AEGIS Cybersecurity Strategy

Continuous investments to keep your data safe.

All AEGIS applications and client data reside entirely within Amazon's secure AWS environment. This is a SOC-1, SOC-2 and SOC-3 certified operation.

All client data is encrypted at rest.

Web Application Firewalls (WAFs) are deployed to prevent common attacks before they occur.

Award-winning endpoint protection installed to sniff out more advanced exploits and attacks.

External penetration tests add an additional level of monitoring and early detection of potential exposures.

Internet

Encrypting data in transit

- All data traveling through the Internet to AEGIS applications is encrypted using 256-bit SSL/TLS encryption

User

Ensuring the right people access the right data

- Authentication performed using a Gartner Magic Quadrant Leader in authentication leveraging best-in-class compliance frameworks
- Multi-factor authentication (MFA) option available
- Unified access controls allow organizational admins to clearly define user access to data and reports
- Secure authorization and session management ensure that users can move freely within the AEGIS ecosystem while the bad guys stay out

Company

Partnering with global leaders in cyber security

- AEGIS outsources an award-winning security operations center (SOC) which is powered by a Gartner Magic Quadrant Leader for Security Information and Event Management (SIEM)
- All company devices are protected against attacks by a Gartner Magic Quadrant Leader for Endpoint Protection Platforms
- The AEGIS network infrastructure is shielded by a Gartner Magic Quadrant Leader in Next Generation Network Firewalls
- All employees undergo classes in phishing, ransomware and other attacks using a Gartner Magic Quadrant Leader for Security Awareness Training
- Employee communications are scanned for threats using native email security tools
- Client data is downloaded only on encrypted devices which are segmented and managed using both on-prem and cloud-based directory services
- Our operations are audited regularly to maintain SOC-1 compliance
- Weekly vulnerability scans add an additional layer of protection

We believe we have the strongest cybersecurity posture in our industry. But we are also realistic. Making systems impenetrable is simply not possible as threats evolve over time. Our cybersecurity investments are made to deter and discourage bad actors. We do this by leveraging leading technologies, detecting attacks 24×7 and responding quickly so that important information is never accessed. We have a responsibility to make our systems difficult to penetrate - but the goal is deterrence so that we can provide uninterrupted service to our customers. You should expect the same of any partner you choose.

AEGIS
HEDGING