Cybersecurity

Ransomware defense: Your strategic blueprint

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

Atos

Phase 1

GOVERN:

Strategic oversight

- Define cyber risk management strategy.
- Establish supply chain risk management.
- Ensure regulatory compliance.

Phase 2

IDENTIFY:

Know your landscape

- Map all IT assets (on-prem & cloud)
- Assess vulnerabilities and attack surface
- Understand supply chain risks
- Develop an incident response & recovery plan
- Run Tabletop Exercises

Phase 3

PROTECT:

Fortify defenses

- Implement strong access controls.
- Segment networks; enforce Zero Trust.
- Maintain air-gapped backups; test recovery.
- Protect endpoints; encrypt sensitive data.
- Train personnel on security awareness.
- Manage vulnerabilities and patching.

Phase 4

DETECT:

Spot threats early

- Collect and analyze security telemetry.
- Monitor for anomalies and malicious activity.
- Utilize threat intelligence.
- Actively hunt for threats.

Phase 5

RESPOND:

Act swiftly

- Execute incident response plan.
- Isolate impacted systems rapidly.
- Gather forensic evidence.
- Coordinate with law enforcement.
- Disrupt attacker activity.

Phase 6

RECOVER:

Restore & rebuild

- Restore operations using clean backups.
- Test disaster recovery plans.
- Prioritize critical data/app recovery.
- Learn from incidents for improvement.

Speak to an Atos cybersecurity expert to build comprehensive ransomware defense.

Learn more >

Atos