REPORT

Contoso

Azure Tenant Assessment Report

March 27, 2024

ACCELERATING DIGITAL TRANSFORMATION

U.S. HEADQUARTERS
3 SEAVIEW BOULEVARD
PORT WASHINGTON, NY
11050

AGILANT
SOLUTIONS INC

1 DOCUMENT CONTROL

APPROVAL

The signatures below certify that this document has been reviewed & accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

	Name	Position
Prepared by	Steven Forti	Chief Information Security Officer
Prepared by	Vincent Gulino	Senior Security Architect
Reviewed by	Harry Taluja	Chief Technology Officer
Reviewed by	Katie Riley	Sr. Director, Business Development & Marketing

AMENDMENT RECORD

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page No.	Context	Revision	Date

COMPANY PROPRIETARY INFORMATION

The electronic version of this document is the latest revision. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this manual is uncontrolled, except when provided with a document reference number and revision in the field below:

Document Ref. _____ Rev _____

Uncontrolled Copy [•] Controlled Copy [ ] Date _____

2 EXECUTIVE SUMMARY

Contoso Financial Services (herein "Contoso") engaged Agilant Solutions, Inc. (herein "Agilant") to conduct comprehensive vulnerability assessments of their Azure cloud infrastructure, consisting of seven (7) servers, three (3) AVD desktops, and three (3) remote surface pro devices.

The test scope included the following elements:
1. External vulnerability assessment
2. Inside vulnerability & penetration assessment
3. Malware readiness assessment
4. End point security configuration review
5. Firewall gateway configuration review

Overall, Contoso's security posture proved very robust and capable of defending the company assets against outside intrusion. As noted below, although medium level vulnerabilities were discovered, they were mitigated by the presence of other controls which closed any gaps.

In addition to tight controls and well-placed security-focused products & services in the network, Contoso leverages the services of a 24/7 security operations center. This appears to be very effective in responding to alerts generated by endpoint systems designed to protect the organization (i.e.: CrowdStrike).

While testing the effectiveness of the local endpoint security solution, our consultants were discovered and shut out within minutes, despite performing tasks which would not be considered highly suspicious (i.e. benign usage of "live off land" binaries such as certutil.exe and hh.exe).

This demonstrates that:
1. The endpoint solution is properly configured to capture events which could be a pathway to future hostile activities.
2. The monitoring company is watching alerts in real-time and responding to those alerts in an effective manner.

3 SCORECARD

GRADING CRITERA		
Examination	**Security**	**Grade**
External Vulnerability Assessment	**Excellent**	**A**
Inside Penetration Test	**Very Good**	**B**
Malware Readiness	**Excellent**	**A**
Endpoint Configuration Review	**Excellent**	**A**
Firewall Gateway Review	**Good**	**C**

4 USING THIS REPORT

This report contains several sections that are helpful to different groups of people.

- The **Scope** describes the boundaries of the vulnerability assessment.
- The **Risk Assessment** evaluates the probability of the worst-case scenarios.
- The **Findings & Recommendations** contains detailed information on the vulnerabilities identified during the assessment. The findings are structured in a table format so they can be placed into other reports. This allows Contoso to give area owners only the findings that pertain to their security responsibilities. Our consultants provide priority guidance on what they deem should be addressed based on ease of implementation and overall effectiveness of change.

5 SCOPE

This report covers the inside section and the tasks conducted were as follows:

- Conduct Kickoff Meeting: Agilant conducted a kickoff meeting with CONTOSO technical staff prior to testing to review the objectives of the internal vulnerability assessment, to obtain any additional required information, and to exchange contact information.
- Determine the overall impact on customer assets.
- Review final report with the customer to determine an appropriate action plan

6 LEVELS OF RISK

Agilant risk ratings are defined as follows:

Critical – The exposure is the most damaging of the high-risk vulnerabilities. These weaknesses are typically exploited by self-propagating worms and have a myriad of publicly available exploit code on the Internet.

High – The exposure may be exploited to produce adverse outcomes such as unauthorized privilege escalation, denial of service, data access, more than one percent downtime per month, or compromise of data. A high-risk rating is given to vulnerabilities where ease of exploitation and impact of exploitation are both high.

Medium – The exposure, when combined with other exposures, may be exploited to produce adverse outcomes such as downtime, system compromise, unauthorized privilege escalation, or unauthorized data access. A medium risk may also indicate a condition that does not expose the system to immediate risk but may expose the system to risk in the future or is a deviation from best practices which could ultimately lead to negative outcomes from a regulatory and/or insurance-based perspective.

Low – The exposure does not contribute to a near-term adverse outcome, but provides further information about the system, application, or network.

Attention – A finding rated as Attention does not have a risk high enough to be called a Low Risk finding. Rather, it is a finding that should be considered to improve security from an already acceptable level. Agilant believes appropriate risk mitigation and security controls exist within the system tested, but security could be further improved with the recommendations provided.

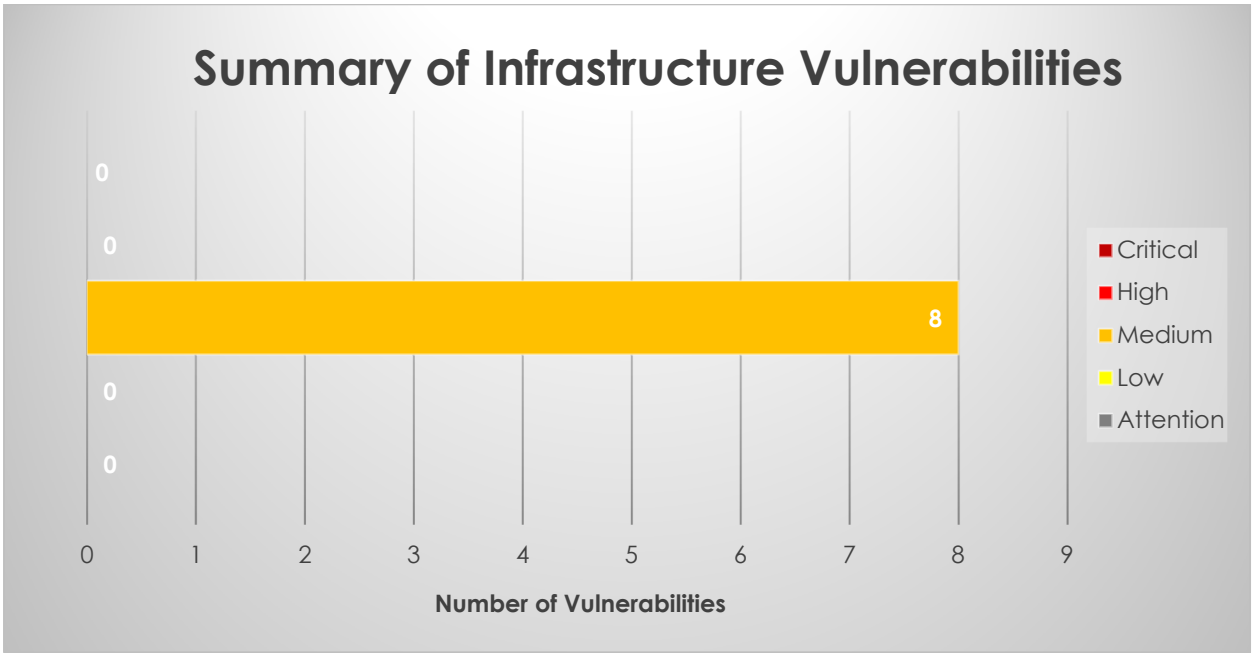
7 CONSOLIDATED SUMMARY OF FINDINGS

While performing the internal penetration test, the Agilant consultants revealed several areas of concern and several vulnerabilities that customer should address. The most critical findings fall within the following categories:

- Configuration parameters
- Device/software version
- Allowed & disallowed services
- Device/software support & age
- Patch Management

7.1 Summary of Infrastructure Vulnerabilities

This chart illustrates the number of vulnerabilities found during the internal penetration test. Details on the specific vulnerabilities are included in the "Findings and Recommendations" section below.



8 METHODOLOGY

8.1 Vulnerability Testing

Agilant conducted network-based vulnerability testing of the infrastructure and blind, unauthenticated testing of web applications. The objective of the penetration testing was to identify security weaknesses that could be exploited by motivated, malicious individuals to gain unauthorized access to the infrastructure. Where a flaw was identified, Agilant sought to verify the presence of said vulnerability through repeated scans using a variety of tools capable of testing for the same type of vulnerability. We used a series of vulnerability scanning tools and manual techniques to identify, validate, and exploit security vulnerabilities.

Testing was conducted in three phases: Discovery, Vulnerability Identification and Verification.

Phase I: Discovery
Agilant performed reconnaissance to gather information including registration data, operating system version and patch level, and service version and configuration.

Phase II: Vulnerability Identification
Agilant used a combination of commercial and open-source tools to identify security vulnerabilities in tested systems.

Phase III: Verification
Vulnerabilities identified by these tools were confirmed by our security staff to ensure there were no false positives.

8.1.1 Network & Web Vulnerability Tests

Agilant performed base-level security scans of all the hosts to identify services and issues within these services. Once this was complete, manual techniques were employed to identify risks that automated tools cannot identify.

The testing techniques included:

- DNS Queries: Query Name databases such ARIN to obtain domain names, IP address block assignments, and registrar information.
- Host Identification: Identify live hosts through ICMP, Reverse DNS, and port scans for common services.
- Network Route Mapping: Map the network route to each system using trace route and Visual Route.
- Operating System Identification: Identify the operating system of each host through analysis of responses to specially crafted TCP/IP packets.
- Network Services Enumeration: Enumerate the services available on each system through TCP and UDP port scanning by using tools such as NMAP.
- Network Service Exploration: Build a detailed profile of each service through automated and manual banner grabbing and service exploration without exploiting any service vulnerabilities.
- Vulnerability Identification: Use commercial and open-source vulnerability scanners to identify known vulnerabilities on each system.
- Vulnerability Exploitation: Use commercial, open source, and private exploitation tools and methods to gain access to the system or sensitive data.
- Agilant performed unauthenticated functional security testing of identified applications and attempted to gain unauthorized access to the application, hosting system, and sensitive data. The testing techniques included:

- Input validation bypass: Client-side validation routines and bounds-checking restrictions were removed to ensure controls are implemented on all application parameters sent to the server.
- SQL injection: Specially crafted SQL commands were submitted through input fields to validate whether input controls were in place to properly protect database data.
- Cross-site scripting: Active content was submitted to the application to cause a user's web browser to execute unauthorized and unfiltered code. This test was meant to validate user input controls.
- Parameter tampering: Query strings, POST parameters, and hidden fields were modified to gain unauthorized access to user data or application functionality.
- Cookie poisoning: Data sent in cookies was modified in order to test application response to receiving unexpected cookie values.
- Session hijacking: Agilant Security Solutions attempted to hijack a session established by another user to assume the privileges of that user.
- User privilege escalation: Agilant Security Solutions attempted to gain unauthorized access to administrator or other users' privileges.
- Credential manipulation: Agilant Security Solutions modified identification and authorization credentials to gain unauthorized access to other users' data and application functionality.
- Forceful browsing: Agilant Security Solutions enumerated files located on a web server to access files and user data not explicitly shown to the user within the application interface.
- Backdoors and debug options: Many applications may contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making it a target for potential exploitation. Application developers may leave backdoors in their code. Agilant Security Solutions identified these options that could potentially allow an intruder to gain additional levels of access.
- Configuration subversion: Improperly configured web servers and application servers are common attack vectors. Agilant Security Solutions assessed the software features, as well as the application and server configuration, for poor configurations.

8.1.2 Common Tools

- Commercially available & open-source tools including, but not limited to:
  - kali Linux
  - Parrot Os
  - Blackarch
  - Nessus
  - Openvas
  - Nexpose
  - Vooki
  - Arachi
  - Burp Suite
  - ZAP proxy
  - Nmap
  - Masscan
  - ike-scan
  - Metasploit
  - Ikeprobe
  - Nikto
  - in-house developed tools
  - dig
  - WMIC

9 TECHNOLOGY FINDINGS & RECOMMENDATIONS

In this section, Agilant details individual infrastructure findings for Contoso's vulnerability assessment. Vulnerabilities are listed in order of importance with critical issues first and low risk issues last. Within each table is the name of the finding, a finding reference number, and the risk rating of the finding. The finding contains a description of the finding, the impact if successful exploitation of the finding is realized, and any sample data or screenshots that accompany the finding. Finally, Agilant suggests recommendations to limit the impact or successful exploitation of the finding.

9.1 Findings

9.1.2 Perimeter Outside Infrastructure remote devices

Synopsis – This portion of our examination tested the outside surface pro devices used to connect into the azure network via the public internet. During our examination no observations were noted on the 3 public IP addresses provided.

9.1.3 Anti-Malware and Firewall review

Synopsis – The purpose of this portion of our examine was to evaluate perimeter controls to determine how well devices positioned between the trusted and trusted networks (i.e. PC infrastructure and the internet) performed with respect to protecting the internal network from malware, rootkits, botnets & phone home viruses.

Vulnerability	**No SSL interception & deep inspection configured at perimeter**					
Synopsis	Our internal to external testing revealed no Intercepting SSL certificate exists					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	All addresses	HTTPS				
Description						
The vast majority of botent, C&C service communication and malware callbacks are conducted over encrypted SSL channels which can completely bypass IP/content filtering solutions which do not perform deep SSL inspection						
Solution						
Configure SSL interception on all outgoing connections so the firewall/ips can examine SSL encrypted traffic for dangerous traffic patterns.						
Additional Resources						
none						
Comments						
This finding is mitigated by the fact that local endpoint solution (CrowdStrike) effectively neutralized all efforts to download code to the endpoint using SSL. Would normally be considered a high risk finding						

Vulnerability	No perimeter blocking of known viruses					
Synopsis	No perimeter device was able to detect viruses which were downloaded into our sandbox environment					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	All addresses	all				
Description						
Several viruses including the famous Eicar test virus were downloaded to our sandboxed laptop as part of the testing. These files made it to the local host over an https encrypted channel and were never intercepted by any inline device. During the insider threat portion of the exam the famous Mimikatz was download to our locally installed appliance via browser and web.client session commandlet without restriction						
Solution						
Configure SSL interception and keep virus signature files up-to-date on perimeter devices						
Comments						
This finding was mitigated by the fact that the endpoint solution effectively neutralized all of these files before a download to the client was completed. Would normally be considered a high risk finding						

Vulnerability	No perimeter blocking of executable content					
Synopsis	Perimeter devices allow the downloading of executable content					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
I	All addresses	all				
Description						
During the examination a variety of file types including **.exe,.wsh,.ps1,.bat,.com,.scr,.vbs** were downloaded successfully for our sandbox over both http and https methods.						
Solution						
Configure the firewall to block executable content and dangerous file types						
Comments						
This finding was mitigated by the fact that the endpoint solution effectively neutralized all of these files before a download to the client was completed. Would normally be considered a high risk finding						

Vulnerability	Unrestricted outbound access					
Synopsis	Egress firewall rules appear to allow any any					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	All addresses	all				
Description						
During the examination our consultants tested outbound communication to our tcp/udp port towers and found all tcp and udp ports are accessible through the firewall. This allows easy access for hackers to establish call back connections to bot net servers and command and control systems which could bypass content inspection tools						
Solution						
Examine business need for all outbound tcp and udp communication and craft rules based upon business need. This is normally done by capturing outbound firewall traffic for a period of 90 days and then building a protocol group for outbound accept firewall rules.						
Additional Resources						
none						
Comments						
This finding was mitigated by the fact that the endpoint solution effectively neutralized all of these files before a download to the client was completed. Would normally be considered a high risk finding						

Vulnerability	Reverse shells possible over TCP & UDP					
Synopsis	Firewall not fully aware of tcp protocol parameters					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	All addresses	all				
Description						
During our examination our consultants were able to execute reverse shells through the firewall over tcp ports 80 and 443 via Netcat as well as UDP port 123. This reverse shell will bypass the need for a NAT translation and allow full remote-control sessions with a minimal footprint much the same way as teamviewer without the need to install software and/or make adjustments to the firewall						
Solution						
Make sure firewall and/or content filter has protocol awareness and configure unknown protocols to generate alerts for further investigation. NGFW (Next Gen Firewalls) such as the Fortigate and Palo Alto have what is known as "APP-ID" for this exact purpose.						
Additional Resources						
none						
Comments						
This finding was mitigated by the fact that the endpoint solution effectively neutralized all of these files before a download to the client was completed. Would normally be considered a high risk finding						

Vulnerability	Access to countries considered a significant threat					
Synopsis	Outbound communication to outside countries considered risky was possible from our internal host					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	All ip address					

Description

As part of our testing our consultants attempted to initiate connections to the top countries known for distributing malware: **Brazil, Iran, North Korea, Russia, China, Hungary, Italy, Romania**

Of the countries listed above we were able to successfully connect to hosts in all of them. This is potentially dangerous as an attacker who gains a foothold into the network will initiate connections back to themselves for further exploitation.

https://www.cyberyug.com/post/top-10-countries-with-most-hackers-in-the-world

Solution

Consider country blocking at the Palo Alto firewall in the same manner the other listed countries are being blocked

Additional Resources

Comments

This finding was mitigated by the fact that the endpoint solution effectively neutralized all of these files before a download to the client was completed. Would normally be considered a high risk finding

9.1.4 Inside Penetration test

Synopsis – The purpose of this portion of our examination was to evaluate the settings, patch levels, and hardening techniques which exist on windows hosts. The overall objective here is to determine if the windows systems in use can be easily compromised through a virus attack, Trojan and or targeted protocol attack

Vulnerability	**Tomcat version less than 9.0.31**					
Synopsis	Multiple vulnerabilities discovered in the version of Tomcat installed					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	0.0.0.0					
Description						
The installed version of Tomcat is prone to multiple vulnerabilities. See cve details link below for the full listing of findings discovered in this version of tomcat.						
Solution						
Update to version 9.0.31						
Additional Resources						
https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/version_id-644763/Apache-Tomcat-9.0.30.html?page=1&year=2020&order=1&trc=10&sha=dff13bd2311d5be773169caf51985d486efe7737						
Comments						
The one public exploit for this finding (CVE-2020-1938) was not effective in gaining access to this system. Based on this information this finding is rated as a Medium as 2020-1938 is the only high-risk vulnerability with exploit code available listed within the vulnerability bundle. This vulnerability should still be considered important and an upgrade should be planned.						

Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection					
Synopsis	Usage of deprecated TLSv1.0 and/or TLSv1.1 protocol on this system					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	0.0.0.0					
Description						
The hosts listed above leverage outdated SSL protocols						
Solution						
Ensure the systems listed above use TLS 1.2 and disable older protocols if possible						

9.1.5 Endpoint Configuration Review

Synopsis – The purpose of this portion of our examination was to login to local AVD workstations and perform tasks an intruder might normally perform once user level access was obtained though some alternative attack mechanism such as phishing.

Once on the workstation several attempts to download code which would help to elevate privileges were made. These attempts were immediately blocked by the local endpoint solution. Afterward several attempts were made to download benign files using utilities which would not normally be in use for such activities. Within minutes the local account was shut down and an alert sent to the IT staff.

No findings observed during this portion of the exam

10 RISK ASSESSMENT MATRIX

Vulnerability	Likelihood	Impact	Asset	Mitigating Control	Mitigating Control Effectiveness	Residual Risk
Malware infection and network compromise, ransomware, trojans	High	High	Computer network & hosts,	CrowdStrike, SOC	Highly Effective	Low
Malware infection and network compromise, ransomware, trojans	High	High	Computer network & hosts,	Firewall	**Improvement recommended**	Remains low
Privilege escalation on windows hosts via OS and application vulnerabilities	High	High	Workstations and servers	CrowdStrike, SOC	Highly Effective	Low
Deep penetration into internal network through web-based vulnerabilities	High	High	Computer network	Firewall, Inline IPS	Highly Effective	Low

11 SUMMARIZED CONCLUSIONS

As noted in the Executive Summary, despite the existence of software vulnerabilities which are inherent in nearly every organization of similar size and scope, our examination revealed a strong and mature security program which requires a few enhancements to be even more effective at combating next generation threats which are constantly evolving.