1. Client Profile

- **Client name:** Jane Doe.
- **Intake date:** 3rd July 2025
- **Profession:** CEO of a boutique cybersecurity firm.
- **Desired Outcome:** Secure Jane Does' Personal & Family's Digital Environment.
- **Conducted by:** Emmanuel Kilimo (Cyber Consultant).
- **Key Concern.** Proactive Hardening**.** The Client wants to ensure her home environment is a fortress against threats targeting security professionals and her family.

2. Urgency

- **Urgency Level:** Medium. There is no active crisis. The goal is proactive hardening, to "practice what she preaches" and ensure her home environment is a fortress against threats targeting security professionals and their family.

3. Goals for Engagement

- Establish simple and practical cybersecurity habits that she and her family can follow.

4. Technical Skill Level

- **Expert:** However, the client is time-poor and wants a seamless, "white-glove" experience that provides robust security for her family without requiring her constant technical intervention.

- **Implication on Solutions:** Solutions and instructions must be highly secure and easy to follow.

5. Consent Acknowledgement

- By engaging the cyber consultant, the client acknowledges and provides consent for the assessment of her digital environment. This includes devices, networks, and relevant online accounts, for the sole purpose of identifying vulnerabilities, analyzing and monitoring threats, analyzing and mitigating risks and implementing related cybersecurity solutions. All information shared will be treated with the utmost confidentiality.

Jane's Digital Asset Inventory

Category	Asset	Purpose	Storage	Notes
Computers & Laptops	"Jane's MacBook Air "	Primary work/personal device	SSD	Will be hardened and configured to be on the 'Work Zone'
	BSCs-Mac-mini" (Apple Mac mini)	Home Use	""	Will be hardened and configured to be on the 'Home Network Zone'
	"Bailey's Gamer" (Custom-built Windows Desktop)	Gaming/Homework	CPU	Accounts logged in to be cross checked. Requires active and ongoing hardening efforts by the user as they are not inherently "hardened" out of the box in the same way a dedicated security appliance would be.
	Eevee" (Intel-based computer)		""	Will be hardened.
Mobile Devices (Phones & Tablets)	Multiple iPhones	Everyday communication and browsing	iOS	Will be hardened and isolated to a separate network.
	Samsung Phone	Used by Visiting Aunt	Android OS	""

	"Deena iPad 10"	Everyday browsing	iPadOS	“”
	Additional Ipad	“”	“”	“”
Network Infrastructure	ISP: Comcast Xfinity (1 Gbps plan)	Internet services		Will be scanned for vulnerabilities and hardened.
	Router: Eero Pro 6 (Mesh network with multiple "eero" nodes)	Offers better internet coverage		Will be used in ‘bridge mode’. Considering the many no. of devices, it will provide better internet coverage.
Entertainment & Gaming	2x Microsoft XBOX consoles	gaming		Need strong passwords and regular updates as hardening is mostly done by manufacturer.
	2x Oculus VR headsets	“”		
	LG webOS TV (OLED65C2PUA)	“”		
	2x Samsung Smart TVs	“”		
	Samsung "The Premiere" LSP7 Projector	“”		

	Sonos speakers			
	Facebook Portal Device	Facebook services		Need to be decommissioned. As of today, Facebook portal devices are no longer being sold.
Smart Home & IoT Devices	Multiple Amazon Blink security cameras	security		A number of recommended cyber security practices like strong password, multifactor authentication for device security, encryption and authentication protocols for secure comms to be implemented then ongoing monitoring to follow.
	Nest Thermostat	comfort		
	Philips Hue smart lighting system	“”		
	Samsung Smart Refrigerator			
	Samsung Smart Range (Oven)			
Data Storage & Peripherals	Local	Data backup and recovery		An effective back up strategy to be identified, and data backed up according to their types and sensitivity.
	Cloud	“”		
	Printer	For work documents		

Personalized Threat Model – CEO

The client is the CEO of a cyber security firm. Security stakes are uniquely high. She regularly handles sensitive business intelligence, proprietary data and advanced threat intelligence. This makes her a high value target for state sponsored actors, corporate espionage and sophisticated cybercriminals.

Her family's digital footprint and key assets include:

- **Computers & Laptops** - personal and work use. Will be hardened.
- **Mobile Devices –** personal. Will be hardened.
- **Network Infrastructure –** Will be scanned for vulnerabilities with dedicated router vulnerability checkers, complemented by vulnerability scanners like OpenVAS and also network scanners like Nmap and hardened afterwards.
- **Gaming –** accounts logged in will be cross-checked for excessive privileges.
- **Smart Home & IOT Devices –** need strong device security, regular patching, and also on placed on a separate network, and monitored for anomalies and suspicious activity.
- **Data Storage & Peripherals-** purpose of accounts and type of data to be established and also linkages to other family members or third parties.

Personalized Threat Profile

The attack tree below helps you systematically assess potential threats, even when there is no active crisis, useful during proactive hardening efforts.

Root Goal: Compromise Jane or family to gain access or create leverage point

[1] First Level Branch: Compromise Jane's Primary Device ("MacBook Air")

- Phishing via personal or work email.
- Zero-day exploit on macOS or third-party software.

[2] Second Level Branch: Exploit Home Network (Eero Pro 6)

- Weak admin credentials on Eero or no MFA.
- Misconfiguration allows internal device discovery.
- VLAN/SSID isolation between IoT, gaming, and work devices.

[3] Third Level Branch: Target Kids' Devices (iPhones, iPads, "Bailey's Gamer")

- Social engineering through online gaming chat.
- Malware via games.

[4] Fourth Level Branch: Exploit Visiting Aunt's Samsung Phone

- Outdated Android OS vulnerable to drive-by download.

[5] Fifth Level Branch: Abuse IoT & Smart Home Devices

- Misuse of microphone-enabled devices (always-on listening).
- TV or fridge data leaks location or account info.

[6] Sixth Level: Attack via Cloud Accounts (iCloud, Dropbox, Google Drive)

- Phishing or credential stuffing.
- Password reuse across family increasing exposure.

[7] Eighth Level: Public Data Exposure & Social Engineering

- Use of social media to map family, school, device usage.

Personalized Cyber Security Plan

This plan outlines specific, actionable steps, tools, and configurations designed to significantly enhance your digital security posture. Leveraging insights from your digital asset inventory, it develops a tailored threat profile. The overarching goal is to provide robust, layered protection for your home network and digital environment. Below are the core recommendations.

Network Segmentation

Network Segmentation is an excellent strategy for proactive hardening. It does this by reducing attack surface, limiting lateral movement, enhanced security controls, improved threat containment. Network Segmentation also signifies compliance with existing regulatory frameworks. This approach employs "Principle of Least Privilege" at a network level, limiting what devices can communicate with each other, thus containing potential breaches.

In network segmentation, we "divide" your home network into smaller isolated sections called "zones". Each zone is like a separate room. We put specific types of devices into each room based on trust and the data/information sensitivity they contain.

This “room” concept is so important for your home security as each zone is configured so that devices within it only have access to what they need to function (need to know access), different security rules and protection levels to each zone, limiting the “blast radius” in case of breach, and traffic monitoring between and within each zone.

In essence, network segmentation is about creating a highly organized, compartmentalized digital environment for your home.

Given the sheer volume of your devices, their diverse operational usages, and the need for granular technical analysis, your network will require four distinct networks zones. These are the Home Network zone, Work zone, IOT zone and the Guest zone. To achieve this level of segmentation, you will need the following equipment:

- **Firewall with VLAN support:** this is the absolute core of segmentation. Your Eero Pro 6 supports a basic “Guest Network” but because of the need for additional network zones, a more advanced firewall appliance is necessary. Also, creating multiple SSIDs each mapped to a separate VLAN directly within the Eero app for fine grained firewall is generally a not a native feature for its standard operating mode. The Firewalla Gold SE provides an excellent choice.
- **Switches (for wired devices):** a managed switch will allow you to assign specific physical ports to specific VLANS. Given the wired devices you have like the desktop PC’s, Xbox consoles, smart TVs, Printer, Philips hue smart lighting system, a switch is necessary.

Firewall Recommendation & Setup Plan

The cyber consultant recommends the Firewalla Gold SE as an advanced firewall option. This is the safest and most secure device required. Below is the setup considerations and justifications as well as its capabilities for network segmentation.

Firewalla Gold SE

A high-performance smart firewall device designed for home and small office networks.
The Gold SE has the following specifications:

Advanced Stateful Firewall and Deep Packet Inspection (DPI).

- Built-in Intrusion Detection and Prevention System (IDS/IPS) using open-source Snort.
- Geo-IP filtering, Ad blocking, and DNS over HTTP/TLS support.

Performance

- Quad-core CPU with 4 GB RAM.
- 3 Gbps routing/firewall throughput.
- Ideal for gigabit (compatible with your ISP) internet connections with overhead for VPN or filtering.

Multi-Gigabit Support & Port Flexibility

- 4 * 2.5 Gbps ethernet ports, supporting high speed LAN/WAN.

Network Segmentation Support

- VLAN and virtual network capabilities.
- Allows isolation of IoT devices, guest networks and critical systems.

Private VPN Capability

Benefit: Secure Access: Encrypted tunnel to home network when traveling.

End to End Encryption: Prevents ISP or hotspot snooping; protects DNS queries with DoH inside VPN.

Geo-Fence Bypass / Fair-Use Streaming: Temporary access to home-region services when abroad.

Site-to-Site Option: Seamless connection to a relative's or second property's Firewalla for shared resources without exposing ports.

Conclusion:

The Firewalla Gold SE offers enterprise-grade functionality with a consumer-friendly experience, making it an ideal choice for Jane's secure home setup. Its flexibility, performance, and security focus justify the moderate upfront cost, and it enables advanced protection such as segmentation, intrusion detection, and secure remote management.

End Point Security Recommendations

Core Principles for ALL Endpoints

1. **Strict Password Policies & Multi-Factor Authentication (MFA/2FA)**

   Mandatory Strong, Unique Passwords: Every single account (OS login, email, online services, gaming platforms, smart home apps) must have a long, complex, and unique password. A high-quality family plan password manager is non-negotiable for generating and storing these.
   MFA Everywhere Possible: Enable MFA on every service that offers it.

2. **Aggressive Patch Management**

   Automate Updates: Enable automatic updates for all operating systems (Windows, macOS, iOS, Android), web browsers, and core applications.

   Prompt Manual Updates: For software without automatic updates, create a strict schedule to manually check for and apply patches immediately.

   Firmware Updates: Don't forget firmware for your router's smart devices and even PC components (e.g., SSDs, graphics cards).

3. **Principle of Least Privilege (User Accounts):**

   Standard User Accounts: Operate all personal computers (laptops, desktops) using a standard user account for daily tasks and browse. Only switch to an administrator account when absolutely necessary for system changes or software installations. This limits the impact of malware.

4. **Data Encryption:**

   Full Disk Encryption (FDE): Ensure all laptops and desktops have FDE enabled (BitLocker for Windows, File Vault for macOS). This protects data if the device is lost or stolen.

Mobile Device Encryption: Modern smartphones (iOS, Android) typically have FDE enabled by default. Verify this.

Cloud Encryption: Use cloud storage providers that offer robust encryption both in transit and at rest, and consider client-side encryption for highly sensitive files before uploading them.

5. **Robust Backup and Recovery:**

3-2-1 Rule: Maintain at least three copies of important data, on two different types of media, with one copy stored off-site (e.g., encrypted cloud backup, external hard drive stored securely elsewhere).

Regularity: Automate backups or schedule them frequently.

Test Restores: Periodically test your backup recovery process to ensure data integrity and your ability to restore.

6. **Secure Browse Habits**

Ad Blockers/Privacy Extensions: Use reputable browser extensions to block ads and trackers.

Phishing Awareness: Constant vigilance against phishing. Never click suspicious links, download unsolicited attachments, or provide your credentials. Verify requests through a separate, trusted channel.

Limit Information Sharing: Be mindful of what personal information is shared on social media or public forums.

Zone-Specific Endpoint Security Recommendations

Work Zone (Highest Security Priority)

These are your most critical assets.

- **Endpoint Detection and Response (EDR):**
    - An enterprise-grade EDR solution will be implemented (e.g., Microsoft Defender for Endpoint) on your work laptop and desktop. These solutions use AI/ML to detect advanced threats, and enable rapid response. For you as a CEO, this is a non-negotiable investment.

- **Application Whitelisting/Control:**
    - Strictly limit what applications can run on work devices. Only approved and necessary software should be allowed. This can be complex but highly effective.

- **Data Loss Prevention (DLP):**
    - Implement DLP solutions or practices to prevent sensitive corporate data from leaving the Work Zone devices without authorization (e.g., uploaded to unauthorized cloud storage, or emailed outside company policy).
- **VPN Always-On:**
    - Use a high-quality, always-on VPN for all internet traffic from work devices, preferably one provided and managed by your enterprise for accessing corporate resources securely. If using a personal VPN, choose a reputable, no-logs provider.
- **Secure Browsers for Work:**
    - Dedicate a specific, hardened browser (e.g., a separate Chrome profile with minimal extensions) solely for work-related browse.

Home Network Zone

These are trusted personal devices, but still need strong protection.

- **Reputable Endpoint Protection Platform (EPP):**
    - Install a high-quality antivirus/anti-malware suite on all personal laptops and desktops. Ensure its kept updated and perform regular scans.

- **Built-in OS Security:**
    - Utilize features like Windows Defender Firewall, macOS Gatekeeper, and built-in privacy controls.
- **Parental Control Software (on Family Devices):**
    - Implement endpoint-based parental control software (e.g., Family Link for Android, Screen Time for iOS, or third-party solutions) to manage app usage, content filtering, and screen time on children's devices.
- **Browser Security:**
    - Use privacy-focused browser extensions and ensure safe browse settings are enabled.
- **Regular Software Audits:**
    - Periodically review installed software and apps on all family devices.
- **Physical Device Security:**

    - Ensure all devices have strong screen lock passcodes/biometrics enabled. Educate the kids on not leaving devices unattended.

Data Back Up Plan (Local & Cloud)

A robust back up plan is the ultimate failsafe against everything from accidental deletion and hardware failure to sophisticated ransomware attacks. The gold standard in backup strategy is the **3-2-1 Rule**. We'll apply it with an emphasis on security and recovery speed.

The 3-2-1 Rule for Jane:

- **3 Copies of Your Data:** This includes the original data on your device and at least two separate backup copies.
- **2 Different Types of Media:** Store these copies on different storage technologies to guard against a single point of failure (e.g., external hard drive and cloud storage).
- **1 Copy Offsite:** At least one copy must be stored in a geographically separate location.

Client’s Different Data Types

Work Zone Data: Absolutely paramount. This includes confidential company documents, intellectual property and financial records. This data requires the highest frequency and most secure backup methods.

Home Devices Data: Family photos, videos, personal documents, financial records, important emails. These are irreplaceable and highly sensitive.

IoT Zone Data: Configuration backups for smart home hubs (like the Hue Bridge), camera footage (if stored locally). While less "critical" in terms of personal loss, their configurations can be time-consuming to recreate.

Backup Types & Frequency (Recovery Point Objective - RPO):

- **Full Backups:** A complete copy of all selected data. These are the most straightforward for recovery but consume the most space and time.
- **Incremental Backups:** Backs up only the data that has changed since the last backup (full or incremental). This is fast and efficient for storage. Recovery can be slower as it requires piecing together the full backup plus all subsequent incremental changes.
- **Differential Backups:** Backs up all data that has changed since the last full backup. Faster to restore than incremental, but each differential backup gets larger over time.

A hybrid approach using a combination is ideal:

- **Work Zone:**
    - **Automated, Frequent Incremental Backups (e.g., hourly/daily):** For active working files, sync to a secure cloud service that maintains version history.
- **Home Devices:**
    - **Automated Daily Incremental Backups:** For personal documents, photos, videos.
- **IoT Zone:**

- **Configuration Backups:** If devices allow (e.g., smart home hubs), backup configurations to the NAS on the Home Devices network, and then include that NAS data in its own backup routine.

3. Diverse Storage Media & Locations:

- **On-site Local Storage (for speed and convenience):**
  - **Network Attached Storage (NAS):** A dedicated device (like a Synology in the Home Devices zone, providing a central, accessible location for backups of all devices. Encrypt data on the NAS.
  - **External Hard Drives:** For individual devices, used for quick, local backups. They should be disconnected immediately after backup to prevent ransomware from encrypting them. Jane should have multiple such drives and rotate them.
- **Offsite Cloud Storage (for disaster recovery and geographic redundancy):**
  - **Reputable Cloud Backup Service:** Use a professional cloud backup service (e.g., Acronis Cyber Protect Home Office, Druva) that offers:
    - **End-to-end encryption:** Data is encrypted before leaving her device and remains encrypted at rest in the cloud.
    - **Versioning:** Ability to restore previous versions of files (crucial for ransomware recovery).
    - **Ransomware protection:** Some services specifically offer features to detect and prevent ransomware from encrypting backups.
    - **Automated scheduling and monitoring.**
  - **Consider a dedicated business-tier cloud backup** for her Work Zone data, even if it's personal equipment, for higher SLAs and features.
- **"Air-Gapped" or "Offline" Backup (The Ultimate Ransomware Defense):**
  - This is the "1" in the 3-2-1 rule. This copy is physically disconnected from the network and power when not actively backing up or restoring.

- **Method:** A dedicated external hard drive (or even multiple, rotated drives) used only for this purpose. Connect it, run the backup, and immediately disconnect it. This prevents malware (especially ransomware) that compromises her live system from ever reaching and encrypting this last-resort backup.
- **Frequency:** Less frequent, perhaps weekly or monthly for critical data that doesn't change hourly, but essential for peace of mind.

4. Security for Backups:

- **Encryption:** All backup data, whether local or cloud, must be encrypted both in transit (when being sent) and at rest (when stored).
- **Access Control:** Limit who has access to backup data and backup management systems. Use strong, unique passwords and MFA for all backup accounts.

7. Disaster Recovery Plan (DRP):

- A documented set of steps outlining how to recover from various data loss scenarios (e.g., single file deletion, hard drive crash, ransomware,). This plan should be accessible even if your primary devices are down (e.g., printed copy, stored on a secure USB drive offsite).

By combining these elements, you will have a robust, resilient backup strategy that safeguards your valuable digital assets against virtually any threat, allowing you to focus on your cybersecurity leadership role with confidence.

Password Management Strategy

Strict Password Policies & Multi-Factor Authentication (MFA/2FA)

Mandatory Strong, Unique Passwords: Every single account (OS login, email, online services, gaming platforms, smart home apps) must have a long, complex, and unique password. A high-quality password manager is non-negotiable for generating and storing these.

MFA Everywhere Possible: Enable MFA on every service that offers it. Prioritize authenticator apps (e.g., Google Authenticator). This is your strongest defense against compromised passwords.

Recommendations for Enhancing Privacy

I. **Foundational Privacy Principles (Apply to All Devices & Accounts):**

1. **Data Minimization:** Only provide the absolute minimum amount of personal data necessary for a service to function.
2. **Consent and Transparency:** Actively seek out and understand privacy policies. While often long, they reveal how data is collected, used, and shared. Be skeptical if a company is not transparent.
3. **Opt-Out Where Possible:** Aggressively opt out of data sharing, personalized advertising, and analytics collection wherever options are provided in settings.
4. **Regular Privacy Audits:** Periodically (e.g., quarterly) review privacy settings on all major accounts (Google, Apple, social media, smart home platforms) as defaults can change with updates or new features.

Security Recommendations for IOT Devices

1. IoT devices need to be configured with **strong passwords and multi factor authentication** to achieve device security.
2. As data is transmitted between these devices, **encryption and authentication** protocols are necessary to secure communication.
3. **Segmenting IoT devices** from other critical systems.
4. **Continious monitoring** of IoT devices and networks to detect anomalies and suspicious behaviour.

Network Zones

The four zones and their purpose:

1. **Home Network Zone:**

Purpose: For general personal devices used by family members.

Devices: Laptops, phones, tablets, and gaming devices.

Security Goal: provide a balance of security and goal. These devices are less critical than work devices but more secure than IOT devices.

2. **Work Zone:**

Purpose: The most secure zone. This zone will be dedicated to your work and highly sensitive data.
Devices: MacBook Air", Secure Printer
Security Goal: Create an impenetrable fortress around your professional assets, prevent lateral movement from any other zones. Protection against corporate espionage and state sponsored attacks.

3. **IoT Zone**

Purpose: For smart home devices that require internet access but are prone to vulnerabilities due to their weak security.
Devices: Multiple Amazon Blink security cameras, Nest Thermostat, Philips Hue smart lighting system, Samsung Smart Refrigerator, Samsung Smart Range (Oven).
Security Goal: Contain any breach of a potential breach of a vulnerable IoT device, preventing the spread to sensitive personal or work devices.

4. **Guest Zone**

Purpose: For visitor's devices. For example, the phone used by the visiting aunt. This zone is to be completely isolated from other internal networks. Provide internet access only.

Devices: Aunt's phone.

Security Goal: Preventing guest devices which you have no control over from becoming an entry point into your home network.

Implementing this four-zone segmentation will significantly enhance your home network security creating a robust multi-layered defense that aligns perfectly with your proactive hardening objective and your work status.

Proposed Home Network Map