Case Study: Strengthening Email Security for Two GTA Businesses with Check Point Harmony Email

Overview

Two GTA-based businesses in different industries faced increasing email-security threats. Both organizations relied on Microsoft 365's default filtering, but escalating spam, graymail, and malicious email activity created operational risk and consumed staff time. AulTECH deployed Check Point Harmony Email to both clients to reduce noise, block advanced threats, and gain clearer visibility into risk.

Despite very different environments and threat volumes, both clients saw immediate and significant improvements within the first month.

Client Profiles

Client A: Financial Planning Firm (GTA)

- 3 staff, 5 mailboxes
- Must adhere to PIPEDA data protection requirements
- Recently affected indirectly by a data breach through their investment group

Client B: Industrial Roofing Company (GTA)

- 11 office staff
- No formal governance or email hygiene standards
- One user arrived after vacation to find more than 5,000 spam emails that bypassed Microsoft 365

Challenges Before Check Point

Financial Planning Firm

- Concern about increased threat activity after their industry partner suffered a breach
- Rising spam and graymail reaching the inbox
- No visibility into threat types or volume
- Need for compliance-grade reporting to satisfy PIPEDA requirements

Industrial Roofing Company

- Microsoft 365's default filters missed large volumes of spam
- One mailbox was mail-bombed with thousands of junk messages
- Users were wasting time sorting and deleting unwanted mail
- No governance structure or monitoring

Why Check Point Harmony Email Was Selected

AulTECH selected Check Point Harmony Email due to its:

- Strong threat-prevention capabilities
- Low false-positive rate
- Clear and detailed reporting
- Competitive licensing
- Fast, seamless deployment with Microsoft 365

Deployment Summary

- **Harmony Email for Microsoft 365** deployed to both tenants
- Deployment time:
    - 10–15 minutes for both clients
- No user disruption or mail flow interruptions
- Immediate impact on inbound email filtering

Results After the First 30 Days

Client A: Financial Planning Firm

Inbound volume: 1,650 emails

Check Point Filtering (already assumed safe by M365 filters):

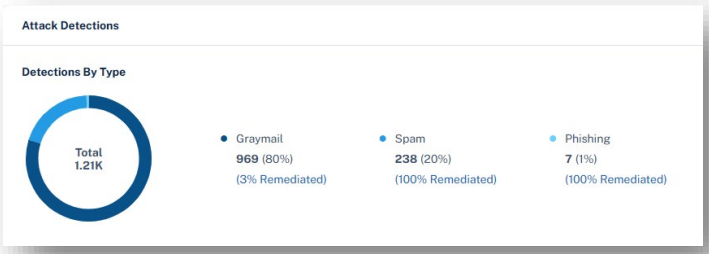
- 264 spam
- 9 malicious
- 9 suspected malicious (delivered with banner)
- 524 graymail (delivered to Junk folder)
- 0 restore requests from quarantine

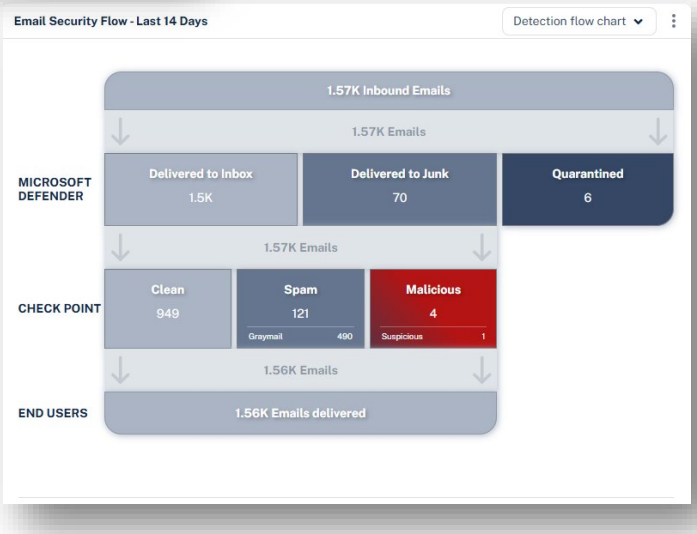
Key Outcomes:

- Clear alignment with PIPEDA requirements
- Zero malicious emails reaching end users
- Reduced time spent by staff sorting unwanted messages

Client Comment:

> *"A lot more emails land in the Junk folder. I don't have to sift through junk in the main inbox."*





Client B: Industrial Roofing Company

Inbound volume: 5,550 emails

Check Point Filtering (already assumed safe by M365 filters):

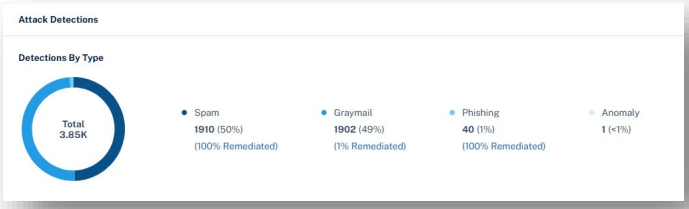
- 1,863 spam
- 40 malicious
- 2 suspicious phishing (delivered with banner)
- 1,102 graymail moved to Junk
- 0 restore requests from quarantine

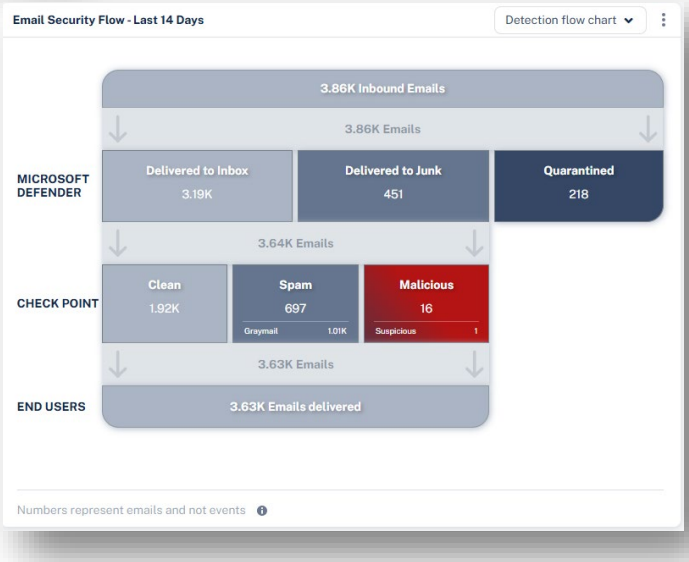
Key Outcomes:

- Immediate end to the mail-bomb event
- Sharp reduction in inbox noise
- Hours of productivity gained each week
- Strong visibility into threat types and volumes

Client Comment:

> *"The daily quarantine and junk reports help a lot. I can glance quickly to see if something shouldn't be there. It definitely reduces the amount of emails I have to look at every morning."*





Combined Business Impact

Across both clients, Check Point delivered immediate and measurable security value:

1. Stronger Protection Against Real Threats

- 49 malicious emails blocked between both firms
- Multiple phishing attempts stopped before reaching staff
- Zero ransomware-related incidents

2. Significant Reduction in Noise

- More than 3,250 spam and graymail messages blocked
- Users regained hours of productivity each week
- No false-positive restores requested

3. Better Visibility and Governance

- Detailed reporting enables faster investigation and compliance alignment
- Clear threat classification supports internal decision-making
- Supports compliance frameworks such as PIPEDA

4. Lower Business Risk and IT Overhead

- Prevented potential financial loss from phishing
- Avoided downtime and costly recovery from malicious payloads
- Reduced burden on internal staff and on AulTECH's helpdesk

Conclusion

In two very different organizations, Check Point Harmony Email delivered immediate and transformative improvements. Both clients saw a dramatic reduction in spam, stronger protection against malicious threats, and improved visibility into their email security posture.

Combined, the results demonstrate how advanced email filtering enhances security, supports compliance, and reduces operational strain for businesses of any size. AulTECH's rapid deployment and ongoing tuning ensured both clients achieved maximum value within the first month.