SOLUTION BRIEF

Ransomware Security Resilience Solutions

RANSOMWARE ATTACKS OCCUR EVERY 11 SECONDS

News headlines continue to show that cybercrime is on a steady upward trajectory with no signs of slowing. And ransomware is today's most common type of cyber-attack.

Crime Pays

Beyond a direct ransom payment to a criminal actor, business costs are often more significant—including data recovery and infrastructure rebuilding expenses, damage to brand and reputation, and service outages.

Average Costs

- Ransomware: $133K
- Malware cost: $2.6M
- Breach: $8.6M US; $4M Worldwide
- Phishing: $17K/minute

AHEAD's Approach to Ransomware Resiliency

Assess and Develop Strategy

Design a Mitigation Architecture

Plan for Data Recovery

AHEAD examines entire security programs from process to technology and identifies any gaps in your current protection, such as:

- Inadequate phishing and endpoint protection
- Unprotected or overly accessible backup solutions
- Inadequate network segmentation

Negative outcomes still preventable		Attack Successful	Impact Determined
Initial Access	**Attack Propagation**	**Attacker Objectives**	**Recovery**
• Email Phishing Protection • Zero Trust Strategy	• Identity and Access Management Solutions • Zero Trust Strategy	• Endpoint Protection	• Data Recovery Protections

Trust Absolutely No One

Zero-Trust Architectures are strongly recommended to help mitigate common data breaches and ransomware attacks.

Verify Every User & Device

Require secure and authenticated access to all resources

Adopt Least Privileges

Provide only necessary privileges required to complete work

Intelligently Limit Access

Use visibility, analytics, and automation to police policies

Network

Segmentation effectively protects IT systems from ransomware attacks, dividing a larger network into smaller sub-networks with limited inter-connectivity between them.

- Macro/micro segmentation
- Firewall architectures and placement
- Secure Access Service Edge (SASE)

Identity & Access Management (IAM)

A zero-trust IAM overlay across the following areas ensures only the right users have appropriate access to technology resources, such as: application, user, and workplace.

Privileged Accounts Usage

Includes solutions for access and management, account lifecycle management, Single Sign On (SSO) options and multi-factor authentication (MFA)

Business-Focused Cyber-Recovery Defense

GOOD

Data Protection Best Practices

- Protect Data everywhere (on premise, cloud, end-point)
- 3rd copy on Disk or Tape
- Network Segregation, Separation of Duties
- Recovery Drills
- Immutable Snapshots
- Up to date code and firmware
- Access controls in place

BETTER

Immutability (Hardening)

- Product specific hardening guides
- Encryption in flight and/or at rest
- Retention lock with separate security officer credentials
- Two-Person Authentication
- Multi Vendor Support

BEST

Air Gap With Immutable Copies & Analytics

- Network, Management and Physical Isolation
- Control planes
- Isolated immutable copies of backup data and catalog
- Data analytics to validate data and provide quick insight into compromise

Let's Build Your Cybersecurity Strategy Together

AHEAD partners with you to set a strategy and translate it into an executable process and plan that works to reduce manual workload and drive efficiency. AHEAD validates all outcomes to ensure the desired results are confirmed. Our holistic approach means applying automation, analytics, and agile thinking across the full security lifecycle.

IDENTIFICATION

AHEAD will help implement a robust vulnerability management program, giving you the insights you need to prioritize risks across your environment.

PROTECTION

AHEAD will put an in-depth strategy in place to protect your organization from attacks, for example, using network micro segmentation to reduce your attack surface.

DETECTION

AHEAD will tap the insight and power of your log data across all systems, as well as network and privileged user monitoring, to detect anomalies and respond faster.

RESPONSE

AHEAD will lean on its deep roots in automation and enterprise service management, to quickly prioritize threats and automate the response to frequent and common security events.

RECOVERY

AHEAD will leverage its heritage of robust backup solutions to ensure minimal disruption to your business and protect your data in the public or private cloud.

AHEAD

Learn. Grow. Achieve

Learn more at
www.ahead.com