

Security Checkup Report

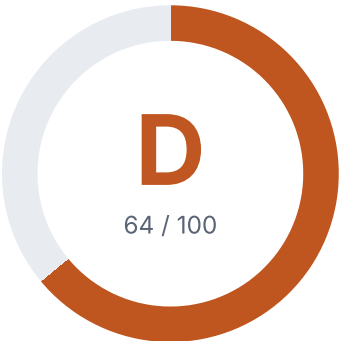
Bayou City Dental (SAMPLE) · October 16, 2026

Prepared by

Arauz Tech Security

hello@arauzatech.com | (281) 826-1372 | arauzatech.com

Significant risks that should be fixed as soon as possible.



3

Action required

12

Needs attention

9

Passed

Computer FRONTDESK-01 · Dell Inc. OptiPlex 7010

Windows Microsoft Windows 11 Pro (build 22631)

Network Workgroup: WORKGROUP

Scanned Oct 16, 2026 9:45 PM as FRONTDESK-01\reception

Top priorities

- 1 Hard drive is encrypted (BitLocker) HIGH**
If the laptop is lost or stolen, files cannot be read without the key.
Fix: Turn on BitLocker (Settings > Privacy & security > Device encryption, or Control Panel > BitLocker) and save the recovery key somewhere safe OFF the computer.
- 2 Firewall is on for every network type HIGH**
Blocks attackers on the same Wi-Fi or network from reaching the PC.
Fix: Windows Security > Firewall & network protection > turn on the firewall for Domain, Private and Public networks.
- 3 Password minimum length MEDIUM**
Short passwords can be guessed or cracked in minutes.
Fix: Set a minimum of 12 characters: run as admin net accounts /minpwlen:12 (or via Group Policy / Intune for business accounts).
- 4 Windows version is still supported CRITICAL**
Unsupported Windows no longer gets security fixes.
Fix: Settings > Windows Update > install the latest Windows 11 feature update.
- 5 Security updates installed recently HIGH**
Most attacks exploit holes that already have a free fix.
Fix: Settings > Windows Update > Check for updates, install everything, and restart.

- 6

Remote Desktop is secured

HIGH

Exposed Remote Desktop is a top way ransomware gangs break in.
Fix: If not needed, turn it off (Settings > System > Remote Desktop). If needed, make sure port 3389 is NOT open on the router - use a VPN instead.
- 7

Everyday account is not an administrator

HIGH

Malware gets full control of the PC if the user who opens it is an admin.
Fix: Create a separate admin account for installs, and change the everyday account to a Standard user (Settings > Accounts > Other users).
- 8

Credential theft protection (LSA)

MEDIUM

Makes it much harder for attackers to steal saved passwords from memory.
Fix: Windows Security > Device security > Core isolation > turn on "Local Security Authority protection", then restart.

Detailed results

Malware protection

STATUS	CHECK	RISK
Pass	Antivirus is installed and running Active: Windows Defender	CRITICAL
Pass	Virus definitions are up to date Definitions are 1 day(s) old.	HIGH
Pass	Tamper Protection is on Tamper Protection is on.	MEDIUM
Needs attention	Credential theft protection (LSA) LSA protection is not enabled. How to fix: Windows Security > Device security > Core isolation > turn on "Local Security Authority protection", then restart.	MEDIUM
Needs attention	Remote-access tools review Installed: AnyDesk How to fix: Confirm every remote-access app listed is known and approved. Uninstall any nobody recognizes and change passwords used on this PC.	MEDIUM

Updates & system

STATUS	CHECK	RISK
Needs attention	Windows version is still supported Microsoft Windows 11 Pro build 22631 is an older Windows 11 version that may no longer receive updates. How to fix: Settings > Windows Update > install the latest Windows 11 feature update.	CRITICAL
Needs attention	Security updates installed recently Last update installed Aug 29, 2026 (48 days ago). How to fix: Settings > Windows Update > Check for updates, install everything, and restart.	HIGH
Pass	Secure Boot is on Secure Boot is enabled.	MEDIUM
Needs attention	No restart waiting to finish updates A restart is pending to finish installing updates. How to fix: Restart the computer.	LOW

Data & network

STATUS	CHECK	RISK
Action required	Hard drive is encrypted (BitLocker) C: is NOT encrypted. How to fix: Turn on BitLocker (Settings > Privacy & security > Device encryption, or Control Panel > BitLocker) and save the recovery key somewhere safe OFF the computer.	HIGH
Action required	Firewall is on for every network type Firewall is OFF for: Public How to fix: Windows Security > Firewall & network protection > turn on the firewall for Domain, Private and Public networks.	HIGH
Pass	Old file-sharing protocol (SMBv1) is off SMBv1 is disabled.	HIGH
Needs attention	Remote Desktop is secured Remote Desktop is ON (with Network Level Authentication). How to fix: If not needed, turn it off (Settings > System > Remote Desktop). If needed, make sure port 3389 is NOT open on the router - use a VPN instead.	HIGH
Pass	No risky services listening on the network None of the commonly abused services are listening.	MEDIUM

STATUS	CHECK	RISK
Needs attention	USB AutoRun is disabled AutoPlay is enabled for removable media. How to fix: Settings > Bluetooth & devices > AutoPlay > turn off "Use AutoPlay for all media and devices".	LOW

Accounts & passwords

STATUS	CHECK	RISK
Pass	Guest account is disabled Guest account is disabled.	HIGH
Needs attention	Everyday account is not an administrator The current user (FRONTDESK-01\reception) is an administrator. Admins: FRONTDESK-01\itadmin, FRONTDESK-01\reception How to fix: Create a separate admin account for installs, and change the everyday account to a Standard user (Settings > Accounts > Other users).	HIGH
Pass	User Account Control (UAC) is on UAC is on.	HIGH
Pass	Built-in Administrator account is disabled Built-in Administrator account is disabled.	MEDIUM
Action required	Password minimum length No minimum password length is set (blank passwords allowed). How to fix: Set a minimum of 12 characters: run as admin net accounts /minpwlen:12 (or via Group Policy / Intune for business accounts).	MEDIUM
Needs attention	Account lockout after failed logins Accounts never lock out after failed passwords. How to fix: Run as admin: net accounts /lockoutthreshold:10 /lockoutduration:15 /lockoutwindow:15	MEDIUM
Needs attention	Screen locks automatically when idle No automatic idle lock of 15 minutes or less was found. How to fix: Settings > Accounts > Sign-in options > "If you've been away, when should Windows require you to sign in again?" = When PC wakes; and set screen off after 10 minutes or less.	MEDIUM
Needs attention	No stale local accounts Enabled but unused 90+ days: frontend2 How to fix: Disable or delete local accounts that are no longer used (Computer Management > Local Users and Groups).	LOW

STATUS	CHECK	RISK
Needs attention	PowerShell activity logging Script block logging is not enabled. How to fix: Enable via Group Policy: Administrative Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block Logging.	LOW

Things to confirm together

These can't be checked automatically. Tick each one you can confirm.

- ☐ Important files are backed up automatically to at least one place OFF this computer (cloud or external drive).
- ☐ A backup has actually been restored as a test in the last 6 months.
- ☐ Email, banking and payroll accounts all use multi-factor authentication.
- ☐ Staff use a password manager instead of reusing passwords.
- ☐ Office Wi-Fi uses WPA2/WPA3 with a strong password, and visitors use a separate guest network.
- ☐ The router admin password was changed from the default and its firmware is up to date.
- ☐ Accounts of former employees were disabled on their last day.
- ☐ Staff know how to spot phishing emails and who to call if they click something suspicious.
- ☐ There is a written plan for what to do if ransomware hits (who to call, where backups are).

Next steps

Araza Tech Security can fix the items above and keep this computer monitored and updated every month. Contact: hello@arazatech.com | (281) 826-1372 | arazatech.com

This report reflects settings found on October 16, 2026 on one computer and is not a guarantee against all threats. The assessment was read-only: no settings were changed. Security Checkup v1.0.0.