SAMPLE / DEMO - Sensitive client data redacted. Not a live client report. Fictional placeholders used.

CyberGuard Professional v8

Diamond Bright LLC | Business Security Assessment Report

Your CyberGuard Business Trust Score™

This is your grade — simple on purpose. It reflects what we found, what is still open, and how prepared your business looks. No scan logs. No tool dump. Just a score you can explain to anyone.

F	48/100	At Risk	30
Letter grade	Trust Score		

		Where you stand	Issues explained below

Business Trust Score graded from this scan's technical depth (DPI 5.28 / CARV C-) and the business control profile on file.

> **How to improve this grade:** Work the action list, close the money-risk items first, and keep your monthly full system check. Your next report should feel lighter — that is the point.

Diamond Business Risk Engine vbre-1.1

Sample Retail Partners LLC **: Trust F (48/100) · 30 issue(s) mapped in plain English · protection from $350/mo**

Sample Retail Partners LLC 30 item(s) on the map. None need panic — all need a plan. Work the list and watch the Trust Score move next month. CyberGuard’s mission is simple: map your real network, teach risks in plain English so you learn while you read, and price serious protection as an alternative to $1,000–$2,500+/mo enterprise or national MSP plans. Primary theme on this check: General security finding. Planning model: ~$3,787/yr disruption pressure addressed vs $350/mo program (and about $10,200/yr less than a typical $1,000+/mo enterprise-style plan). Scroll each issue: what it is, what it costs if ignored, and the fix — no jargon wall.

> **Our promise to owners:** We do not sell mystery. We sell a map, a teacher, and a fair price — so business owners can make security decisions the same way they make every other business decision: with clear facts and clear dollars.
>
> Every finding from the authorized scans was translated for business owners: what it is, what it costs in plain money terms, one teachable takeaway, and how to fix it. Nothing is left as a raw tool line.

Your network themes (not a jargon dump)

Think of this as a simple map of where risk clusters. Each theme is explained later with money language and fixes — so you learn your environment while you read.

Business theme	Issues	Critical	High
General security finding	19	0	0
Website & encryption trust	8	0	0
Remote access risk	2	0	0
Device & admin panel risk	1	0	0

At a glance — pure clarity

Critical	F	30	221
Business risk level	Trust grade	Issues explained	Devices mapped

Everything below is written for business owners. You will not see raw scan logs, port dumps, or tool noise — only what matters, what it costs if ignored, and what to do.

AI Client Protection Brief

Sample Retail Partners LLC **: Trust F (48/100) · 30 issue(s) mapped in plain English · protection from $350/mo**

Your network: Sample Retail Partners LLC 30 item(s) on the map. None need panic — all need a plan. Work the list and watch the Trust Score move next month. CyberGuard's mission is simple: map your real network, teach risks in plain English so you learn while you read, and price serious protection as an alternative to $1,000–$2,500+/mo enterprise or national MSP plans. Primary theme on this check: General security finding. Planning model: ~$3,787/yr disruption pressure addressed vs $350/mo program (and about $10,200/yr less than a typical $1,000+/mo enterprise-style plan). Scroll each issue: what it is, what it costs if ignored, and the fix — no jargon wall.

Your devices: We looked at 221 business system(s) and devices tied to this review. Most items are lower pressure, but cleaning them up still reduces surprise bills later. Multi-factor authentication does not appear fully enabled — this is one of the fastest ways to protect employee devices and accounts. Endpoint protection may not be consistently deployed across all business devices.

Steps to fix and reduce risk

Step 1: Exposed HTTP service on port 80

Review whether HTTP on HOST-OFFICE.sample.local [redacted host] 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: HOST-OFFICE.sample.local [redacted host]

Step 2: Server remote login (SSH) is reachable

Review whether SSH on HOST-OFFICE.sample.local 22 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: HOST-OFFICE.sample.local

Step 3: Exposed ipp service on port 631

Review whether ipp on HOST-OFFICE.sample.local 631 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: HOST-OFFICE.sample.local

Step 4: Exposed zeroconf service on port 5353

Review whether zeroconf on HOST-OFFICE.sample.local 5353 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: HOST-OFFICE.sample.local

Step 5: Server remote login (SSH) is reachable

Restrict management access to VPN/admin IPs, enforce MFA where possible, patch systems, and monitor login activity.

Applies to: HOST-OFFICE.sample.local

Step 6: Exposed http service on port 3000

Review whether http on MEDIA-LOBBY.sample.local 3000 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: MEDIA-LOBBY.sample.local [redacted-host]

Step 7: Exposed rtsp service on port 7000

Review whether rtsp on MEDIA-LOBBY.sample.local [redacted-host] 7000 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: MEDIA-LOBBY.sample.local [redacted-host]

Step 8: Website or service encryption needs attention

Review whether ssl/http on MEDIA-LOBBY.sample.local [redacted-host] 3001 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: MEDIA-LOBBY.sample.local [redacted-host]

Step 9: Exposed upnp service on port 1040

Review whether upnp on MEDIA-LOBBY.sample.local [redacted-host] 1040 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: MEDIA-LOBBY.sample.local [redacted-host]

Step 10: Exposed upnp service on port 2003

Review whether upnp on MEDIA-LOBBY.sample.local [redacted-host] 2003 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: MEDIA-LOBBY.sample.local [redacted-host]

Step 11: Exposed tcpwrapped service on port 8888

Review whether tcpwrapped on IOT-SPEAKER-01.sample.local [redacted host] 8888 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to: IOT-SPEAKER-01.sample.local [redacted host]

Step 12: Exposed HTTP service on port 80

Review whether HTTP o IOT-SENSOR-01.sample.local [redacted host] 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

Applies to IOT-SENSOR-01.sample.local [redacted host]

Need help? Your CyberGuard team can schedule remediation, verify fixes, and rerun the scan to confirm your protection score improves.

Client Profile

Client Contact	Alex Morgan
Contact Email	contact@sample-retail.example
Business / Organization	Sample Retail Partners LLC
Business Type	General Business
Employees	5
Estimated Revenue Per Day	$1,000

Cyber Insurance	No
Backups	No
Backups Tested Recently	No
Critical Systems	No
Remote Access / Remote Workers	No
Sensitive Data	No
Estimated Compliance Records	5000
Mapped Compliance Frameworks	FTC
Mapped Data Types	Not specified
MFA Enabled	No
EDR / Endpoint Protection	No
Security Training	No
Incident Response Plan	No
Vendor Risk Review	No

Business Impact Analysis

$3,000 Minor Incident	**$12,000** Moderate Incident	**$28,000** Major Incident	**$1,000/ day**

			Your revenue basis

Based on a Diamond CyberGuard score of 53/100 and the supplied business profile, CyberGuard estimates business risk as Critical. A minor incident could cost approximately $3,000, a moderate outage could cost approximately $12,000, and a major ransomware or operational disruption event could exceed $28,000.

Insurance note: $250,000-$500,000 cyber liability coverage recommended

Your money math — ROI without the scare tactics

Big firms often sell fear at $1,200+ per month and still hand you a technical PDF. CyberGuard shows you the map, teaches each issue in plain English, prices protection at $350/mo, and measures progress with a Trust Score you can actually understand.

In dollars: protecting against ~$3,787/yr of disruption pressure under CyberGuard Diamond™ at $350/mo (ops ROI -9.8%). Compliance model adds a separate lens (~4627.3% ROI). Versus common $1,000+/mo enterprise-style plans, you keep roughly $10,200/yr in budget — money that can go to fixes, staff, and growth.

$350/mo	**$1,200+/mo**	**$10,200/yr**	**-9.8%**
CyberGuard program	Typical enterprise-style plans	Budget you keep vs $1k+/mo	Ops ROI (model)

$3,787	**$4,200**	**4627.3%**	**41.1**

Avoided disruption / yr	Program annual cost	Compliance ROI (model)	Months of CG per 1 enterprise year

Expected annual disruption pressure	$5,569
Avg annual compliance exposure (planning)	$291,980
Recommended package	CyberGuard Diamond™
Enterprise benchmark used	$1,000–$2,500+/mo enterprise or national MSP plans

How we do the math (no black box): Your money math: expected disruption pressure ~$5,569/yr × 68% reduction ≈ $3,787 protected. CyberGuard Diamond™ costs $350/mo ($4,200/yr) → ops ROI -9.8%. Compliance planning ROI (separate): 4627.3%. Compared with typical $1,000–$2,500+/mo enterprise or national MSP plans (~$1,200/mo), CyberGuard is about $10,200/yr less while still mapping every finding into owner language.
ROI figures are decision-support models based on your scan findings, business profile, and published package pricing. Enterprise price benchmarks are market illustrations, not a quote from any specific vendor. Not insurance, legal advice, or a guarantee of savings.

Annual Compliance Exposure ROI vs. CyberGuard Cost

$291,980	$2,580	$151,830	5784.9%
Avg Annual Compliance Risk	Avg Annual CyberGuard Cost	Avg Avoided Annual Exposure	Annual Compliance ROI

CyberGuard modeled compliance exposure across detected frameworks for this business profile, control gaps, sensitive-data indicators, and scan findings. The **average yearly compliance exposure risk** is **$291,980** (midpoint of modeled low/high range: $53,080 – $530,880). That annual risk is compared to the **average annual CyberGuard portfolio cost** of **$2,580** ($215/month across CyberGuard Essential™, CyberGuard Guardian™, CyberGuard Diamond™). Recommended plan: **CyberGuard Diamond™** at **$4,200**/year.

Annual Compliance ROI: With portfolio-average risk reduction of **52%**, CyberGuard is modeled to avoid **$151,830** in average annual compliance exposure against an investment of **$2,580** — a net annual value of **$149,250** and ROI of **5784.9%**. One year of average compliance risk equals about **113.2** year(s) of the average CyberGuard package. The recommended **CyberGuard Diamond™** tier models **68%** reduction, **$198,546** avoided annual exposure, and **4627.3%** annual ROI at **$4,200**/year.

Framework	Why It May Apply	Model Inputs	Modeled Low	Modeled High
FTC / Safeguards / Consumer Data per violation	Modeled exposure for FTC-style privacy/security enforcement, Safeguards Rule, or unfair/deceptive security representations.	10 issue(s) 5000 modeled record(s)	$53,080	$530,880

Annual Compliance ROI by Package

Package	Avg Annual Cost	Modeled Risk Reduction	Avoided Annual Exposure	Annual ROI	Years of Coverage
CyberGuard Essential™	$98/mo $1,176/yr	35%	$102,193	8589.9%	248.3

CyberGuard Guardian™	$197/mo $2,364/yr	52%	$151,830	6322.6%	123.5
CyberGuard Diamond™	$350/mo $4,200/yr	68%	$198,546	4627.3%	69.5

Compliance exposure is a planning model, not legal advice or an official fine calculation. Actual fines depend on regulator, jurisdiction, facts, harm, prior history, cooperation, and corrective action. Annual compliance ROI compares the average yearly compliance exposure risk against the average annual CyberGuard portfolio cost (Essential™, Guardian™, and Diamond™), using portfolio-average risk reduction.

About this check

Date	2026-07-17 22:57:59
Prepared for	Sample Retail Partners LLC
Type of review	CyberGuard Deep Scan™
Issues explained	30
Devices mapped	221

This document is the owner summary. Internal scan details stay with CyberGuard so your reading experience stays calm and clear.

Your prioritized action list

Start at the top. Each step is written so you know what “done” looks like.

1. **Exposed HTTP service on port 80** — Review whether HTTP on HOST-OFFICE.sample.local [redacted host] 80 must be reachable on the

internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)

2. **Server remote login (SSH) is reachable** — Review whether SSH on HOST-OFFICE.sample.local [redacted host] 22 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~1–3 hours)
3. **Exposed ipp service on port 631** — Review whether ipp on HOST-OFFICE.sample.local [redacted host] 631 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
4. **Exposed zeroconf service on port 5353** — Review whether zeroconf on HOST-OFFICE.sample.local [redacted host] 5353 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
5. **Server remote login (SSH) is reachable** — Restrict management access to VPN/admin IPs, enforce MFA where possible, patch systems, and monitor login activity. (~1–3 hours)
6. **Exposed http service on port 3000** — Review whether http on MEDIA-LOBBY.sample.local [redacted host] 3000 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
7. **Exposed rtsp service on port 7000** — Review whether rtsp on MEDIA-LOBBY.sample.local [redacted host] 7000 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
8. **Website or service encryption needs attention** — Review whether ssl/http on MEDIA-LOBBY.sample.local [redacted host] 3001 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~1–2 hours)
9. **Exposed upnp service on port 1040** — Review whether upnp on MEDIA-LOBBY.sample.local [redacted host] 1040 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
10. **Exposed upnp service on port 2003** — Review whether upnp on MEDIA-LOBBY.sample.local [redacted host] 2003 must be reachable on the

internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)

11. **Exposed tcpwrapped service on port 8888** — Review whether tcpwrapped on IOT-SPEAKER-01.sample.local [redacted host] 8888 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
12. **Exposed HTTP service on port 80** — Review whether HTTP o IOT-SENSOR-01.sample.local [redacted host] 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
13. **Exposed HTTP service on port 80** — Review whether HTTP on GW-ROUTER-01 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
14. **Exposed dhcps service on port 67** — Review whether dhcps on GW-ROUTER-01 67 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
15. **Exposed domain service on port 53** — Review whether domain on GW-ROUTER-01 53 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~Varies — usually under half a day)
16. **Website or service encryption needs attention** — Review whether ssl/https? on GW-ROUTER-01 443 must be reachable on the internal network. Restrict access to trusted devices and patch the service. (~1–2 hours)
17. **Website or service encryption needs attention** — Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily. (~1–2 hours)
18. **Website or service encryption needs attention** — Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily. (~1–2 hours)

19. **Website or service encryption needs attention** — Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily. (~1–2 hours)
20. **Website or service encryption needs attention** — Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily. (~1–2 hours)

Every issue — explained so you can breathe

No raw scan output. No tool noise. For each issue we found you get plain English, money terms, a short lesson, and a fix checklist. Read it like a walkthrough of your own business — because it is.

Worth fixing · Exposed HTTP service on port 80

General security finding · Where: HOST-OFFICE.sample.local · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether HTTP on HOST-OFFICE.sample.local [redacted host] 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Server remote login (SSH) is reachable

Remote access risk · Where: HOST-OFFICE.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: SSH is a powerful remote admin doorway. If it is open broadly, bots will try to guess passwords or use stolen keys.

Why it matters for your business: A single compromised server can become a launch pad for attacks against the rest of your business.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: if a stranger can knock on a remote-login door, they do not need to ‘hack’ anything fancy — they only need one weak password.

What to do next (1–3 hours · usually IT / hosting provider):

1. Review whether SSH on HOST-OFFICE.sample.local [redacted host] 22 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Allow SSH only from trusted admin IPs or a VPN.
3. Disable password login; use keys and MFA where supported.

4. Keep the server patched; remove unused admin accounts.

Worth fixing · Exposed ipp service on port 631

General security finding · Where: HOST-OFFICE.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether ipp on HOST-OFFICE.sample.local [redacted host] 631 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed zeroconf service on port 5353

General security finding · Where: HOST-OFFICE.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether zeroconf on HOST-OFFICE.sample.local [redacted host] 5353 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Server remote login (SSH) is reachable

Remote access risk · Where: HOST-OFFICE.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: SSH is a powerful remote admin doorway. If it is open broadly, bots will try to guess passwords or use stolen keys.

Why it matters for your business: A single compromised server can become a launch pad for attacks against the rest of your business.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: if a stranger can knock on a remote-login door, they do not

need to ‘hack’ anything fancy — they only need one weak password.

What to do next (1–3 hours · usually IT / hosting provider):

1. Restrict management access to VPN/admin IPs, enforce MFA where possible, patch systems, and monitor login activity.
2. Allow SSH only from trusted admin IPs or a VPN.
3. Disable password login; use keys and MFA where supported.
4. Keep the server patched; remove unused admin accounts.

Worth fixing · Exposed http service on port 3000

General security finding · Where: MEDIA-LOBBY.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

In money terms: In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

Something useful to remember: Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether http on MEDIA-LOBBY.sample.local [redacted host] 3000 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed rtsp service on port 7000

General security finding · Where: MEDIA-LOBBY.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether rtsp on MEDIA-LOBBY.sample.local [redacted host] 7000 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Website or service encryption needs attention

Website & encryption trust · Where: MEDIA-LOBBY.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Review whether ssl/http on MEDIA-LOBBY.sample.local [redacted-host] 3001 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

Worth fixing · Exposed upnp service on port 1040

General security finding · Where: MEDIA-LOBBY.sample.local [redacted-host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether upnp on MEDIA-LOBBY.sample.local [redacted host] 1040 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed upnp service on port 2003

General security finding · Where: MEDIA-LOBBY.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether upnp on MEDIA-LOBBY.sample.local [redacted host] 2003 must be reachable on the internal network. Restrict access to trusted devices and patch the service.

2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed tcpwrapped service on port 8888

General security finding · Where: IOT-SPEAKER-01.sample.local [redacted host] · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether tcpwrapped on IOT-SPEAKER-01.sample.local [redacted host] 8888 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed HTTP service on port 80

General security finding · Wher[redacted host] IOT-SENSOR-01.sample.local · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether HTTP o IOT-SENSOR-01.sample.local [redacted host] 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed HTTP service on port 80

General security finding · Where: GW-ROUTER-01 · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

Something useful to remember: Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether HTTP on `GW-ROUTER-01` 80 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed dhcps service on port 67

General security finding · Where: `GW-ROUTER-01` · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

In money terms: In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

Something useful to remember: Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether dhcps on `GW-ROUTER-01` 67 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Exposed domain service on port 53

General security finding · Where: GW-ROUTER-01 · Preventable cost — plan it before it escalates

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Review whether domain on GW-ROUTER-01 53 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Worth fixing · Website or service encryption needs attention

Website & encryption trust · Where: GW-ROUTER-01 · Preventable cost — plan it before it escalates

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $1,585 of the larger disruption model (~1.6 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Review whether ssl/https? on `GW-ROUTER-01` 443 must be reachable on the internal network. Restrict access to trusted devices and patch the service.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

Small cleanup · Website or service encryption needs attention

Website & encryption trust · Where: `HOST-OFFICE.sample.local` · Cheap fix now beats expensive fire later

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $528 of the larger disruption model (~0.5 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

Small cleanup · Website or service encryption needs attention

Website & encryption trust · Where: IOT-SPEAKER-01.sample.local [redacted host] · Cheap fix now beats expensive fire later

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $528 of the larger disruption model (~0.5 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

Small cleanup · Website or service encryption needs attention

Website & encryption trust · Wher[redacted host]IOT-SENSOR-01.sample.local · Cheap fix now beats expensive fire later

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $528 of the larger disruption model (~0.5 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.

4. Redirect HTTP to HTTPS for customer-facing sites.

Small cleanup · Website or service encryption needs attention

Website & encryption trust · Where: GW-ROUTER-01 · Cheap fix now beats expensive fire later

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $528 of the larger disruption model (~0.5 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

Small cleanup · Website or service encryption needs attention

Website & encryption trust · Where: GW-ROUTER-01 · Cheap fix now beats expensive fire later

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: even smaller issues compound. This one carries about $528 of the larger disruption model (~0.5 day(s) of revenue). Clean it up on a calm Tuesday, not during a crisis.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm this web service is authorized, patched, TLS protected, and not exposing a default/admin portal unnecessarily.
2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

FYI · ipp exposed on HOST-OFFICE.sample.local :631/tcp

General security finding · Where: HOST-OFFICE.sample.local · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · zeroconf exposed on HOST-OFFICE.sample.local [redacted.local] :5353/udp

General security finding · Where: HOST-OFFICE.sample.local [redacted.local] · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · A device admin page or smart device is exposed

Device & admin panel risk · Where: MEDIA-LOBBY.sample.local · Worth knowing

What this means: Cameras, printers, routers, and smart devices often ship with weak defaults and rarely get updates.

Why it matters for your business: Compromised IoT can spy on the business or help attackers move deeper into the network.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: cameras and printers are computers too. If nobody updates them, they become free parking for attackers.

What to do next (2–6 hours · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Change default admin passwords; put IoT on a separate Wi-Fi/VLAN if possible.
3. Block admin pages from the internet.
4. Update firmware or replace end-of-life devices.

FYI · rtsp exposed on MEDIA-LOBBY.sample.local :7000/tcp

General security finding · Where: MEDIA-LOBBY.sample.local · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · Website or service encryption needs attention

Website & encryption trust · Where: MEDIA-LOBBY.sample.local · Worth knowing

What this means: Encryption (HTTPS/TLS) protects customers and staff when they connect. Weak or expired certificates undermine trust and can block modern browsers.

Why it matters for your business: Broken encryption hurts customer confidence and can contribute to compliance exposure.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: the lock icon on a website is customer trust. Broken encryption is a quiet way to look unprofessional — and get sued.

What to do next (1–2 hours · usually Web host / IT):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.

2. Install or renew a valid certificate from a trusted provider.
3. Disable outdated protocols (e.g. TLS 1.0/1.1) on public services.
4. Redirect HTTP to HTTPS for customer-facing sites.

FYI · upnp exposed on MEDIA-LOBBY.sample.local [redacted host] :1040/tcp

General security finding · Where: MEDIA-LOBBY.sample.local [redacted host] · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · upnp exposed on MEDIA-LOBBY.sample.local [redacted host] :2003/tcp

General security finding · Where: MEDIA-LOBBY.sample.local [redacted host] · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · dhcps exposed on GW-ROUTER-01 :67/udp

General security finding · Where: GW-ROUTER-01 · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

FYI · domain exposed on GW-ROUTER-01 :53/tcp

General security finding · Where: GW-ROUTER-01 · Worth knowing

What this means: CyberGuard detected a security condition on your network or a device. It may not be an active attack, but it increases the chance of disruption or data loss if ignored.

Why it matters for your business: Addressing smaller issues early prevents them from becoming emergencies.

> **In money terms:** In owner terms: most breaches are not Hollywood hacks — they are unfixed basics that turn into overtime, customer apologies, and surprise bills.

> **Something useful to remember:** Owner lesson: small openings stack. The businesses that stay online treat each one like a leaky pipe, not a mystery.

What to do next (Varies — usually under half a day · usually IT / CyberGuard):

1. Confirm business need, owner, patch level, and firewall restrictions for this service.
2. Re-scan or request validation after the fix so your monthly grade can improve.

Devices we saw on your network

Friendly names only — not a port scan printout.

Device	Notes
GW-ROUTER-01 (10.50.0.1)	On your network
IOT-HUB-01.sample.local [redacted host] (10.50.0.16)	On your network
IOT-SPEAKER-01.sample.local [redacted host] (10.50.0.25)	On your network
MEDIA-LOBBY.sample.local [redacted host] (10.50.0.27)	On your network
IOT-SENSOR-01.sample.local [redacted host] (10.50.0.33)	On your network
HOST-OFFICE.sample.local [redacted host] (10.50.0.164)	On your network
10.50.0.0	On your network
10.50.0.2	On your network
10.50.0.3	On your network
10.50.0.4	On your network
10.50.0.5	On your network
10.50.0.6	On your network
10.50.0.7	On your network
10.50.0.8	On your network
10.50.0.9	On your network
10.50.0.10	On your network
MEDIA-CONSOLE.sample.local [redacted host] (10.50.0.11)	On your network
10.50.0.12	On your network
STAFF-PHONE-05.sample.local [redacted host] (10.50.0.13)	On your network
10.50.0.14	On your network
10.50.0.15	On your network
10.50.0.17	On your network
STAFF-PHONE.sample.local [redacted host] (10.50.0.18)	On your network

[redacted host] TABLET-LOBBY.sample.local (10.50.0.19)	On your network
10.50.0.20	On your network
10.50.0.21	On your network
10.50.0.22	On your network
10.50.0.23	On your network
10.50.0.24	On your network
10.50.0.26	On your network
10.50.0.28	On your network
10.50.0.29	On your network
10.50.0.30	On your network
10.50.0.31	On your network
STREAM-TV-01.sample.local [redacted host] (10.50.0.32)	On your network
10.50.0.34	On your network
10.50.0.35	On your network
10.50.0.36	On your network
10.50.0.37	On your network
10.50.0.38	On your network
10.50.0.39	On your network
10.50.0.40	On your network
10.50.0.41	On your network
10.50.0.42	On your network
10.50.0.43	On your network
10.50.0.44	On your network
10.50.0.45	On your network

10.50.0.46	On your network
10.50.0.47	On your network
10.50.0.48	On your network
10.50.0.49	On your network
10.50.0.50	On your network
10.50.0.51	On your network
10.50.0.52	On your network
10.50.0.53	On your network
10.50.0.54	On your network
10.50.0.55	On your network
10.50.0.56	On your network
10.50.0.57	On your network
10.50.0.58	On your network
10.50.0.59	On your network
10.50.0.60	On your network
10.50.0.61	On your network
10.50.0.62	On your network
10.50.0.63	On your network
10.50.0.64	On your network
10.50.0.65	On your network
10.50.0.66	On your network
10.50.0.67	On your network
10.50.0.68	On your network
10.50.0.69	On your network

10.50.0.70	On your network
10.50.0.71	On your network
10.50.0.72	On your network
10.50.0.73	On your network
10.50.0.74	On your network
10.50.0.75	On your network
10.50.0.76	On your network
10.50.0.77	On your network
10.50.0.78	On your network
10.50.0.79	On your network
10.50.0.80	On your network
10.50.0.81	On your network
10.50.0.82	On your network
10.50.0.83	On your network
10.50.0.84	On your network
10.50.0.85	On your network
10.50.0.86	On your network
10.50.0.87	On your network
10.50.0.88	On your network
10.50.0.89	On your network
10.50.0.90	On your network
10.50.0.91	On your network
10.50.0.92	On your network
10.50.0.93	On your network

10.50.0.94	On your network
10.50.0.95	On your network
10.50.0.96	On your network
10.50.0.97	On your network
10.50.0.98	On your network
10.50.0.99	On your network
10.50.0.100	On your network
10.50.0.101	On your network
10.50.0.102	On your network
10.50.0.103	On your network
10.50.0.104	On your network
10.50.0.105	On your network
10.50.0.106	On your network
10.50.0.107	On your network
10.50.0.108	On your network
10.50.0.109	On your network
10.50.0.110	On your network
10.50.0.111	On your network
10.50.0.112	On your network
10.50.0.113	On your network
10.50.0.114	On your network
10.50.0.115	On your network
10.50.0.116	On your network
10.50.0.117	On your network

10.50.0.118	On your network
10.50.0.119	On your network
10.50.0.120	On your network
10.50.0.121	On your network
10.50.0.122	On your network
10.50.0.123	On your network
10.50.0.124	On your network
10.50.0.125	On your network
10.50.0.126	On your network
10.50.0.127	On your network
10.50.0.128	On your network
10.50.0.129	On your network
10.50.0.130	On your network
10.50.0.131	On your network
10.50.0.132	On your network
10.50.0.133	On your network
10.50.0.134	On your network
10.50.0.135	On your network
10.50.0.136	On your network
10.50.0.137	On your network
10.50.0.138	On your network
10.50.0.139	On your network
10.50.0.140	On your network
10.50.0.141	On your network

10.50.0.142			On your network
10.50.0.143			On your network
10.50.0.144			On your network
10.50.0.145			On your network
10.50.0.146			On your network
10.50.0.147			On your network
10.50.0.148			On your network
10.50.0.149			On your network
10.50.0.150			On your network
10.50.0.151			On your network
10.50.0.152			On your network
10.50.0.153			On your network
10.50.0.154			On your network
10.50.0.155			On your network
10.50.0.156			On your network
10.50.0.157			On your network
10.50.0.158			On your network
10.50.0.159			On your network
10.50.0.160			On your network
[redacted host]	STAFF-MAC-01.sample.local	(10.50.0.161)	On your network
10.50.0.162			On your network
10.50.0.163			On your network
10.50.0.165			On your network
10.50.0.166			On your network

10.50.0.168	On your network
10.50.0.169	On your network
10.50.0.170	On your network
10.50.0.171	On your network
10.50.0.172	On your network
10.50.0.173	On your network
10.50.0.174	On your network
10.50.0.175	On your network
10.50.0.176	On your network
10.50.0.177	On your network
10.50.0.178	On your network
10.50.0.179	On your network
10.50.0.180	On your network
10.50.0.181	On your network
10.50.0.182	On your network
10.50.0.183	On your network
10.50.0.184	On your network
10.50.0.185	On your network
10.50.0.186	On your network
10.50.0.187	On your network
10.50.0.188	On your network
10.50.0.189	On your network
10.50.0.191	On your network
10.50.0.225	On your network

10.50.0.226	On your network
10.50.0.227	On your network
10.50.0.228	On your network
10.50.0.229	On your network
10.50.0.230	On your network
10.50.0.231	On your network
10.50.0.232	On your network
10.50.0.233	On your network
10.50.0.234	On your network
10.50.0.235	On your network
10.50.0.236	On your network
10.50.0.237	On your network
10.50.0.238	On your network
10.50.0.239	On your network
10.50.0.240	On your network
10.50.0.241	On your network
10.50.0.242	On your network
10.50.0.243	On your network
10.50.0.244	On your network
10.50.0.245	On your network
10.50.0.246	On your network
10.50.0.247	On your network
10.50.0.248	On your network
10.50.0.249	On your network

10.50.0.250	On your network
10.50.0.251	On your network
10.50.0.252	On your network
10.50.0.253	On your network
10.50.0.254	On your network
10.50.0.255	On your network

Recommended CyberGuard plan

CyberGuard Diamond™
Best fit

98%
Match confidence

Critical
Business risk today

30
Issues in this plan

Why This Package Was Recommended

- Patch or update risk signals were detected.
- Remote access or management exposure should be reviewed.
- No backup program was reported.

Recommended Services

- Backup & Disaster Recovery Planning
- Firewall & Remote Access Review
- Patch Management Review

CyberGuard Diamond™ Includes

Best For: Organizations that need executive-level technology planning, disaster recovery strategy, and cyber risk oversight.

- Monthly Executive Meeting
- Complete Threat Assessment
- Disaster Recovery Planning
- Cyber Risk Trend Analysis
- Technology Planning
- Vendor Management

- AI Executive Reports
- Emergency Priority Response

Next Step: Schedule a remediation consultation with Diamond Bright LLC to review this assessment, prioritize fixes, and select the right CyberGuard service plan.

Email: contact@sample-retail.example
Phone: (618) 936-8308
Website: diamondguards.com

Business Continuity Value Analysis

$12,000	122.4	60.9	60.9
Estimated One-Day Downtime	Months of Essential™	Months of Professional™	Months of Executive™

An estimated one-day business disruption could cost approximately $12,000. That same amount could fund multiple months of proactive CyberGuard protection depending on the selected service plan.

Why this matters: The estimated cost of a single day of downtime may exceed the cost of several months of proactive CyberGuard protection. Preventive cybersecurity services are designed to reduce disruption, improve readiness, and support long-term business continuity.

CyberGuard Protection Plans

Plan	Best For	Assessment	Monitoring	Priority Support
CyberGuard Essential™	Small Business	Monthly	Basic	No

CyberGuard Professional™	Growing Businesses	Monthly	Advanced	Yes ✓
CyberGuard Executive™	Executive Protection	Continuous	AI Monitoring	VIP ✓

Your Recommended Plan: **CyberGuard Diamond™**

CyberGuard automatically selected this plan based on your Diamond scan findings, business profile, and operational risk.

What “better” looks like next month

Close the urgent and important items, keep your monthly full system check, and your Trust Score should feel more stable — fewer surprises, clearer spend, and a network you understand. That is the relief this report is built for.

A note from CyberGuard

Dollar figures are planning estimates from your business profile and this check — tools for decisions, not invoices or legal advice. If anything still feels unclear, that is on us: call or email and we will walk the list with you in plain language.

CyberGuard Deep Scan™ — Multi-Step Assessment Bundle

Authorized remote scan node SAMPLE-NODE-**OFFICE-DEEP-SCAN** completed 8 coordinated assessment step(s). This deliverable merges technical evidence, business impact, compliance exposure, downtime value, and ROI analysis.

#	Scan Step	Status	Result
1	CyberGuard Reach Check™	completed	Ping check completed.
2	CyberGuard Pulse Map™	completed	Quick discovery completed.
3	CyberGuard Surface Guard™	completed	Surface snapshot completed.
4	CyberGuard Web Shield™	completed	Web & TLS posture completed.
5	CyberGuard Identity Watch™	completed	Identity exposure completed.
6	CyberGuard Apex Core™	completed	Diamond sample_deep_scan completed: 3 host(s), 6 phase(s), 0 failed. Internal LAN complete; WAN/CVE layer runs from owner command center. (client nmap fallback)
7	CyberGuard Endpoint Posture™	completed	Diamond endpoint_posture_probe completed: 2 host(s), 6 phase(s), 0 failed. (client nmap fallback)
8		completed	Diamond sample_perimeter_check

	CyberGuard Perimeter Watch™	completed: 2 host(s), 6 phase(s), 0 failed. (client nmap fallback)

Endpoint Posture Highlights

Windows updates: **gap** · AV/EDR: **gap** · Printers: **not_detected**

Bundle Evidence Excerpt

```
nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 7.22 seconds

### identity
Starting Nmap 7.99 ( https://nmap.org ) at 2026-07-17 17:51 -0500
Nmap scan report for [redacted-host] (HOST-OFFICE.sample.local (10.50.0.164 )
Host is up, received user-set (0.000040s latency).
Not shown: 14 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 10.3p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 2.45 seconds

### deep
Starting Nmap 7.99 ( https://nmap.org ) at 2026-07-17 17:51 -0500
No profinet devices in the subnet
Pre-scan script results:
| targets-ipv6-multicast-echo:
|   IP: fe80::sample:0                  MAC: aa:bb:cc:dd:ee:01          IFACE: wlan0
|   IP: fe80::sample:1                  MAC: aa:bb:cc:dd:ee:00          IFACE: wlan0
|_  Use --script-args=newtargets to add the results as targets
| targets-ipv6-multicast-invalid-dst:
|   IP: fe80::sample:1                  MAC: aa:bb:cc:dd:ee:00          IFACE: wlan0
|_  Use --script-args=newtargets to add the results as targets
|_knx-gateway-discover: ERROR: Script execution failed (use -d to debug)
|_targets-sniffer: Sniffed 0 address(es).
| targets-ipv6-multicast-mld:
|   IP: fe80::sample:0                  MAC: aa:bb:cc:dd:ee:01          IFACE: wlan0
|
|_  Use --script-args=newtargets to add the results as targets
| eap-info:
| Available authentication methods with identity="anonymous" on interface
eth0
|   unknown  EAP-TTLS
|   unknown  EAP-TLS
|   unknown  EAP-MSCHAP-V2
|_  unknown  PEAP
| broadcast-listener:
|   ether
```

```
|       ARP Request
|         sender ip     sender mac         target ip
|         10.50.0.1     aa:bb:cc:dd:ee:01  10.50.0.165
|         0.0.0.0       aa:bb:cc:dd:ee:02  10.50.0.33
|         10.50.0.33    aa:bb:cc:dd:ee:02  10.50.0.33
|         10.50.0.27    aa:bb:cc:dd:ee:03  10.50.0.73
|   udp
|       DHCP
|         srv ip       cli ip         mask           gw
dns          vendor
|         10.50.0.1     10.50.0.165    255.255.255.0  10.50.0.1
10.50.0.1          -
|         10.50.0.1     10.50.0.166    255.255.255.0  10.50.0.1
10.50.0.1          -
|_broadcast-pppoe-discover: ERROR: Script execution failed (use -d to debug)
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_broadcast-igmp-discovery: ERROR: Script execution failed (use -d to debug)
|_broadcast-eigrp-discovery: ERROR: Script execution failed (use -d to
debug)
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
|_mrinfo: ERROR: Script execution failed (use -d to debug)
|_broadcast-ospf2-discover: ERROR: Script execution failed (use -d to debug)
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: wlan0
|     IP Offered: 10.50.0.166
|     Server Identifier: 10.50.0.1
|     Subnet Mask: 255.255.255.0
|     Broadcast Address: 10.50.0.255
|     Router: 10.50.0.1
|     Domain Name Server: 10.50.0.1
|_    Domain Name: sample.local
|_broadcast-pim-discovery: ERROR: Script execution failed (use -d to debug)
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's
API. See https://www.robtex.com/api/
Nmap scan report for GW-ROUTER-01 (10.50.0.1)
Host is up, received user-set (0.011s latency).
Not shown: 994 closed tcp ports (conn-refused), 3 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE REASON  VERSION
53/tcp  open  domain  syn-ack dnsmasq 2.80
| vulners:
|   cpe:/a:thekelleys:dnsmasq:2.80:
|       EDB-ID:42943    9.8     https://vulners.com/exploitdb/EDB-ID:42943
*EXPLOIT*
|       EDB-ID:42942    9.8     https://vulners.com/exploitdb/EDB-ID:42942
*EXPLOIT*
|       EDB-ID:42941    9.8     https://vulners.com/exploitdb/EDB-ID:42941
*EXPLOIT*
|       CVE-2017-14493  9.8     https://vulners.com/cve/CVE-2017-14493
|       CVE-2017-14492  9.8     https://vulners.com/cve/CVE-2017-14492
|       CVE-2017-14491  9.8     https://vulners.com/cve/CVE-2017-14491
|       CVE-2020-25682  8.3     https://vulners.com/cve/CVE-2020-25682
|       CVE-2020-25681  8.3     https://vulners.com/cve/CVE-2020-25681
|       SSV:96623       7.8     https://vulners.com/seebug/SSV:96623
*EXPLOIT*
|       EXPLOITPACK:708148DF89AFEA44750A9B84E292A6B9    7.8     https://
vulners.com/exploitpack/EXPLOITPACK:708148DF89AFEA44750A9B84E292A6B9
*EXPLOIT*
|       EDB-ID:42946    7.8     https://vulners.com/exploitdb/EDB-ID:42946
*EXPLOIT*
|       CVE-2017-14496  7.8     https://vulners.com/cve/CVE-2017-14496
|       1337DAY-ID-28727 7.8    https://vulners.com/zdt/1337DAY-ID-28727
*EXPLOIT*
|       SSV:96620       7.5     https://vulners.com/seebug/SSV:96620
*EXPLOIT*
```

```
|       SSV:96619       7.5     https://vulners.com/seebug/SSV:96619
*EXPLOIT*
|       SSV:96618       7.5     https://vulners.com/seebug/SSV:96618
*EXPLOIT*
|       EXPLOITPACK:E661AED6AF5BCC1565D1CB0F9878E40B    7.5     https://
vulners.com/exploitpack/EXPLOITPACK:E661AED6AF5BCC1565D1CB0F9878E40B
*EXPLOIT*
|       EXPLOITPACK:95340EB39AF331E01096F2B1CF7F1DE2    7.5     https://
vulners.com/exploitpack/EXPLOITPACK:95340EB39AF331E01096F2B1CF7F1DE2
*EXPLOIT*
|       EXPLOITPACK:572F56450B83EECCA41D07EF1B33B48B    7.5     https://
vulners.com/exploitpack/EXPLOITPACK:572F56450B83EECCA41D07EF1B33B48B
*EXPLOIT*
|       EDB-ID:42945    7.5     https://vulners.com/exploitdb/EDB-ID:42945
*EXPLOIT*
|       CVE-2023-50387  7.5     https://vulners.com/cve/CVE-2023-50387
|       CVE-2023-28450  7.5     https://vulners.com/cve/CVE-2023-28450
|       CVE-2022-0934   7.5     https://vulners.com/cve/CVE-2022-0934
|       CVE-2019-14513  7.5     https://vulners.com/cve/CVE-2019-14513
|       CVE-2017-15107  7.5     https://vulners.com/cve/CVE-2017-15107
|       CVE-2017-14495  7.5     https://vulners.com/cve/CVE-2017-14495
|       CVE-2017-13704  7.5     https://vulners.com/cve/CVE-2017-13704
|       CVE-2015-8899   7.5     https://vulners.com/cve/CVE-2015-8899
|       CVE-2005-0877   7.5     https://vulners.com/cve/CVE-2005-0877
|       1337DAY-ID-287247.5     https://vulners.com/zdt/1337DAY-ID-28724
*EXPLOIT*
|       1337DAY-ID-287237.5     https://vulners.com/zdt/1337DAY-ID-28723
*EXPLOIT*
|       1337DAY-ID-287207.5     https://vulners.com/zdt/1337DAY-ID-28720
*EXPLOIT*
|       CVE-2020-25687  7.1     https://vulners.com/cve/CVE-2020-25687
|       CVE-2020-25683  7.1     https://vulners.com/cve/CVE-2020-25683
|       SSV:66871       6.8     https://vulners.com/seebug/SSV:66871
*EXPLOIT*
|       SSV:12710       6.8     https://vulners.com/seebug/SSV:12710
*EXPLOIT*
|       SSV:12174       6.8     https://vulners.com/seebug/SSV:12174
*EXPLOIT*
|       PACKETSTORM:80896       6.8     https://vulners.com/packetstorm/
PACKETSTORM:80896       *EXPLOIT*
|       EXPLOITPACK:ECB83F9533371579F3997366C239FB4D    6.8     https://
vulners.com/exploitpack/EXPLOITPACK:ECB83F9533371579F3997366C239FB4D
*EXPLOIT*
|       EDB-ID:9617     6.8     https://vulners.com/exploitdb/EDB-ID:9617
*EXPLOIT*
|       CVE-2009-2957   6.8     https://vulners.com/cve/CVE-2009-2957
|       CVE-2015-3294   6.4     https://vulners.com/cve/CVE-2015-3294
|       EDB-ID:42944    5.9     https://vulners.com/exploitdb/EDB-ID:42944
*EXPLOIT*
|       CVE-2026-12725  5.9     https://vulners.com/cve/CVE-2026-12725
|       CVE-2017-14494  5.9     https://vulners.com/cve/CVE-2017-14494
|       CVE-2026-12969  5.3     https://vulners.com/cve/CVE-2026-12969
|       SSV:96622       5.0     https://vulners.com/seebug/SSV:96622
*EXPLOIT*
|       EXPLOITPACK:C0456C7DF1625677A211CB9799B79F9A    5.0     https://
vulners.com/exploitpack/EXPLOITPACK:C0456C7DF1625677A211CB9799B79F9A
*EXPLOIT*
|       CVE-2013-0198   5.0     https://vulners.com/cve/CVE-2013-0198
|       CVE-2012-3411   5.0     https://vulners.com/cve/CVE-2012-3411
|       1337DAY-ID-287265.0     https://vulners.com/zdt/1337DAY-ID-28726
*EXPLOIT*
|       SSV:96621       4.3     https://vulners.com/seebug/SSV:96621
*EXPLOIT*
|       SSV:12173       4.3     https://vulners.com/seebug/SSV:12173
*EXPLOIT*
|       EXPLOITPACK:22D470FAFA79A3DB978CC3F8766CC759    4.3     https://
vulners.com/exploitpack/EXPLOITPACK:22D470FAFA79A3DB978CC3F8766CC759
*EXPLOIT*
```

```
|       CVE-2021-3448   4.3     https://vulners.com/cve/CVE-2021-3448
|       CVE-2020-25686  4.3     https://
```

CyberGuard Professional™ v8
Developed by Diamond Bright LLC

AI-Powered Cybersecurity • Technology Consulting • Business Protection

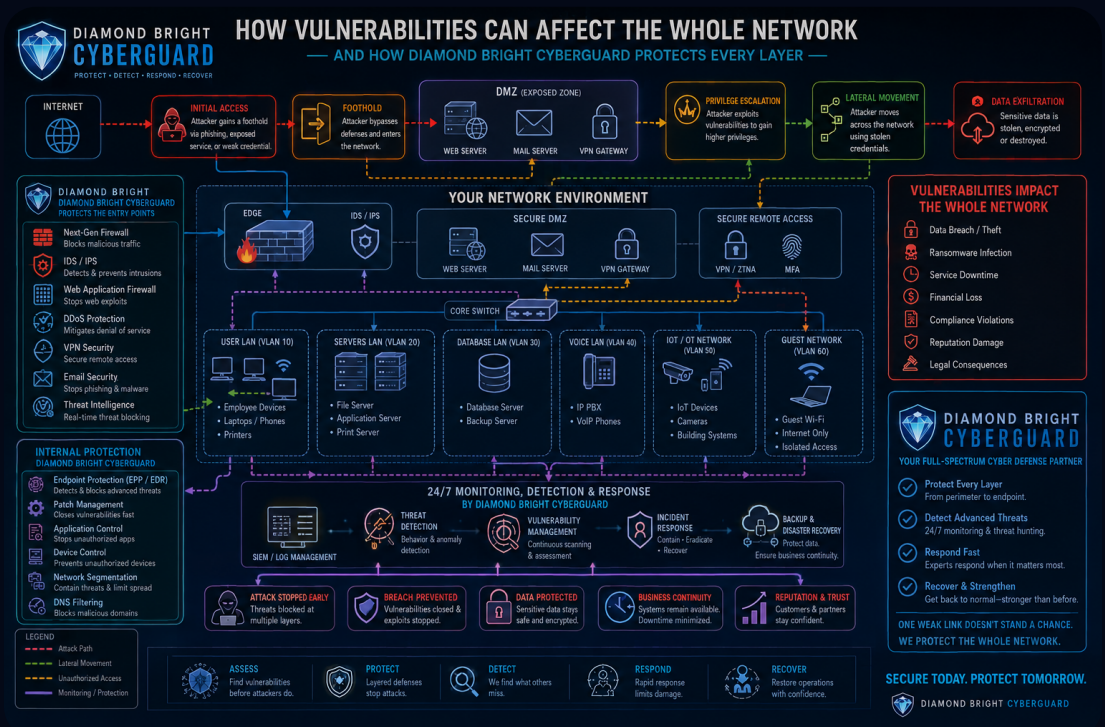
Prepared for: Sample Retail Partners LLC
Date: 2026-07-17 22:57:59

Prepared by:
Diamond Bright LLC
AI-Powered Cybersecurity & Technology Consulting

Email: contact@sample-retail.example
Phone: (618) 936-8308
Website: diamondguards.com

Network Security Architecture

How vulnerabilities can affect the whole network — and how Diamond Bright CyberGuard protects every layer.



Diamond Bright CyberGuard™ · Protect. Prevent. Empower.