



# *Ransomware Defense Strategy: A Zero Trust + Microsoft Security Approach*

From backup to breach response — building a multi-layer defense that stops ransomware in its tracks.


[perparimlabs.github.io](https://perparimlabs.github.io)







# Why Ransomware Remains the #1 Cyber Threat

 PerparimLabs

- **Sophistication is rising** – Ransomware gangs now use *double extortion* (data theft + encryption).
- **Speed to impact** – Average dwell time before encryption is < 24 hours.
- **Target scope** – Hitting enterprises, small businesses, and even government agencies.
- **Cost impact** – Average recovery cost exceeds \$1.85M (source: Sophos 2024 Report).
- **Common entry points:**
  - Phishing emails with malicious attachments or links.
  - Exploited vulnerabilities in public-facing apps.
  - Compromised RDP/remote access accounts.





# Zero Trust: The Core of Ransomware Defense

PerparimLabs



**Never trust, always verify** – Every access request is authenticated, authorized, and encrypted.



IDENTITY

DEVICES

NETWORK

APPLICATIONS

DATA

**Identity-first security** – Strong MFA, Conditional Access, and risk-based sign-in policies.

**Device compliance** – Only healthy, compliant devices get access (via Intune & Defender).

**Least privilege** – Access rights are minimized and time-bound with Privileged Identity Management (PIM).

**Micro-segmentation** – Limit lateral movement within the network to contain breaches.



# Microsoft Security Tools Mapped to Ransomware Defense Phases

PerparimLabs

## 1. Prevent (Stop the attack before it starts)

- **Microsoft Entra ID** → Conditional Access, risk-based sign-in policies, MFA.
- **Microsoft Intune** → Device compliance, security baselines, app protection policies.
- **Defender for Office 365** → Safe Links, Safe Attachments, phishing detection.

PREVENT

DETECT

## 2. Detect (Identify threats early)

- **Microsoft Defender XDR** → Cross-domain detection (email, endpoints, identities, apps).
- **Microsoft Sentinel** → Centralized SIEM + threat analytics + custom detection rules.

## 3. Respond (Contain and mitigate impact)

- **Microsoft Defender for Endpoint** → Automated investigation & response (AIR), device isolation.
- **Microsoft Sentinel** → Playbooks for automated incident response.

RESPOND

RECOVER

## 4. Recover (Restore operations quickly)

- **Azure Backup** → Immutable backups for critical workloads.
- **Microsoft 365 Backup (if available)** → Rapid restore for SharePoint, OneDrive, and Exchange data.



# 🛡️ *Integrated Ransomware Defense Architecture*



## • **Outer Layer – Threat Prevention**

- Email & collaboration protection (Defender for Office 365).
- Network segmentation & VPN/ExpressRoute security.

## • **Middle Layer – Identity & Device Security**

- Microsoft Entra ID Conditional Access + MFA.
- Intune compliance & Defender for Endpoint.

IDENTITY  
& DEVICES

DATA  
RESILIENCE

DETECTION  
& RESPONSE

## • **Inner Layer – Detection & Response**

- Microsoft Defender XDR alerts feeding Microsoft Sentinel.
- Sentinel analytics + automation playbooks for containment.

## • **Core – Data Resilience**

- Azure Backup & Microsoft 365 Backup with immutability.
- Tested recovery plans & regular DR drills.

# ⚡ *Ransomware Incident Response Playbook*



## DETECT

### Phase 1 – Detect & Alert

- Confirm alert from Microsoft Defender XDR or Sentinel.
- Identify affected devices, accounts, and data.

## CONTAIN

### Phase 2 – Contain the Threat

- Isolate infected endpoints with Defender for Endpoint.
- Disable compromised accounts in Microsoft Entra ID.
- Block malicious IPs/URLs at the firewall or via Defender.

## ERADICATE

### Phase 3 – Eradicate

- Remove malicious files & registry changes.
- Patch exploited vulnerabilities.
- Reset credentials for compromised accounts.

## RECOVER

### Phase 4 – Recover

- Restore systems from Azure Backup / Microsoft 365 Backup.
- Validate integrity of restored data.
- Re-onboard devices into compliance with Intune.

## REVIEW

### Phase 5 – Post-Incident Review

- Run Sentinel investigation to trace attack path.
- Update Conditional Access / security baselines to close gaps.
- Document lessons learned and share with security teams.



SIMULATE



# *Keep the Defense Strong: Test, Learn, Improve*



REPORT

## • **Regular Attack Simulations**

- Use Microsoft Defender Attack Simulation Training (phishing, credential harvesting).
- Run red team / blue team tabletop exercises.

## • **Backup & Restore Drills**

- Quarterly test restores from Azure Backup and Microsoft 365 Backup.
- Validate RPO (Recovery Point Objective) and RTO (Recovery Time Objective) goals.

## • **Policy & Configuration Reviews**

- Audit Conditional Access, Intune compliance, and Sentinel rules monthly.
- Update based on latest threat intelligence from Microsoft Security Center.

## • **Metrics & Reporting**

- Track incidents prevented, mean time to detect (MTTD), and mean time to respond (MTTR).
- Share metrics with leadership to justify continued investment in security.

REVIEW