UniFi Home Network Review

Summary of findings

Critical	High	Medium	Low	Info
2	2	4	3	1

1. Summary

Your hardware is in great shape — a current-generation UDM-Pro gateway, two PoE switches, five WiFi 6 access points, and eight cameras, all online and on current firmware. The findings below are not about broken gear; they describe how the network is configured to handle remote access, Wi-Fi security, and how devices are grouped together.

Two items deserve prompt attention. First, there are three openings on the public internet pointed at your Crestron control system. Crestron — the manufacturer — now tells installers to switch to a cloud relay for the homeowner's phone app and a private VPN tunnel for setup tools, and to remove those openings afterward. Second, the console is owned by your AV integrator rather than by you, so control of your network sits outside the household. Nothing here indicates an active incident, and there was no sign of unauthorized devices in the data reviewed.

Everything in this report is something you, your IT person, or your integrator can review and apply on your own schedule. Only settings were read — nothing was changed.

2. Scope of review

A remote, read-only configuration review of the UniFi console across Wi-Fi, networks and VLANs, WAN, firewall and policy, port-forwarding, VPN, CyberSecure, admin/identity, and the full device and client inventory.

No configuration was changed, no passwords were requested, and no active scanning or penetration testing was performed. A few things can’t be confirmed from a read-only review and are flagged as questions rather than findings: the gateway’s configuration-backup cadence and remote-restore readiness, and whether any current integrator tool still depends on the existing port-forwards.

3. How the system is arranged

Item	Detail
Site	Manhattan-area private residence (fictional)
Gateway	UniFi Dream Machine Pro (UDM-Pro) · UniFi OS 4.x · Network app 9.x
Switches	USW Pro 24 PoE (Layer 3) · USW 16 PoE (Layer 2, uplinked off Pro)
Access points	5 total — U6-Pro ×3 (living, master, dining) · U6-LR ×2 (rack, study) — all WiFi 6
Cameras	UniFi Protect — 8 cameras (G4 Pro ×2, G4 Bullet ×4, G4 Doorbell ×2) on a CK-G2-Plus NVR
AV / automation	Crestron Home processor (CP4-R) at 192.168.88.20 · Lutron HomeWorks processor at 192.168.88.30 · 2N IP Verso intercom · Sonos zones
ISP / WAN	Verizon FiOS Gigabit, single uplink · dynamic public IPv4 · no IPv6
LAN	Single network “Default” — 192.168.88.0/24, DHCP 100–250, ~55 leases in use
Wi-Fi SSIDs	5 total — House, House-Guest, House-IoT, House-AV, House-Service — all bound to Native Network, all WPA2
Clients	62 total (54 online, 8 offline) — 38 wired, 24 wireless
Admin accounts	5 total — 2 homeowner (Super Admin) · 3 AV integrator (1 Owner + 2 Custom)
Remote access	3 port-forward rules to 192.168.88.20 (Crestron) on external 8443 to 443, 50001 to 50001, 41796 to 41796 · From: Any · no VPN configured

4. Findings

Each finding records what was observed, why it matters, the recommended action, and who is in a position to carry it out. Severity reflects the consequence of leaving the item as it is, not the effort required to correct it.

Critical F-01

Your Crestron automation system has three doors open to the internet

OBSERVATION

Your Crestron control system can be reached directly from the public internet through three separate openings — from anywhere in the world.

Evidence · Settings > Port Forwarding

CHome-HTTPS	8443 to 192.168.88.20 : 443	From:	Any
CHome-App	50001 to 192.168.88.20 : 50001	From:	Any
CHome-CIP	41796 to 192.168.88.20 : 41796	From:	Any

WHY IT MATTERS

The manufacturer no longer recommends this. Crestron’s own current guidance is a secure cloud relay for your phone app and a private tunnel (a VPN) for your installer’s setup tools — and to remove these openings afterward.

RECOMMENDATION

Closing all three changes nothing about how you use the house day to day. The conversation to have with your integrator is collaborative: bring the system in line with Crestron’s current guidance and retire the inbound openings.

High F-02

There’s no private tunnel (VPN) for remote access yet

OBSERVATION

There’s no private, encrypted tunnel — a VPN — into your home network. A VPN is the modern, safe way for your installer to reach equipment remotely without leaving anything open to the public internet.

WHY IT MATTERS

Because there’s no tunnel, every remote-access need has turned into another open door on the internet — which is exactly what created the Crestron exposure above.

RECOMMENDATION

Stand up a VPN so remote access runs through one private tunnel, then retire the open doors it replaces.

High F-03

One camera still uses its factory password

OBSERVATION

One of your cameras — the driveway-facing bullet camera — is still using the password it shipped with from the factory. The other seven cameras have unique, managed passwords.

WHY IT MATTERS

Factory passwords are public knowledge and are the first thing automated attacks try.

RECOMMENDATION

Rotate it — a two-minute fix — so the camera stops using its factory default.

Medium F-04

Your Wi-Fi uses older encryption than your equipment supports

OBSERVATION

All five of your Wi-Fi networks use the older WPA2 encryption mode. The newer WPA3 is supported by virtually all current phones, laptops, and tablets — and by every access point you already own.

Evidence · Settings > WiFi

House	Security: WPA2	PMF: Disabled
House-Guest	Security: WPA2	PMF: Disabled
House-IoT	Security: WPA2	PMF: Disabled
House-AV	Security: WPA2	PMF: Disabled
House-Service	Security: WPA2	PMF: Disabled

WHY IT MATTERS

WPA2 without the newer protections leaves the door open to a nuisance attack that can knock devices off the Wi-Fi.

RECOMMENDATION

A mixed WPA2/WPA3 mode lets older devices keep working while newer ones get the stronger encryption; turning on “Protected Management Frames” blocks that nuisance attack.

Medium F-05

Everything is on one big network

OBSERVATION

Right now your phones, computers, IP intercoms, Crestron and Lutron processors, cameras, Sonos, and printer all share one network — the same digital street.

Evidence · Clients — all on one network

Personal (laptops, phones)	Default	192.168.88.0/24
Crestron CP4-R	Default	192.168.88.20
Lutron HomeWorks	Default	192.168.88.30
G4 cameras · 2N intercom	Default	192.168.88.0/24

WHY IT MATTERS

If any single device is taken over — say, an older smart-home gadget — it can reach everything else directly.

RECOMMENDATION

Give each type of device its own lane (a VLAN), with rules that stop the smart-home and camera lanes from reaching your personal devices.

Critical F-06

Your installer owns the console, and one login is shared

OBSERVATION

Five people can log in to manage this network. The top-level “Owner” account belongs to your AV integrator, and one integrator login looks like a shared account used by several technicians.

Evidence · Settings > Admins

Homeowner ×2	Super Admin	named
Integrator ×2	Custom	named
service@<integrator>.example	Owner	shared?

WHY IT MATTERS

The Owner is the only account that cannot be removed by anyone else, and the only one able to transfer the console. While the integrator holds it, the integrator can remove your access and you cannot remove theirs, and changing installers depends on their cooperation. A shared login also makes it impossible to tell who did what, and harder to remove access cleanly when staff change.

RECOMMENDATION

Have the integrator transfer ownership of the console to your own account, keep the integrator as a named administrator with a limited role, and replace the shared login with per-person technician accounts.

Medium F-07

A feature that lets devices open their own internet doors is switched on

OBSERVATION

A convenience feature called UPnP is turned on. It lets devices inside your home open their own openings to the internet automatically, without anyone reviewing them.

WHY IT MATTERS

On a network that already has openings pointed at the Crestron system, this quietly widens the surface in ways you can’t easily see.

RECOMMENDATION

Turning it off is the safer default; anything that genuinely needs an opening can be set up deliberately.

Medium F-08

The open doors allow more traffic types than they need

OBSERVATION

The three openings pointed at the Crestron system currently allow two kinds of network traffic (TCP and UDP) when only one — TCP — is actually needed.

WHY IT MATTERS

The extra traffic type is exposed surface with no benefit to how anything works.

RECOMMENDATION

Narrowing them to the one needed traffic type shrinks the exposed surface with zero effect on day-to-day use.

Low F-09

Your Wi-Fi names look separated but aren’t

OBSERVATION

You have five Wi-Fi names (House, Guest, IoT, AV, Service) that suggest separation — but underneath they all connect to the same single network.

WHY IT MATTERS

The separation is in name only, so a device on one name has the same reach as a device on any other.

RECOMMENDATION

This is a natural starting point for the network-lanes work above: keep the names, give each its own real lane, and rotate the Service network passphrase after each major integrator visit.

Low F-10

Your internet name-lookups use the provider’s defaults

OBSERVATION

The system that translates website names into addresses is using your internet provider’s default servers, unencrypted.

WHY IT MATTERS

Provider DNS typically offers fewer privacy and security-filtering options than a dedicated encrypted resolver.

RECOMMENDATION

Switching to a privacy-focused encrypted provider (like Cloudflare or Quad9) is a small quality-of-life and privacy improvement.

Low F-11

There’s no stable name for your changing home internet address

OBSERVATION

Your home’s public internet address can change without notice.

WHY IT MATTERS

Remote-access tools that rely on a fixed address can break silently when it changes.

RECOMMENDATION

Setting up a stable nickname for it (Dynamic DNS) means remote-access tools keep working even when the address changes — useful once the VPN is in place.

Info F-12

Some Apple devices show up as “new” repeatedly — this is normal

OBSERVATION

A few Apple devices in your client list show up under changing hardware IDs, which can look like “new devices” appearing over and over.

WHY IT MATTERS

This is completely normal — it’s Apple’s Private Wi-Fi feature working as designed. Nothing here is a security problem.

RECOMMENDATION

No action is needed. If the repeated “new device” entries bother you, the setting can be turned off per-network on each Apple device.

5. Working well

- **Firmware is current.** The UDM-Pro, the Network application, the Protect application, and all 16 infrastructure devices are on the Official channel with auto-update on.
- **WAN health is excellent.** The Verizon FiOS Gigabit uplink shows low-double-digit-millisecond latency to the first ISP hop and no observed loss in the visible window.
- **Intrusion Prevention is active.** CyberSecure IPS runs in Notify-and-Block mode with all categories selected; signatures are current.
- **Region Blocking is doing measurable work.** Inbound flows from blocked regions are dropped at the gateway and surface in the logs.
- **WAN mode is appropriate.** The single WAN is set to Failover-Only — correct for a single-ISP deployment.
- **Rogue DHCP detection is on.** The gateway will alert if another device on the LAN starts handing out leases.
- **Spanning Tree is configured correctly.** RSTP is enabled on the switches, preventing loops if a cable is miswired.
- **Wi-Fi 6 hardware is current.** Every access point supports WPA3 and PMF natively — which is why the Wi-Fi upgrade (F-04) is a software-only change, not a hardware refresh.
- **Protect runs on a dedicated NVR.** The camera workload sits on a CK-G2-Plus and is not competing with the gateway for compute or storage.

6. Priority actions

In recommended order.

#	Action	Severity	Responsible	Effort
1	Follow Crestron's current guidance and retire the three open port-forwards. Phase 1: tighten From to the integrator's public IP range and Protocol to TCP. Phase 2: cloud relay for the homeowner app + VPN for installer setup, then remove the port-forwards.	Critical		P1 Low · Low- / P2 Medium · Low
2	Stand up a UniFi WireGuard VPN on the UDM-Pro — the required precursor for Phase 2 of item 1.	High		Medium · Low
3	Rotate the password on the G4 Bullet flagged "Default Password In Use."	High		Low · Low
4	Move Wi-Fi to WPA2/WPA3 transition mode with PMF = Optional; verify on the IoT SSID first.	Medium		Low · Low
5	Introduce VLAN segmentation — promote the soft-segregation SSIDs into real VLANs (Trusted / Automation / IoT / Camera).	Medium		High · Medium
6	Have the integrator transfer console Ownership to a homeowner account, keep it as a named administrator with a limited role, and replace the shared service account with per-individual technician accounts.	Critical		Low · Low
7	Disable UPnP on the WAN interface.	Medium		Low · Low
8	Tighten port-forward protocol from TCP/UDP to TCP on any rules that remain during Phase 1 of item 1.	Medium		Low · Low
9	After VLANs are in place (item 5), rotate the Service SSID passphrase and adopt a cadence for rotating it after each major service visit.	Low		Low · Low

7. Optional next steps

- Firmware and applications are current and on the Official channel with auto-update on — keep it that way; optionally schedule the auto-updates for low-impact hours so a reboot never lands mid-day.
- Schedule a gateway configuration-backup cadence (UniFi Site Manager > Backups) so any configuration drift after these changes is recoverable.
- Consider a UPS on the rack housing the UDM-Pro, switches, and NVR — a graceful shutdown during a power blip protects SSDs and avoids the Protect database recovery cycle.
- If the Lutron HomeWorks processor moves onto a dedicated Automation VLAN as part of F-05, verify the Lutron app still reaches it via the Smart Bridge cloud relay (no inbound port-forwarding required by design).
- When AP hardware is next refreshed, plan for WiFi 6E / WiFi 7 access points and tighten WPA3 + PMF further on the modern radios.

8. References

1. Crestron Home Documentation — Remote System Access. Documents the current cloud-relay model for the homeowner mobile app, VPN guidance for system configuration, and the explicit recommendation to remove port mapping from the router after secure remote access is set up. (https://docs.crestron.com/en-us/8525/Content/CP4R/Appendix/Enable-Remote-System-Access.htm)
2. Crestron Home Documentation — Ports Used by Crestron Home. Documents the protocol scope of each port — TLS over TCP for 443, 41796 (Secure CIP), 50001 (Crestron Home App), and others. (https://docs.crestron.com/en-us/8525/Content/Ports.htm)
3. Lutron Support — Caséta / Smart Bridge connection FAQ. Documents that the Lutron app connects to the Smart Bridge via the cloud, and the Smart Bridge makes outbound connections only — no inbound port-forwarding is required. (https://support.lutron.com/us/en/product/casetawireless/faqs/bridge-connection/how-does-the-lutron-app-connect-to-the-smar
4. Control4 — 4Sight Services. Documents 4Sight as a cloud-based subscription enabling remote access, with the note that 4Sight is available for systems installed before April 23, 2024; for systems installed after that date, Control4 Connect is the replacement service. (https://docs.control4.com/o/4sight-services)
5. Savant Support — Savant Pro knowledge base. Documents Savant Home Manager as a cloud application providing system access, monitoring, and dealer remote-management features. (https://support.savant.com/pro)
6. IEEE Registration Authority. The 802 standards family defines the 48-bit MAC address format, including the Individual/Group (I/G) and Universal/Locally-administered (U/L) flag bits in the first octet. The U/L bit is bit 1 (second-least-significant) of that octet. (https://standards.ieee.org/products-programs/regauth/)
7. IETF RFC 7858 — Specification for DNS over Transport Layer Security (TLS). The standards-track specification for encrypted DNS that gateways (including UniFi) reference when offering an Encrypted DNS option. (https://datatracker.ietf.org/doc/html/rfc7858)
8. IETF RFC 2132 — DHCP Options and BOOTP Vendor Extensions. Defines option 55 (Parameter Request List), option 60 (Vendor Class Identifier), and option 12 (Host Name). These option fields are what network controllers use to fingerprint a client's vendor and model independent of its MAC address. (https://datatracker.ietf.org/doc/html/rfc2132)
9. Apple Support — Use private Wi-Fi addresses on iPhone, iPad, Apple Watch, and Vision Pro. Documents the Private Wi-Fi Address feature, the OS versions on which it ships, and the per-network toggle that turns it off where stable identification is required. (https://support.apple.com/en-us/102509)
10. IEEE 802.11 — Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Protected Management Frames (management-frame protection) were introduced in the 802.11w-2009 amendment and folded into the base standard; they defend the management frames that WPA2-only networks leave unprotected, blocking the deauthentication and beacon-spoofing attacks that can knock clients offline. The Wi-Fi Alliance requires PMF on all newly certified devices. (https://standards.ieee.org/ieee/802.11/7028/)