DATA GUARD
BY ACTIVE CYPHER

The Cyber Security Industry Vision Is Out of Focus

About $93 billion was spent for network security in 2019 and the estimated cost of ransomware attacks in that same year was $1.5 trillion. These breaches cost about 40% more than what we spend to protect our information. Despite the amount of time and money we commit to securing our network perimeters and monitoring hybrid networks hackers still get in. The industry has continued to build systems that let us watch looters run out the doors with our most valuable assets.

New Privacy Regulations, Hefty Penalties, and Effective Solutions

New regulations have been written in the EU and the US that assign liability for data privacy breaches to the holder of that information. GDPR calls for damages suffered but California's CCPA is far more specific. It calls for $100 - $750 per violation, which translates to per record compromised. This makes a 300 million record breach a very costly event. Between regulatory compliance fines and ransom costs for regaining access to your own business data, the cost of cyber security becomes trivial.

The Real Goal of Cyber Security is to Ensure Data Remains Safe

Active Cypher's **Data Guard** turns the industry approach on its head by focusing on the ultimate goal of cyber protection, securing your data without burdening your users.

Treat the disease rather than the symptom

Security Spend vs Loss 2019

Global spend for cyber security:

$92.7 Billion

- Security Services - $64.2 b
- Infrastructure Protection - $15.3 b
- Network Security Equipment - $13.2 b

Global cost of data breaches:

$2.1 Trillion

- Ransomware extortion cost - $1.5 trillion
- Ransomware recovery costs - $5 billion
- Average cost of cybercrime for an organization - $13 million

Cost of cybercrime tools and kits:
$1 - $500

Active Cypher's **Data Guard** protects your files from unauthorized access and ensures that people have free use of the information they need without adding extra burdens on their workflow.

Data Guard Personal ensures document privacy and complete control over who has access and what they can do. Secure File Share allows you to track and protect your files even after they are emailed. It records when files are opened, how much time is spent on each page, and shows the geolocation of every file. You control whether the documents are read only, printable, or editable and you can limit the duration of access, regardless of where you sent it, and can be revoked at any time.

Data Guard's Advanced version provides all of these features and cloaks your files from ransomware or malware. As added protection, **Data Guard Advanced** provides real-time cloud backup with 1-click recovery for complete protection. **File Fortress,** the **enterprise** platform, provides optional 256-bit AES or quantum-resistant encryption of all files across the network, whether they're on your employee's laptop, on fileservers, or in the cloud.

Cybercriminals may gain access to your network, but will never touch your data

94% of malware is delivered via email and phishing attacks account for more than 80% of security incidents. Criminals might gain a presence on a computer, but they won't see the data on that device or any other with **Data Guard's** proprietary file cloaking. Active Cypher leverages 256-bit AES encryption to ensure data safety now and has developed a proprietary crypto-agile infrastructure that accommodates rapid conversion to any future encryption standard.

Criminals get through firewalls and continue to go unobserved

Cybercriminals may gain access to your network, but they can't access your data thanks to Active Cypher's **Data Guard**. It's now cheap for cybercriminals to get inside the firewall but we can now protect the data itself regardless of the direction of attack. CIOs, CISOs and other I.T. professionals can sleep better at night knowing that their data are secure, regardless of the point of entry.