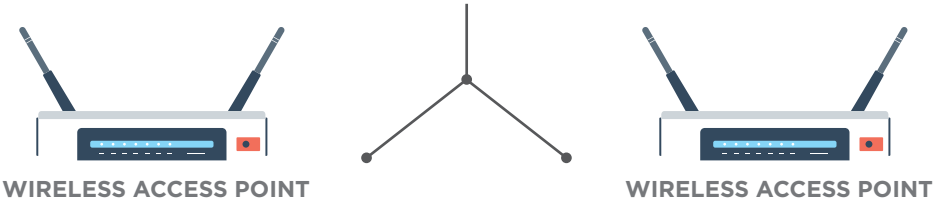
TECHSPERT data services LLC

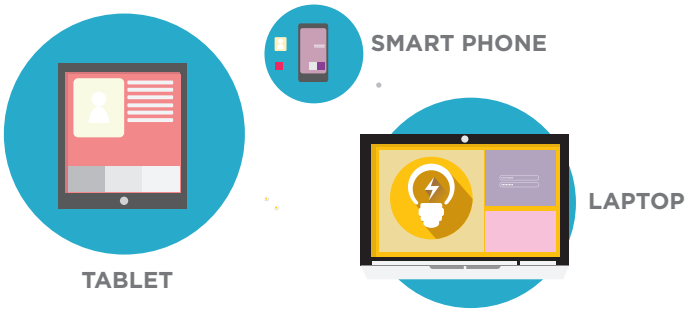


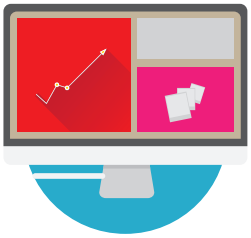
MANAGED WIRELESS

CENTRALIZED MANAGEMENT

Manage multiple wireless access points from a single web-based console.







VISIBILITY AND CONTROL

Ensure consistent security settings and gain real-time visibility into wireless usage.

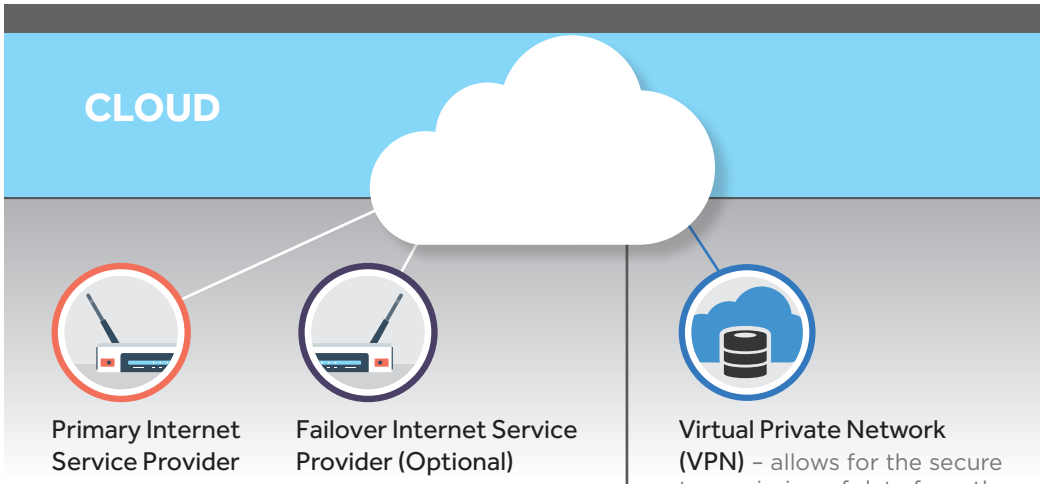
END POINTS

WHY IS THIS IMPORTANT?

Wi-Fi has quickly become a necessity for most businesses. As more and more SmartPhones and tablets are brought into the office, it's now an expectation that wireless access be available. To improve security, many businesses provide a separate wireless guest network for their partners and visitors. Nonetheless, wireless is inherently less secure because it doesn't require a physical connection. Special security considerations need to be made when configuring and providing Wi-Fi and the devices being utilized should be managed and monitored for threats and bandwidth consumption.

INTERNET SECURITY APPLIANCE

TECHSPERT data services LLC



Primary Internet Service Provider

Failover Internet Service Provider (Optional)

ISP Load Balancing – the device can monitor several internet circuits and switch between them in case one of them fails. This increases Internet uptime and automatically provides better availability of cloud services.

Virtual Private Network (VPN) – allows for the secure transmission of data from the internal network to endpoints such as laptops, remote locations and cloud storage.

Internet Security Appliance

A network **firewall** is a hardware based device that acts as a physical layer between the Internet based cloud and protects the internal network from unwanted traffic. It actively blocks traffic that matches predetermined security rules but doesn't inspect anything inside the packets.
Many Internet Security Appliances are enhanced with **Unified Threat Management** and combine other security features with those of the firewall. This provides for a simple solution which is easier to manage and may help meet complex regulatory compliance requirements.

Features include:

Gateway Anti-Virus & Anti-Spyware

Content Filtering

Intrusion Prevention & Detection System

Application Layer Filtering

Reporting

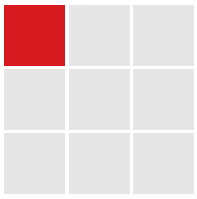
END POINTS

INTERNET SECURITY APPLIANCE

WHY IS THIS IMPORTANT?

An Internet Security Appliance or network firewall is the first line of defense when protecting your network and data from Internet borne threats and outside attackers. The hardware provided by an Internet Service Provider (ISP) or a residential grade router is not enough to effectively protect a business. Implementing a monitored appliance with Unified Threat Management security services activated and up to date is a great start towards ensuring that critical data is protected. If you don't have an Internet Security Appliance, your business is exposed to a myriad of risks.

SECURITY



NEXT GEN ENDPOINT PROTECTION

TECHSPERT data services LLC

CLOUD

A next generation endpoint protection solution needs to stand on its own to secure endpoints against both legacy and advanced threats throughout various stages of the malware lifecycle. Administrators must be confident they can completely replace the protection capabilities of their existing legacy, static-based solution with one labeled as next generation endpoint protection.

CRITICAL COMPONENTS OF A NEXT GEN ENDPOINT PROTECTION PLATFORM

Prevention
Reputation-based preemptive block & prevention polices - Protect from known threats

Dynamic Exploit Detection
Protect from app and memory based exploits, drive by downloads

Dynamic Malware Detection
Full system monitoring to protect from evasive, packed malware, social engineering/spear phishing

Mitigation
Quarantine files and endpoints

Remediation
Automatic remediation to undo system changes

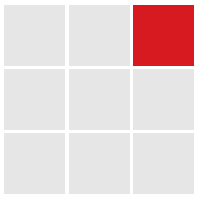
Forensics
Real-time analysis & root cause forensic investigation

END POINTS

WHY IS THIS IMPORTANT?

Effective protection against modern, sophisticated threats requires an innovative approach in the way they are detected, blocked, mitigated, remediated and analyzed. With less threats being comprised of file-based malware, signature-based antivirus and other static solutions could be considered inadequate protection. A next generation endpoint protection (NGEPP) solution protects against all major types of cyberattacks and doesn't depend on signatures or heuristic file analyses. NGEPP detects threats dynamically, based on behavior and protects endpoints across all attack vectors.

SECURITY



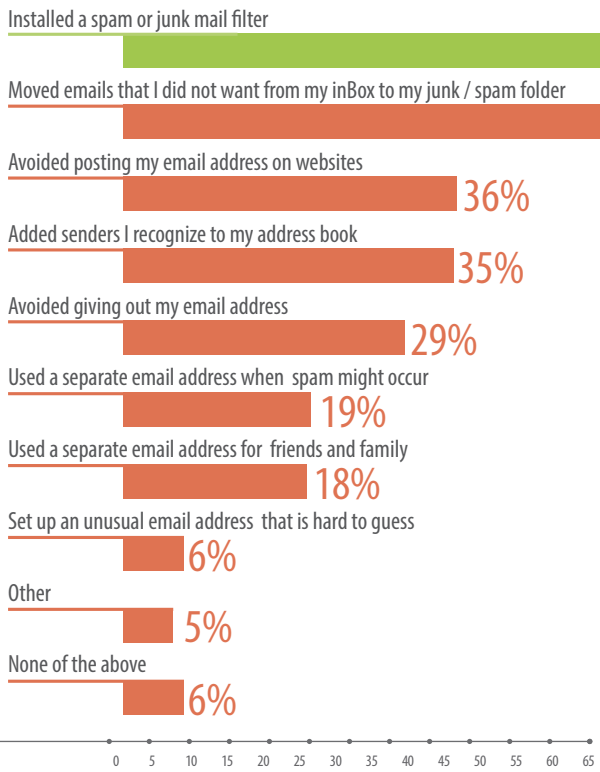
ANTI-SPAM & VIRUS FILTER

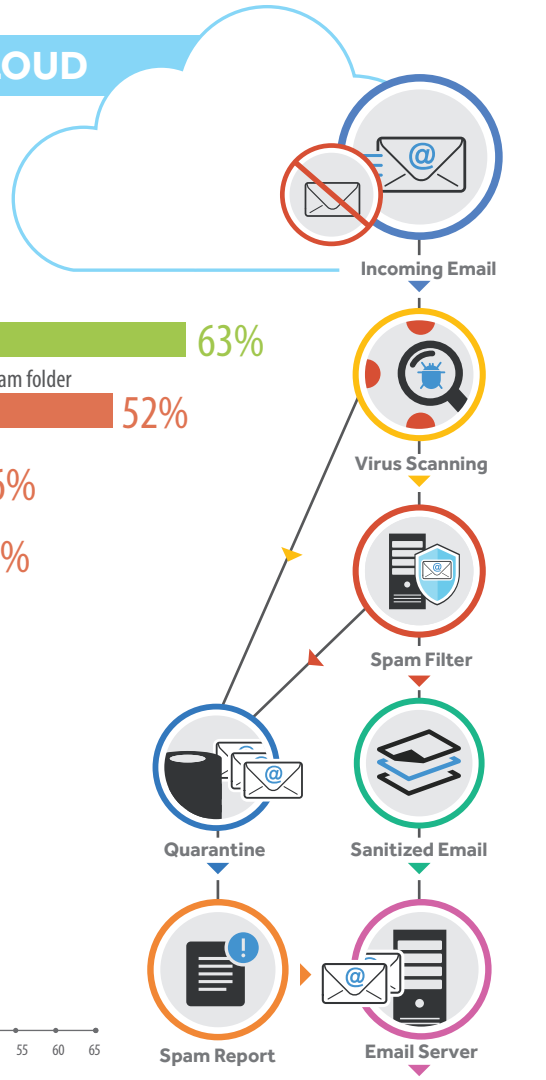
TECHSPERT data services LLC

SINCE 2001, THE THREAT LANDSCAPE HAS DRAMATICALLY CHANGED

from unorganized, electronic vandalism to funded, organized theft of personal data, intellectual property and financial information. Protection against these threats begins with modern software and workstations running the latest operating system. Today, many offices allow employees to bring their own devices to the office. While this increases flexibility and productivity and helps lower costs, it also makes your data more vulnerable to attack. Proactively managing all endpoints and ensuring that they are up to date and supported is of paramount importance to your IT infrastructure.

HOW DO YOU KEEP YOUR INBOX FREE OF SPAM?



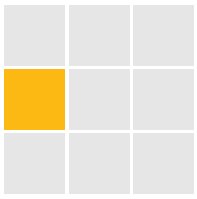


END POINTS

WHY IS THIS IMPORTANT?

One of the main ways viruses and other malware infiltrate a network is through email. With so much riding on the high availability of an electronic communication system, it is important to add a 3rd party layer of filtered protection. Most filters will allow for the simple release of quarantined messages and include a daily report of held email for review. You should consider a filter separate from your email server or hosted provider. That way, if there is any type of outage and email can't be delivered, your anti-SPAM filter will hold the messages and deliver them when the server becomes available.

SECURITY



E&O INSURANCE

TECHSPERT data services LLC

ERRORS & OMISSIONS (E&O) INSURANCE

Errors & Omissions insurance, otherwise known as Professional Liability Insurance, is often overlooked by IT providers. Although there is no standard form, E&O insurance protects your IT provider from claims of professional negligence or failure to perform their professional duties. These could include loss of your data, software or system failure, claims of non-performance or the negligent oversell of products or services. It's important to note that these types of claims are NOT covered by General Liability insurance.

At a minimum, make sure your IT provider is covered for:

- **Client Data Loss**
  Covers the costs of recovering or restoring lost data
- **Network Security Liability**
  Covers the inadvertent transmission of a virus or the failure to prevent unauthorized access to computer systems by a third party or unauthorized employee
- **Breach of Contract**
  Covers the costs related to your IT provider's failure to fulfill their contractual obligations
- **Independent Contractors**
  Covers any independent contractors that your IT provider may utilize

In addition, your IT provider should carry a **Cyber Liability** policy with the following coverages:

- **Privacy Liability** – covers the disclosure or misuse of Protected Health Information and Personal Identifying Information
- **Privacy Breach Notification Costs** – covers the costs to provide notification to the individuals who are required to be notified by the applicable Breach Notification Law
- **Forensic Expense Coverage** – covers the costs to hire a computer security expert to determine the existence and cause of any electronic data breach
- **Crisis Management Expense** – covers the costs of a public relations consultancy for the purpose of averting or mitigating material damage
- **Regulatory Defense / Penalties Coverage** – covers the claims expenses and penalties which you are legally obligated to pay because of any claim in the form of a regulatory proceeding resulting from a violation of a Privacy Law

You should consider your own Cyber Liability policy to protect yourself from a rogue employee, staff errors and lost or stolen unencrypted laptops and mobile devices.

WHY IS THIS IMPORTANT?

Unlike other regulated industries, there's nothing that requires your IT provider to purchase coverage for errors & omissions (E&O) or other forms of cyber liability insurance. You should make sure that your IT provider has adequate coverage for the services that they provide or your business could be exposed to serious risk without any ability to seek reasonable financial restitution. Without E&O insurance containing the proper coverages, most IT providers lack the financial resources to absorb heavy losses from lawsuits and the costs to defend them. If you're unsure if you're protected, ask your IT provider for a Certificate of Insurance for their Cyber Liability E&O policy.

MANAGED SUPPORT & SERVICES

Prepared For: Tempest Fitness
Presented By: Techspert Data Services, LLC