CYBERSHIELD-360

PROJECT PART 1: DATA CLASSIFICATION & RISK ASSESSMENT

COMPANY: HEWLETT-PACKARD

1. COMPANY OVERVIEW

Hewlett-Packard (HP Inc. & Hewlett-Packard Enterprise)

Hewlett-Packard, commonly known as HP, was initially founded in 1939 in Palo Alto, California, and remains a global leader in technology, serving over 150 countries. In 2015, HP was split into two entities:

HP Inc.'s core business focuses on personal systems (laptops, desktops), printers, and imaging solutions. On the other hand, **Hewlett Packard Enterprise (HPE)** concentrates on enterprise-level IT infrastructure, servers, storage, networking, cloud solutions, and cybersecurity services.

SCOPE OF SECURITY ASSESSMENT:

Data Security & Privacy: Assess how sensitive customer and enterprise data is stored, protected, and transmitted.

Threat Management: Identifying vulnerabilities, patch management practices, and incident response readiness.

Compliance & Governance: Reviewing alignment with standards and industry best practices.

2. DATA TYPES AND CLASSIFICATION SCHEME

Level 1 – Public (Label: HP-Public)

Information approved for public release. No damage if disclosed.

Examples: Published marketing content, job postings, and press releases.

Level 2 – Internal (Label: HP-Internal)

Routine business information not for public distribution. Limited impact if disclosed.

Examples: Most internal emails/docs, non-sensitive process docs, internal org charts without PII.

Level 3 – Confidential (Label: HP-Confidential)

Sensitive business/technical/regulated data. Material harm, regulatory exposure, or competitive loss if disclosed.

Examples: Customer contracts, non-public financials, moderate-sensitivity PII, product roadmaps, non-public source code.

Level 4 – Restricted (Label: HP-Restricted)

Highest sensitivity. Severe business, legal, or safety impact if disclosed. Examples: Pre-IPO earnings, M&A strategy, authentication secrets/keys, security configs, high-risk PII (SSNs, government IDs, health data), PCI card data, highly sensitive source code/algorithms, embargoed strategic plans**.**

DATA CLASSIFICATION WORKFLOW

Create/Tag → Assign label to data - document/email and repository metadata.

Protect → Apply encryption - limit access if needed.

Review → Access and review data annually or quarterly.

Declassify/Archive → Dispose or downgrade content once obsolete or public.

Data Type	Recommended Default	Notes
Internal documents & emails	**Internal** → elevate to **Confidential** when they include sensitive metrics, security details, or roadmaps; **Restricted** if market-moving or containing secrets/keys.	Use email tags; IRM for Confidential/Restricted; avoid attachments for Restricted.
Customer & employee data	**Confidential** for standard PII; **Restricted** for high-risk PII (IDs, financials, health, biometrics).	Apply GDPR principles and NIST PII protections; use DPAs with vendors. GDPR NIST CSRC
Financial records & source code	**Financials**: Confidential; **embargoed/SOX/earnings** → Restricted. **PCI CHD** → **Restricted-PCI** only in segmented, logged environments. **Source code**: Confidential; **security-critical/keys** → Restricted.	Follow PCI DSS and strong key management/masking practices. PCI Compliance Hub -
Confidential business strategy	**Confidential**; elevate to **Restricted** for M&A, pricing, or executive strategy under embargo.	Owner approval for any external sharing; watermark and limit via IRM.

Control Area	Level 1 Public	Level 2 Internal	Level 3 Confidential	Level 4 Restricted
Where to store	Public web, approved repos	Approved internal repos	Approved encrypted repos with access groups	Segmented, encrypted repos; dedicated "Restricted" spaces
Access	Anyone	HP workforce	Need-to-know; named users; MFA	Strict need-to-know; exec/owner approval; MFA; session recording where feasible
Email/Sharing	Unrestricted	Internal only; external by Owner	External with NDA, IRM, link-only, expiry	No attachments; secure transfer only DLP block to personal domains
Encryption (rest/transit)	Recommended	Recommended	**Required/Required**	**Required/Required** (FIPS-validated where applicable)
Third parties	N/A	Contracted vendors only	DPA + security review; monitor	Contract + audit rights; strong controls (e.g., PCI-validated if CHD)
Printing	Allowed	Caution	Secure print; locked storage	Avoid; exception-based only; secure destruction
Retention	As needed	Per schedule	Per schedule; legal hold aware	Minimum necessary; frequent review prompt secure delete
Incident response	Monitor	Monitor	Immediate escalation	Immediate escalation; exec/legal notification

2.3 COMPARISON OF RISK ASSESSMENT METHODOLOGIES

NIST SP 800-30 Rev. 1

Overview: A comprehensive guide for conducting risk assessments, emphasizing asset identification, threat analysis, and impact evaluation.

Strengths:

Highly structured and detailed.

Aligns with HP's existing Information Security Framework.

Supports quantitative and qualitative analysis.

Challenges:

Resource-intensive (requires extensive documentation and staffing).

It may be complex for rapid assessments.

OCTAVE Allegro

Overview: A streamlined risk assessment methodology focused on information assets and operational context.

Strengths:

More straightforward to implement with fewer resources.

Emphasizes organizational context and stakeholder input.

Challenges:

Less detailed in technical threat modeling.

May lack depth for large-scale enterprise environments.

2.4 RECOMMENDED METHODOLOGY

Recommendation: NIST SP 800-30 Rev. 1

Justification:

1. HP's cybersecurity framework is already aligned with NIST standards, making integration seamless.
2. The methodology's depth supports HP's complex infrastructure and global

operations.

3. It enables robust documentation and repeatable processes, essential for long-term compliance and audits.

Given HP’s size, global operations, and complex IT environment, the NIST SP 800-30 methodology is recommended. Although it requires more time, resources, and staffing, its structured and comprehensive framework ensures a thorough risk assessment. This is critical for a multinational organization like HP that manages large volumes of sensitive customer, financial, and proprietary data. The rigor of NIST provides the reliability and depth necessary to safeguard HP’s assets against evolving cyber threats.

References

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University, Software Engineering Institute.

National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). U.S. Department of Commerce.

Global Information Assurance Certification (GIAC). (n.d.). Data Classification Guide. SANS Institute.

GIAC Data Classification Guide: https://www.giac.org/paper/gsec/736/data-classification/101635

NIST SP 800-30 Rev. 1: https://csrc.nist.gov/pubs/sp/800/30/r1/final

OCTAVE Allegro: https://www.sei.cmu.edu/library/introducing-octave-allegro-improving-the-information-security-risk-assessment-process/

HP Official Site: https://www.hp.com/us-en/hp-information.html

HP Security Measures: https://www.hp.com/content/dam/sites/worldwide/privacy/pdf/security-measures/English.pdf

PROJECT PART 2: GAP ANALYSIS PLAN

COMPANY: HEWLETT-PACKARD

3.1. SECURITY OBJECTIVES

INTRODUCTION:

HP is always ensuring we have the answers to ensure maximum security. That's where a security gap analysis comes in. This is basically a health check for our information systems. The goal is to assess the company's current position, its desired future state, and the necessary steps to achieve it. HP takes it very seriously and considers it a survival strategy. The threats HP faces aren't just the usual viruses and malware, but advanced attacks that could compromise sensitive customer data, interrupt operations, or damage its reputation. By taking a closer look at HP's security posture and comparing it with that of other viable companies and recognized standards, the company can focus its resources on the areas that matter most.

GAP ANALYSIS:

HP will conduct a professional gap analysis structured around established frameworks, such as the NIST Cybersecurity Framework, the CIS Critical Security Controls, and ISO/IEC 27001. HP will also utilize tools such as vulnerability scanners, governance platforms, and monitoring systems to collect and analyze this information.

Each of these offers a blueprint and follows the processes below:

1. Take inventory of the current state - Understand what security controls are in place.
2. Benchmark against best practices - Compare those controls with standards. 3. Spot the gaps - Identify where protections are weak, inconsistent, or missing. 4. Prioritize by risk - Rank the gaps based on their level of danger and exploitation. 5. Build a roadmap - Lay out a plan to close the highest-risk gaps first.

3.2. CURRENT VS. DESIRED STATE:

HP's current security versus where we want to be:

Objective	Current State	Desired State	Gap	Risk Level
Zero Trust	Network segmented, but still relying on perimeter defenses	Company-wide Zero Trust architecture	Not fully implemented	High
Access Controls	MFA only for remote users; admin privileges not consistently managed	MFA for everyone, centralized admin control	Gaps in MFA coverage and privilege management	High
Data Protection	Some data is encrypted at rest; in-transit protection is inconsistent	End-to-end encryption, tokenization for customer data	Encryption coverage is uneven	Medium
Logging & Monitoring	SIEM is in place, but not all systems feed data into it	Full visibility across all systems	Limited visibility in some areas	Medium
Infrastructure Hardening	Regular patching, but legacy systems are still exposed	Automated patching, baseline hardening, EDR everywhere	Legacy risks remain	High

3.3. IDENTIFIED GAPS

HP has identified a few key objectives to guide its security strategy.

These are based on industry best practices but tailored to the kinds of risks HP faces:

Don't assume any user or device can be trusted - Zero Trust

Tighten access controls by expanding multi-factor authentication (MFA).

Enhance data protection via data encryption.

Strengthen monitoring by ensuring security events are captured everywhere.

Harden infrastructure by patching vulnerabilities, securing configurations, and using advanced endpoint protection.

3.4. RECOMMENDATIONS/ROADMAP

Below is our roadmap for HP to move closer to its desired security posture:

PHASE 1 (0–6 MONTHS)

Roll out MFA for all users, not just remote access.

Launch a Zero Trust pilot for the most sensitive systems.

Patch critical vulnerabilities in legacy environments.

PHASE 2 (6–12 MONTHS)

Deploy Privileged Access Management (PAM) tools.

Expand encryption to protect all in-transit data.

Standardize log collection across on-premises and cloud systems.

PHASE 3 (12–24 MONTHS)

Scale Zero Trust principles across the company.

Strengthen monitoring with AI-based anomaly detection.

Automate vulnerability scanning and patch management.

References

Shaw, R. (2012). Conducting an information security gap analysis [Report]. Faulkner Information Services.

Kim, D., & Solomon, M. G. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Ghaznavi-Zadeh, R. (2018). Information Security Architecture: Gap Assessment and Prioritization. *ISACA Journal, 2*. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/information-security-architecture-gap-assessment-and-prioritization

PROJECT PART 3: MALWARE INCIDENT ANALYSIS

COMPANY: HEWLETT-PACKARD

4.1. INCIDENT SUMMARY

On January 16, 2025, IntelBroker posted on the dark web claiming that they had gained unauthorized access to HPE's infrastructure and stolen sensitive information, including source code, private keys, repositories, Docker builds, certificates, and personal information. HPE filed a notice of data breach with the Massachusetts Attorney General, indicating that an "unauthorized party" accessed certain personal information (names, social-security numbers, driver's license numbers) given to HPE. This incident is a good example to consider for analysis.

4.2. ROOT CAUSE ANALYSIS

Because the investigation is ongoing and the hacker's claims have not been fully verified, the full scope remains uncertain. Still, from the information we have now about the data breach, we can analyze some of HPE's potential weaknesses. According to the hacker's claims, they had access to HPE systems for "about two days." It is unclear exactly how initial access was gained, whether via compromised credentials, phishing, vulnerability exploitation, or third-party compromise. Based on our research, some analysts suggest that, given the nature of IntelBroker's prior attacks, it may have involved a vulnerable or misconfigured public-facing asset.

4.3. IMPACT ASSESSMENT

What was affected/exposed:

1. Source code repositories (private GitHub) of HPE products (Zerto, iLO) and Docker builds.
2. Internal credentials, certificates (private & public keys), and internal service endpoints/configurations according to hacker-shared screenshots.
3. Legacy PII (personally identifiable information) related to past product deliveries of HPE

to users, as claimed by the hacker.

4. HPE later disclosed in a filing that some names, SSNs, and driver's license numbers had been accessed.

Vulnerabilities Exposed:

1. **Weak Controls**

   The breach implies that HPE's development and pre-production sections were accessible and potentially less tightly guarded than other areas. This could also suggest potential gaps in third-party/vendor controls.

2. **Insufficient segmentation or credential access controls**

   The ability of the attacker to access APIs, self-hosted GitHub, WePay, and internal sectors suggests insufficient credential management, overly broad access privileges, or inadequate segmentation between environments.

3. **Insufficient Detection/Monitoring**

   The fact that an attacker claims two-day access and exfiltration suggests that the access was not detected promptly or that monitoring did not flag abnormal behaviors.

Business & Operational Impact:

1. **Reputational risk**

   Exposure of source code and product keys undermines customer trust (partners, enterprise customers) and could affect sales or renewals.

2. **Intellectual property loss**

   Theft of proprietary source code could allow competitors to reverse engineer, create counterfeit products, exploit vulnerabilities, and undercut the market.

3. **Product security risk**

   A compromised internal product code could enable insertion of malicious tampering or vulnerabilities in devices sold to customers, resulting in large-scale exploitation or

product recalls.

4. **Regulatory & legal exposure**

   Access to PII (names, SSNs, driver's licenses) triggers data-privacy regulatory obligations and state data breach laws to come into effect. It could lead to lawsuits and/or fines.

5. **Customer/vendor trust erosion**

   Enterprise customers may demand more stringent audit and security assurances. A breach can raise vendor liability and contractual obligations.

6. **Future operational and remediation costs**

   On top of the loss of data and intellectual property, future operational and remediation costs will pile up.

4.5. PROPOSED COUNTERMEASURES

Recovery & Response Actions HPE should take:

1. Launch an investigation and notify all interested parties involved.
2. Conduct post-incident reports to assess all damages.
3. Strengthen segmentation and monitoring in all systems by implementing zero-trust across all environments and implementing HSMs and stricter auditing.
4. Enhance third-party controls and validation, and rotate all potentially affected credentials, certificates, and keys.
5. Implement new rules and regulations at HPE directly in response to this incident.
6. Run incident-response drills in the case of another data breach.

Implementing these measures will reduce exposure, increase detection speed, and preserve customer data and trust.

References

Kim, D., & Solomon, M. G. (2022). *Fundamentals of information systems security* (4th ed. p. 74 & 106). Jones & Bartlett Learning. ISBN 9781284238815

Gatlan, S. (2025, January 20). *HPE investigates breach as hacker claims to steal source code*. BleepingComputer. https://www.bleepingcomputer.com/news/security/hewlett-packard-enterprise-investigates-new-breach-claims/

Alspach, K. (2025, January 21). *HPE investigating breach claims involving source code: Report*. CRN. https://www.crn.com/news/security/2025/hpe-investigating-breach-claims-involving-source-code report

Console and Associates, P.C. (2025, February 7). *Hewlett-Packard Enterprise Company files notice of recent data breach*. JD Supra. https://www.jdsupra.com/legalnews/hewlett-packard-enterprise-company-3944876/

Waqas. (2025, January 19). *Hackers claim breach of Hewlett Packard Enterprise, lists data for sale*. Hackread. https://hackread.com/hackers-claim-hewlett-packard-data-breach-sale/

OpenAI. (2025, October 19). *Analysis of Hewlett-Packard cybersecurity breach and recommendations* [ChatGPT conversation]. ChatGPT (GPT-5). https://chat.openai.com/

PROJECT PART 4: THREAT MODELING

COMPANY: HEWLETT-PACKARD

5.1. System/Process Chosen

For our system analysis, we will be examining HP's Web-Based Customer Account Portal. This system allows users to log in, manage HP device warranties, view purchase history, and access support.

5.2. STRIDE Analysis

Key Components of HP's Web-Based Customer Portal:

Users / External Entities

Customer (Browser/App) – Accesses the HP account portal.
Email Service – Sends verification links and password resets.

Processes

Web Front-End Server – Handles HTTPS requests, displays pages, and validates input.
Authentication Service – Verifies credentials and issues session tokens.
Account Management Service – Manages user profiles, device info, and support data.
Database Server – Stores user credentials, personal info, and device/warranty data.

Data Stores

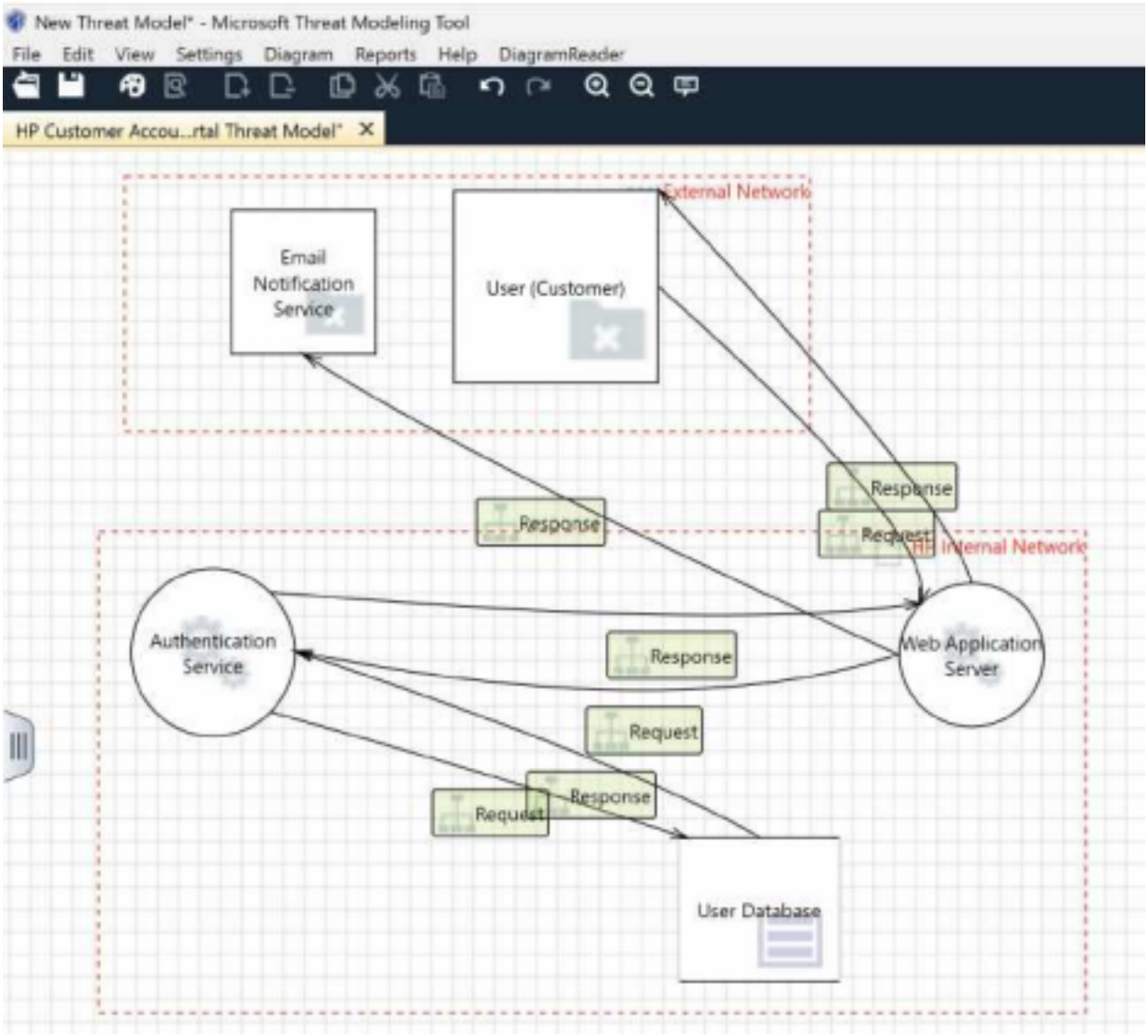
User Database – Contains user profiles, hashed passwords, and account details.
Session Store – Keeps session tokens and active login data.
Logs/Audit Store – Records login attempts and key system events.

How The Data Flows:

1. **User** → **Web Front-End:** Login or register via HTTPS form.
2. **Web Front-End** → **Authentication Service:** Sends credentials for verification.
3. **Authentication Service** → **Database:** Checks stored user data..
4. **Authentication Service** → **Web Front-End:** Returns session token if valid. 5. **Web Front-End** → **User:** Sends secure cookie/session token to browser. 6. **User** → **Account Management Service:** Requests account info or other data. 7. **Account Management Service** → **Database:** Reads/writes user/other details. 8. **Account Management Service** → **Email Service:** Sends notifications or reset links. 9. **All Components** → **Logs/Audit Store:** Write security and usage events.

Customer (Browser/App)	Spoofing (1)	Fake HP login pages trick users into entering credentials (phishing).	Enforce HTTPS and HSTS; utilize DMARC/SPF/DKIM; educate users on phishing prevention.
Customer (Browser/App)	Information Disclosure (4)	Sensitive info exposed via insecure storage or mixed content.	Use Secure, HttpOnly, and SameSite cookies; force HTTPS-only communication.
Web Front-End Server	Tampering (2)	Attackers alter form data or URLs to access other accounts.	Validate all inputs server-side, sanitize and encode data, and enforce strong session checks.
Web Front-End Server	Denial of Service (5)	Attackers flood the portal with requests to overload it.	Utilize rate limiting, WAF, and load balancing to mitigate DDoS attacks.
Authentication Service	Spoofing (1)	Attackers attempt credential stuffing or brute force login attacks.	Use account lockout, CAPTCHA, and a strong password policy.
Authentication Service	Elevation of Privilege (6)	Malicious users manipulate tokens or sessions to gain admin access.	Enforce strict token validation; implement privilege separation.
Account Management Service	Repudiation (3)	Users modify or delete data and later deny the action.	Maintain secure, timestamped audit logs; ensure the integrity of records.
Account Management Service	Information Disclosure (4)	Unauthorized access to the profile due to insecure APIs.	Use access control on every API call; encrypt sensitive data in transit and at rest.
Database Server	Tampering (2)	Attackers alter stored data.	Use parameterized queries, least-privilege DB accounts, and encryption.
Database Server	Information Disclosure (4)	Data breach exposing user PII and credentials.	Encrypt data at rest, hash passwords, and use strict database access controls.
Email Service	Information Disclosure (4)	Password reset or verification links intercepted or reused.	Use one-time tokens with short expiry; enforce HTTPS links in all emails.
Logs/Audit Store	Repudiation (3)	Logs have been tampered with to conceal malicious activities.	Use write-once or append-only logs, and protect them with access controls and integrity checks.

5.3. Microsoft Threat Modeling Tool Outputs

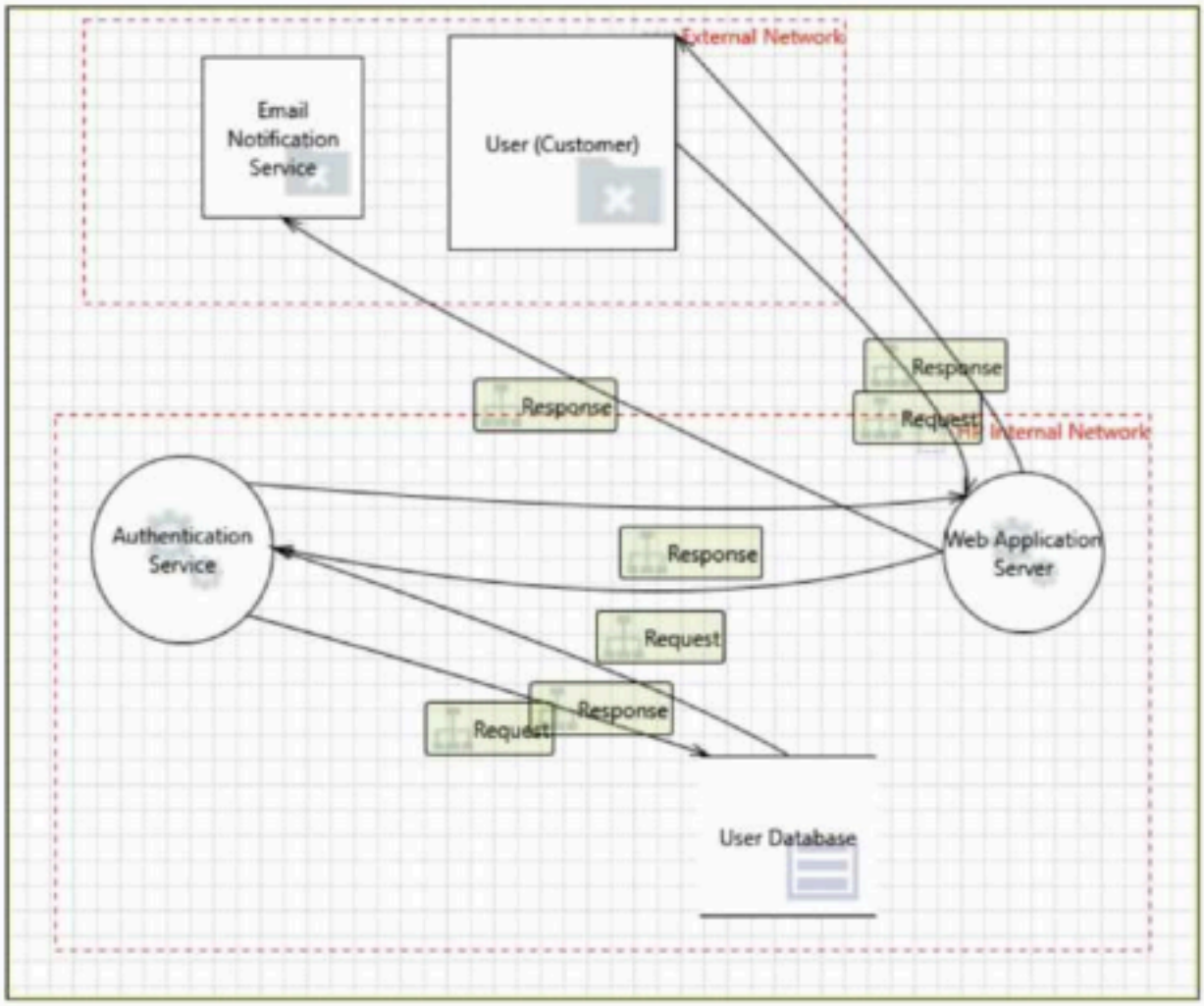


Using the Microsoft Threat Modeling Tool (MTMT), two trust boundaries were defined: one external and one internal. The system includes a user, web app, authentication, database, and email components. MTMT identified multiple STRIDE-based threats, primarily related to spoofing, tampering, and information disclosure across trust boundaries. Key mitigations include enforcing HTTPS with HSTS, implementing MFA, encrypting all sensitive data, and applying RBAC with least privilege.

Priority	Mitigation Strategy	Threats Addressed
1	Enforce HTTPS (TLS 1.3) with HSTS	Tampering, Info Disclosure

	2 Implement MFA and strong session management	Spoofing, Info Disclosure
	3 Apply WAF and rate limiting for login endpoints	DoS
	4 Encrypt all sensitive data (at rest/in transit)	Elevation of Privilege, Info Disclosure
	5 Enable secure logging and auditing	Repudiation
	6 Use least-privilege IAM and RBAC	Tampering, Elevation of Privilege

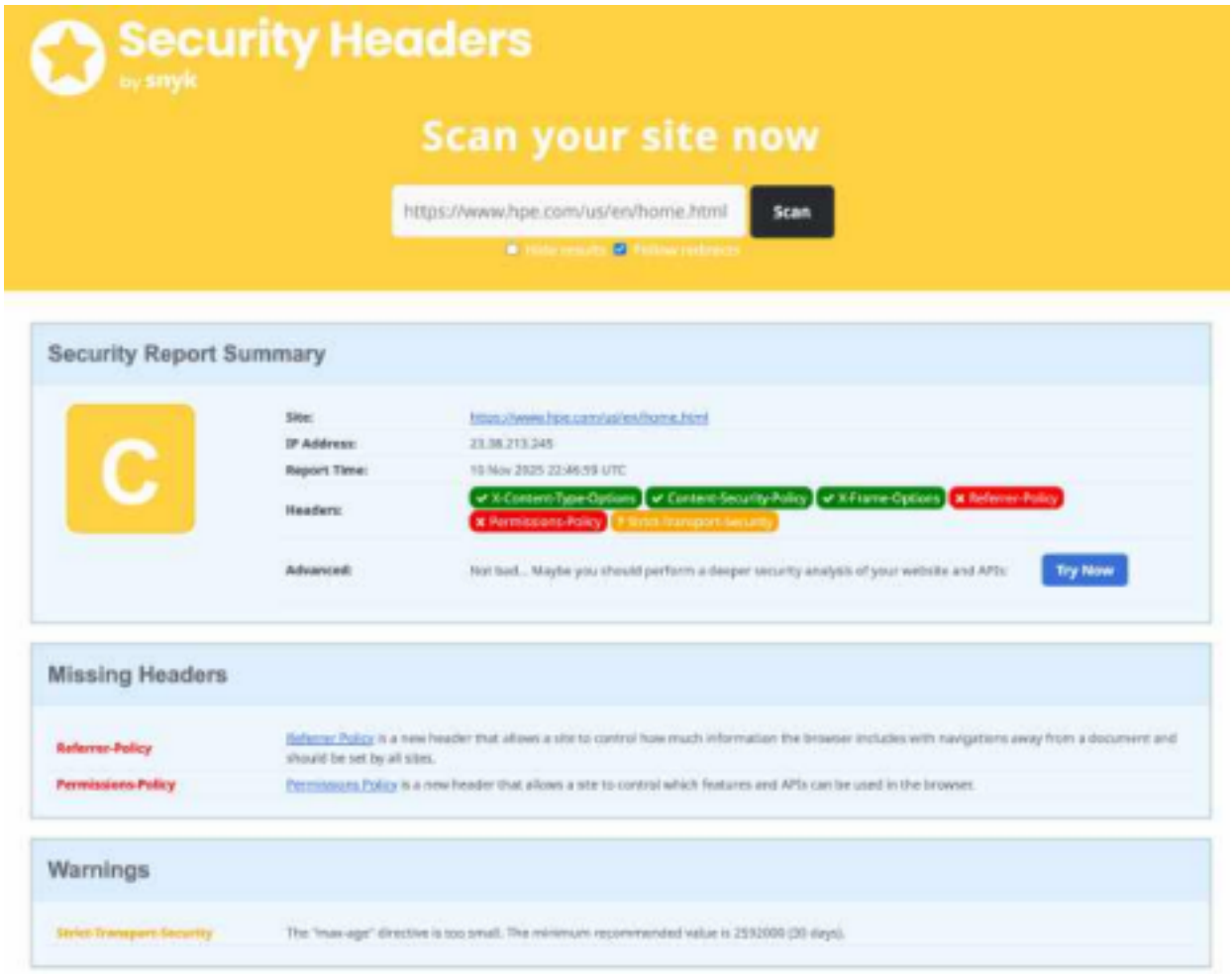
Diagram: HP Customer Account Portal Threat Model"



HP Customer Account Portal Threat Model" Diagram Summary:

Not Started	0
Not Applicable	0
Needs Investigation	12
Mitigation Implemented	0
Total	12

5.4. Web Application Security Scan Results



Our company website is missing two headers: Referrer-Policy and Permissions-Policy. The Referrer-Policy is vital because it controls how much information is sent when a user navigates away from a page. Without it, sensitive info may leak to external sites. The recommended solution is to add the Referrer-Policy header. The Permissions-Policy is also missing**.** This is not ideal because it defines which browser features are allowed to be used. Without this policy, broader access can be tapped into than intended. The recommended solution is to add the Permissions-Policy header. Additional recommendations include strengthening Strict-Transport-Security, combining strong headers with TLS 1.3, utilizing preload lists, and implementing continuous security header scanning. Doing regular header auditing and using a Web Application Firewall (WAF) will ensure smooth sailing.

5.5. Top Threats Summary

To summarize, HP's web-based customer portal is good but not great. It has many vulnerabilities and is short of perfect. To resolve all the issues, it is recommended to use: (1) HTTPS, HSTS, and secure cookies everywhere. (2) Enforce input validation and parameterized queries. (3) Implement multi-factor authentication (MFA) and role-based access control (RBAC). (4) Encrypt sensitive data both in transit and at rest. (5) Maintain immutable audit logs for non-repudiation and (6) Protect availability with WAF, rate limiting, and DDoS defenses.

HP's company website demonstrates moderate security maturity but needs minor configuration improvements to achieve a strong A rating. Implementing the missing headers and strengthening HTTPS enforcement will enhance privacy, prevent data leakage, and fortify the site against common browser-level threats, such as clickjacking and XSS. By following these steps, HP will improve its overall security across its web portal and website.

References

Kim, D., & Solomon, M. G. (2023). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

Open Worldwide Application Security Project. (n.d.). *Threat Modeling Process*. OWASP Foundation. Retrieved November 10, 2025, from https://owasp.org/www-community/Threat_Modeling_Process

OWASP Cheat Sheet Series Team. (n.d.). *Threat Modeling Cheat Sheet*. OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

STRIDE threat modeling using Microsoft threat modeling tool. (2021, March 3). [Video]. YouTube. Retrieved November 10, 2025, from https://www.youtube.com/watch?v=Wry2get_RRc

OpenAI. (2025, November 10). *ChatGPT conversation with the user about threat modeling and HTTP header analysis*. ChatGPT. https://chat.openai.com/

PART 5: SYSTEM HARDENING AND AUDITING

COMPANY: HEWLETT-PACKARD

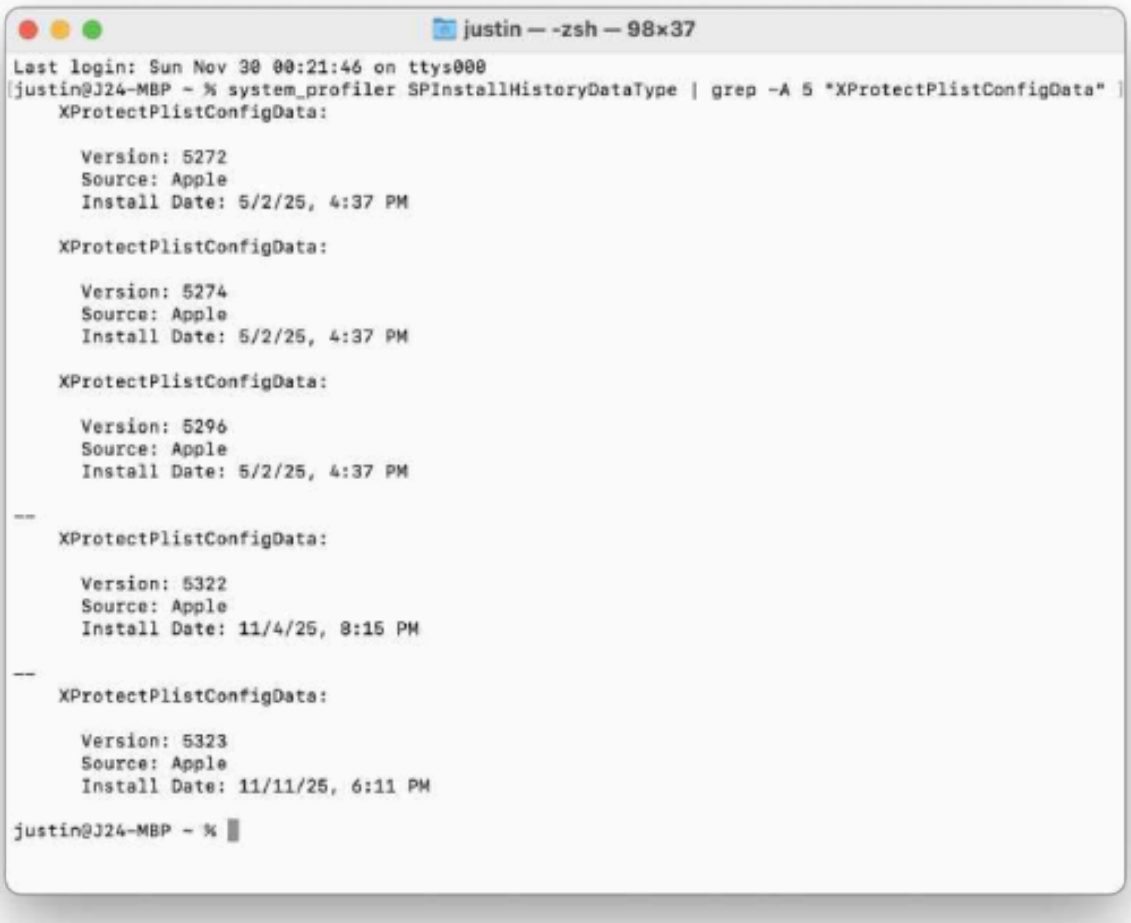
6.1. Platform Chosen

macOS 13.7.8 (22H730)

6.2. Hardening Steps Performed

1. Verify antivirus is active, updated, and scanning regularly via Terminal:

Keeping your antivirus active and up to date provides steady, reliable protection. These commands were run in the terminal to confirm that the antivirus is active, up to date, and running regular scans.



2. Enable the system firewall via Terminal:

Enabling the firewall adds an extra layer of safety by blocking unwanted connections, protecting your apps, and giving you more control. The command below was run to confirm.

Configure basic rules via Terminal:

By allowing trusted, built-in, and signed software to connect without constant pop-ups, it makes for a more seamless workspace. Also, enabling logging is highly recommended for security auditing. The commands were executed below.

3. Apply pending OS and software updates via Terminal:

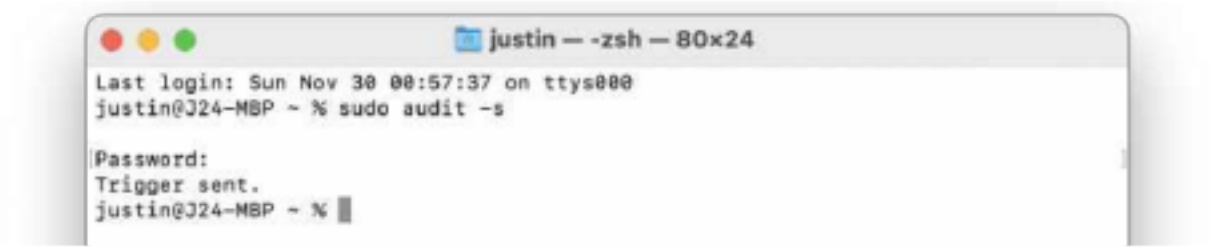
System and software updates keep your device secure, stable, and running at its best. Running the command below checked for available system and app updates.

4. Disable guest or unused user accounts via Terminal:

Disabling a guest or unused account makes the system safer, cleaner, and easier to manage. The commands below were used to disable and check.

6.3. Audit Log Configuration

macOS includes a built-in auditing system called auditd, which records security-related events. I enabled and configured it through the directory.



1. Check if auditing is enabled

2. Check what's being logged

5

Based on the results above, the audit logging system is enabled and working correctly.

The

configuration logs:

1. Logins
2. authentication events
3. command usage with arguments
4. admin user actions

Enabling audit logs gives better visibility, accountability, and a reliable record of what's happening in the system.

6.4. 24 Hour Monitoring Observations

Running the command in the terminal resulted in a successful and clean scan.
There were no failed login attempts, malware quarantine or detection events, or unusual or suspicious behavior. This is good news!

6.5. Security Enhancement Summary

How does System hardening + auditing improve security?

Hardening locks down systems, reducing the number of ways attackers can get in.

Auditing keeps a record of what happens so you can spot problems and trace issues.

Together, they prevent attacks, help you catch suspicious activity early, and keep your organization safer overall.

6.6. Emerging Threat Researched

Cybersecurity is one of the many areas that artificial intelligence is transforming. But AI is also being used by cybercriminals to improve their attack capabilities. Hackers can more easily get over conventional security measures thanks to AI-driven attacks, which can automate and scale operations. Recommended strategies to combat AI-driven attacks include integrating AI and machine learning into their cybersecurity plans. AI is not going anywhere and is only getting better by the day. By using AI to analyze large volumes of data in real time, it can identify anomalies and respond to threats more effectively. Use AI to fight AI basically.

7. Summary of Recommendations

The best way to keep your macOS system in tip-top shape is to always keep it up to date. This is key because new threats emerge every day. It doesn't stop there. Ensure FileVault encryption is enabled, activate the firewall, and ensure your antivirus software is up to date to fortify it. Eliminate unnecessary starting items, disable guest and unused accounts, and check your system for any redundant services. Lastly, turn on audit logging to monitor significant activities and identify problems early. When combined, these actions make your Mac cleaner, safer, and much harder for hackers to exploit.

References

Kim, D., & Solomon, M. G. (2023). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

Hoffman, C. (2018, July 9). *How to view the system log on a Mac*. How-To Geek. https://www.howtogeek.com/356942/how-to-view-the-system-log-on-a-mac/

Funky Space Monkey. (n.d.). *Hardening macOS: The basics*. https://www.funkyspacemonkey.com/hardening-macos-the-basics

Adelia Risk. (n.d.). *Mac security guide: 10 best practices to lock down your mac*. https://adeliarisk.com/mac-security-guide-10-best-practices/

MacMost. (2024, March 20). *15 Mac Settings To Make Your Mac More Secure (Updated for 2024)* [Video]. YouTube. https://www.youtube.com/watch?v=NSoUh3Duqrc

Molina, A. E. (2025, January 14). *The emerging cybersecurity threats in 2025: What you can do to stay ahead*. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2025/01/14/the-emerging-cybersecurity-threats-in-2025-what-you-can-do-to-stay-ahead

OpenAI. (2025, November 29). ChatGPT conversation with the user about macOS hardening and auditing. ChatGPT. https://chat.openai.com/