GBS

Anti-Ransomware Defending Against Ransomware in the Middle East

OUR COURSE OF ACTION

Presented By

GBS Cybersecurity Team

www.gbsits.com

1. Executive Summary

Introduction

Ransomware has emerged as the most pervasive cybersecurity threat in the Middle East, especially across critical sectors like finance, healthcare, and government. With a 68% increase in ransomware incidents reported in the region (Group-IB, 2023), organizations need more than traditional antivirus tools—they need resilient, AI-powered, and managed defense solutions.

This paper outlines the critical risks, evolving tactics of ransomware actors, and how modern anti-ransomware solutions empower IT leaders to detect, contain, and recover from attacks without business disruption.

Let's begin with a simple poll we did at GBS. We asked:
Why do companies still get breached in 2025? Here's how it played out:

What Causes Most Breaches? : Poll Vs Reality

89% of People Voted

- Lack of Skilled Personnel
- Weak Passwords

Let's Check the Reality -

60% of Breaches Involved Supply Chain or Third-Party Risk

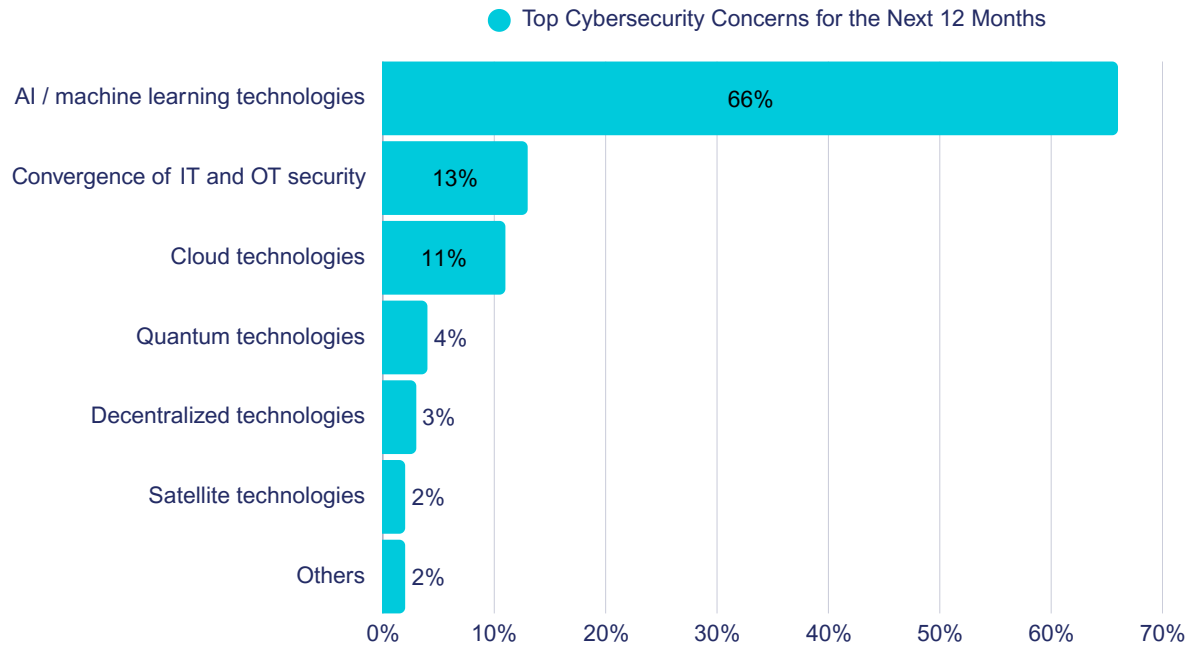
70% had No Tested Incident Response Plan

Most were Using Antivirus or EDR Only, with No Resilience Strategy

2. Threat of Ransomware

The Growing Threat of Ransomware in the Middle East

The GCC region has witnessed a marked increase in ransomware attacks, driven by geopolitical tensions, AI-powered malware, and expanding digital infrastructure. Here's how cybersecurity is evolving,



In your view, which of the following will most significantly affect cybersecurity in the next 12 months?

UAE alone saw a 32% YOY increase in 2024, with critical sectors like financial services and healthcare particularly vulnerable.

Ransomware-as-a-Service (RaaS), phishing, and compromised MSPs are key vectors. The average downtime post-attack ranges from 7–12 days, with recovery costs exceeding $4 million per incident (IBM, 2024).

3. Anti-Ransomware

What Is Anti-Ransomware:

Why It Matters?

Anti-ransomware solutions differ from traditional cybersecurity in that they are purpose-built to combat encryption-based threats. They use AI/ML models to detect suspicious behavior, offer automated rollback of encrypted files, and enable safe recovery without paying ransoms.

01

AI/ML- Powered Anomaly Detection

02

Immutable Backups and Decryption Tools

03

Data Exfiltration Prevention (DXP)

04

Rapid Incident Response Capabilities

05

Threat Intelligence and Analytics Dashboards

GBS

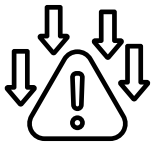
4. The Biggest Problems Caused by Ransomware

With 85% of companies encountering at least one attack annually and many experiencing multiple breaches, ransomware is a persistent crisis.
The key Problems include:

1. **Financial Devastation from Ransomware Attacks**
2. **Operational Disruptions**
3. **Reputational and Trust-Related Fallout**
4. **Possible Lawsuits**
5. **Compliance and Regulatory Pressures**
6. **Strategic and Competitive Impact**
7. **Business Continuity**
8. **Threat of Data Loss and Delayed Data Recovery**
9. **Remediation and Restoration Costs**
10. **Employee Burnout**

5. Operational Impact

Anti-ransomware platforms aren't just IT tools—they drive tangible business outcomes:



Reduce Mean Time to Detect (MTTD) and Respond (MTTR)

Ensure Regulatory Compliance (e.g. UAE Cyber Resilience Act)

Cut Breach Recovery Costs Significantly

Protect Brand Trust and Customer Confidence

According to the Veeam Ransomware Trends Report, 72% of companies saw their backups compromised during attacks. Only resilient, end-to-end protection can ensure continuity

6. Industries at Risk

In the Middle East, rapid digital transformation and increasing connectivity have made businesses more vulnerable than ever. Here's a closer look at the top industries in the region and why anti-ransomware solutions are essential.

Oil and Gas

Finance

Healthcare

Telecommuni-cations

E-Commerce

Management Consulting

Education

EdTech

FinTech

Whether it's oil, finance, healthcare, or education—data is the new oil, and ransomware is the new digital war. Every industry in the Middle East has a unique threat surface, but one shared need: a comprehensive, behavior-focused, multi-layered defense strategy.

7. Attack in Action

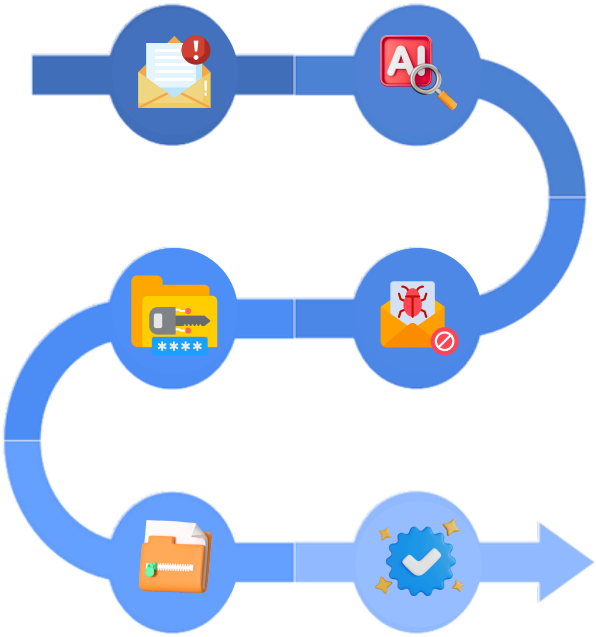
Meet Ahmed — IT Manager at a mid-sized logistics company in the UAE

It's a regular Wednesday. Ahmed's sipping his coffee and scanning through dashboards. Unknown to him...

Step 1

A suspicious email arrives

An **employee receives** a seemingly harmless **invoice PDF**. They **click**. It's **malware** in disguise.



Step 2

Pre-execution AI kicks in

Anti-ransomware **platform recognizes** abnormal **traits** using AI trained on 1M+ ransomware samples. **Blocked**. Instantly quarantined. But let's say it wasn't blocked...

Step 3

Behavioral defense activates

The platform sees encryption behavior — **file access spikes**, abnormal registry changes. Boom — the **malicious process is neutralized** mid-flight. Backups? Still intact. Endpoints? Still safe.

Step 4

Encryption — keys captured

If encryption began before detection, the solution silently **collects the encryption key**. All affected files? Automatically restored. **No ransom needed**

Step 5

Exfiltration attempt spotted

The malware tries to steal customer data. Outbound flow spikes. **Sensitive files begin to move. Blocked by Data Exfiltration** Protection. Nothing leaves.

Step 6

Ahmed gets alert, not a nightmare

He receives a clear dashboard report. **No downtime. No panic.** And he didn't even need to call the boardroom in

Final Outcome: Business continuity. Zero ransom. Full control

Instead of days of downtime, Ahmed's team reviews a blocked threat summary over lunch. They tune policy settings, and get back to work.

8. Anti-Ransomware Beyond Basics

In 2023 alone, Group-IB reported a 68% increase in ransomware incidents across the Middle East and Africa—a signal that business-as-usual cybersecurity is no longer enough.

GBS's anti-ransomware solution is purpose-built to outmaneuver ransomware's ever-evolving tactics. But beyond threat mitigation, these tools now drive tangible improvements in data protection, operational continuity, and IT strategy across regional enterprises.

🔐 1. Enhanced Data Protection.

💪 2. Improved IT Resilience.

🚨 3. Streamlined Incident Response.

👥 4. Enhanced Employee Awareness.

🕒 5. Reduced Operational Downtime.

🧾 6. Regulatory Compliance Made Easier

💸 7. Tangible Cost Savings.

🛠️ 8. Enhanced Disaster Recovery.

🔐 9. Strengthened Network Security.

🧭 10. Smarter Strategic Decision-Making

The ransomware battleground in the Middle East is intensifying—but the right anti-ransomware solution does more than defend. It builds resilience, safeguards data sovereignty, enhances operational readiness, and unlocks strategic clarity for IT leaders.

For organizations aiming to stay secure, compliant, and competitive, investing in purpose-built platforms delivered and curated by GBS—is no longer optional. It's foundational.

8. Anti-Ransomware Beyond Basics

Ransomware has evolved beyond simple encryption. Today, threats range from Ransomware-as-a-Service, insider attacks, and human-operated campaigns, to kernel-level exploits and encryption-less extortion. Organizations across the Middle East face growing complexity—fueled by sector-specific attacks, legal minefields, and even psychological damage to IT teams post-breach.

Our Solutions provides layers of defense—detailing where traditional tools fail and how next-gen anti-ransomware solutions fill those gaps.

- ✅ **Stop ransomware even when AV/EDR fails**
- ✅ **Prevent exfiltration, double/triple extortion**
- ✅ **Strengthen cyber hygiene & Zero Trust implementation**
- ✅ **Safeguard your team's mental resilience**
- ✅ **Navigate cyber insurance & compliance traps**
- ✅ **Defend against vertical-specific ransomware tactics**

With a solution like GBS's Anti-Ransomware, your organization can not only withstand attacks but also recover quickly and emerge stronger.

CONTACT GBS TEAM TODAY

9. GBS: Your Partner in Ransomware Defense

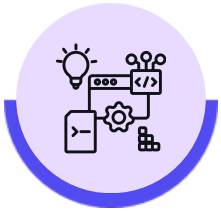
Overview

At GBS, we specialize in delivering curated anti-ransomware strategies for organizations in the Middle East. We align technology, people, and process to help IT teams stay ahead of advanced ransomware threats.

Over the past 19+ years, GBS has established a strong presence as a leading technology solutions provider, delivering successful projects across various industry verticals in the Middle East & Asia. With offices in Saudi Arabia, United Arab Emirates & India we can serve a wide range of industries & provide comprehensive services. Our areas of expertise span across cloud solutions, cyber-security, enterprise networking, enterprise data management, & IT managed services.

At GBS, our team consists of over 100 world-class professionals who are committed to delivering exceptional service. Customer satisfaction is our top priority, & we offer round-the-clock support to our 1000+ customers. So Whether you're modernizing security or building it from the ground up —GBS is your partner in cyber resilience.

Managed SOC with 24/7 Ransomware Monitoring



Integration of Industry-Leading Platforms

Strategic Advisory and Cybersecurity Assessments

Incident Playbooks and Rollback Procedures

Transparent Operations with Timely Reports

Cost & Time Efficient Project Delivery

Tailor Made Solution Designs

Contact Us for Further Inquiries

info@gbsits.com

+971 4529 3916

www.gbsits.com

GBS