



SYNERGY

IT SOLUTIONS

The background features a collage of office scenes, including server rooms with rows of monitors and call centers with employees at desks. These images are framed by a series of overlapping hexagonal outlines in a golden-yellow color.

2023 Network Assessment **Executive Summary**



Introduction

At the request of our client, Synergy IT Solutions conducted a full IT Network Assessment. That assessment included an Enterprise Network Infrastructure Discovery and Assessment, Virtualization & Storage Systems Discovery, Backup & Disaster Recovery Assessment, and Essential Security Preview and Internal Vulnerability Assessment. This report summarizes the findings from those assessments which were conducted over a period of 3 months.

Overview

In general, we would characterize the state of the client's information technology platform as fair. With the speed of business technology evolution, companies will need to expand their adoption of digital solutions to meet stakeholder demands, and this client is no exception. As you develop your technology plan and set your priorities, we believe you should consider the following key findings and recommendations to ensure your technology infrastructure is up to industry standards and best practices.

Key Findings

Below is a summary of our key findings by Assessment Area.

- **Network Infrastructure** – By making some targeted improvements in its network, the company could significantly increase performance, stability, resilience, and security which would lead to operational efficiencies through improved end-user performance and reduced downtime.
- **Virtualization & Storage Systems Discovery** – Largely, the client's virtualization and storage systems are supporting its mission critical application access and availability which in today's environment of work from anywhere is crucial.
- **Backup & Disaster Recovery Assessment** – The current disaster recovery solution is considered acceptable; however, it does not protect against a regional disaster. Beyond that, we would expect a company of this size and scope to have a documented disaster recovery plan in place.
- **Essential Security Preview and Internal Vulnerability Assessment** – With the nature the current security environment, it is critical for companies that store personal data to uphold a high level of network security and maintain constant vigilance of evolving threats.

Recommendations

As is typical in an assessment like this, the number of recommendations for improvement is not insignificant. Our goal is always to ensure our recommendations separate wants from needs and provide a roadmap to consider as you develop a plan to bring the company up to industry standards. As with the key findings, our recommendations are organized by assessment area.



Networking Infrastructure

Essential

1. Review physical wiring requirements for change from Tree Topology to Star Topology
2. Replace End-of-Life Switching Equipment
3. Replace End-of-Life Wireless Equipment
4. Implement Redundant Firewalls
5. Implement Backup ISP
6. Harden Network Management Protocols
7. Implement Black Hole VLAN
8. Correct identified switch trunk port setting mismatches.
9. Remove the VLAN 1 (192.168.1.X) addresses from the access switches in favor of the 10.1.1.X management VLAN

Recommended

1. Implement Network Access Control system for secure access with least privilege.
2. Implement 802.1x authentication on internal networks.
3. Implement internal firewall policies limiting traffic between VLAN's and offices for least privilege.
4. Implement Egress filtering on the firewalls.
5. Investigate SD-WAN as a cost savings.
6. Implement a DMZ design for published servers.

Storage and Virtualization

Essential

1. Configure multiple data stores for performance and protection.
2. Upgrade switching to 10GB backbone for performance and redundancy.
3. Upgrade VMware vSphere to 8.0 U2 or >

Recommended

1. Consider Cloud Based Virtual Desktop Solution

Backup & Disaster Recovery

Essential

No recommendations

Recommended

1. Document/Formalize a Business Disaster Recovery Plan
2. Consider Cloud Services such as Azure Site Recovery & Reserved Instances



Security

Essential

1. Upgrade or Replace Devices with Unsupported Operating Systems
2. Endpoint Protection Inconsistencies – Install and review server deployment process.
3. Address Account Lockout & Screen Lock
4. Review External Vulnerability Scan Results
5. Review Internal Vulnerability Scan Results
6. Unrestricted Outbound System Traffic
7. Unsecured WiFi Networks
8. Apply Security Policies to Computers vs. Users
9. Create GPO to disallow password storage in browser cache.
10. Address Password Vulnerabilities
11. Review Privileged Account / Service Account Use
12. Review Shared / Generic Account Use
13. Active Directory Hygiene / Cleanup
14. Review Equipment Replacement Prioritization (Servers / Endpoints / Switching / Wireless)
15. Review User Login Reports
16. Review Data Breach Liability Report

Recommended

1. Develop formal Written Information Security Policies (aka WISP)
2. Migrate to Microsoft Exchange Online

Estimated Cost

To assist the client in its planning process, we are providing the estimated cost of the above recommendations.

Recommendation	Estimated Cost
Configure Multiple Datastores	
Estimated Implementation: IT Advisor Services	\$XXX.XX
Upgrade VMware to vSphere 8.X	
Estimated Implementation: IT Advisor Services	\$XXX.XX
Network Cabling	
Network Cabling Required to Configure Star Topology	\$XXX.XX
Replacement Networking Infrastructure	
Network Switching Equipment	\$XXX.XX
Estimated Installation & Customization: IT Advisor Services	\$XXX.XX
Replacement Wireless Networking	
Wireless Equipment	\$XXX.XX
Estimated Installation & Customization: IT Advisor Services	\$XXX.XX



Recommendation	Estimated Cost
Replace End-Of-Support OS/Desktops & Laptops	
Desktop / Laptop Hardware Estimate	\$XXX.XX
Implement Redundant Firewall	
Fortigate-201F w/3Yr 24x7	\$XXX.XX
Estimated Installation & Customization: IT Advisor Services	\$XXX.XX
Implement Backup ISP	
Secondary Internet Service Provider	\$XXX.XX
Estimated Implementation: IT Advisor Services	\$XXX.XX
Implement Black Hole VLAN	
Estimated Implementation: IT Advisor Services	\$XXX.XX
Correct identified switch trunk port setting mismatches.	
Estimated Implementation: IT Advisor Services	\$XXX.XX
Remove the VLAN 1 (192.168.1.X) addresses from Access switches.	
Estimated Implementation: IT Advisor Services	\$XXX.XX

Recommendation	Estimated Cost
Recommended Action Items	
Disaster Recovery Workshop	\$XXX.XX
Cybersecurity WISP Program - Security Policy Development	\$XXX.XX
Migrate to Exchange Online	
- MS Business Premium License - Annual	\$XXX.XX
- Estimated Implementation Services	\$XXX.XX
Suggested Improvements	
Implement Network Access Control System	\$XXX.XX
Implement 802.1x authentication on internal networks. (If no NAC)	\$XXX.XX
Implement internal firewall policies limiting traffic between VLAN's and offices for least privilege.	\$XXX.XX
Implement Egress filtering on the firewalls.	\$XXX.XX
Investigate SD-WAN as a cost savings. - Consulting	\$XXX.XX
Investigate a DMZ design for published servers. - Consulting	\$XXX.XX
Future Considerations	
Azure VDI Proof of Concept	\$XXX.XX