ACTIVE CYPHER™

Microsoft Security

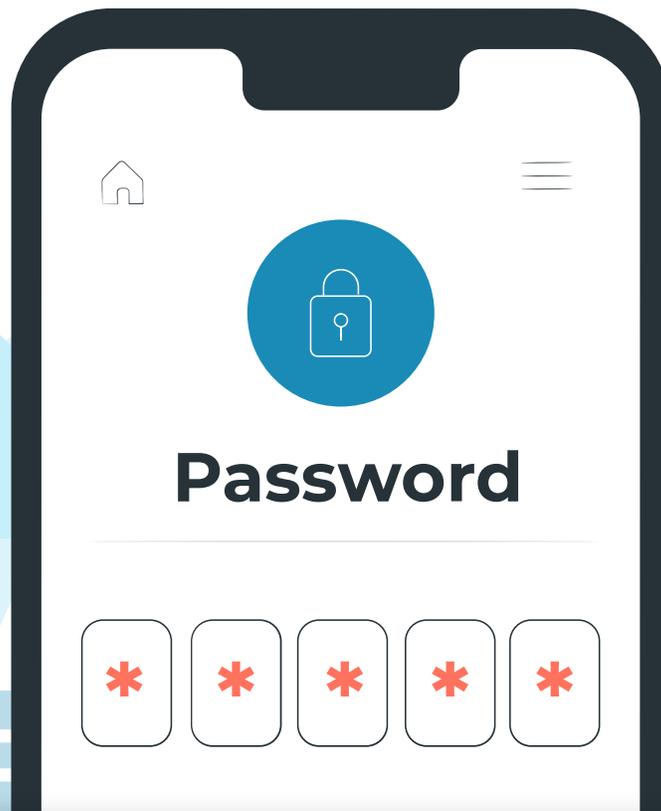# Secure your data supply chain

Provide user and device-based data security across your entire organization with Active Cypher and Azure AD.

Password

Is your cloud adoption outpacing your security upgrades?

Protect your most valuable assets against ransomware and other cyberthreats

In today's increasingly data-driven world, the looming threat of security breaches and ransomware attacks remain a constant concern. And as more organizations move their critical information to the cloud, the need for a comprehensive and reliable security solution to defend against threats grows.

- By 2025, the world will store 200 zettabytes of data, including data stored on private and public cloud datacenters and on personal computing devices.[1]
- Last year, ransomware made up nearly a quarter of the incident-response engagements for IBM Security's X-Force threat intelligence group, with 59% of the ransomware incidents involving double-extortion attacks.[2]
- Attacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation.[3]

Contents

Discover a proactive security solution for comprehensive data protection

Leveraging deep integration with Azure Active Directory, Cloud Fortress by Active Cypher offers companies a comprehensive data security product that helps protect against insider mistakes and cyberthreats like ransomware.

Enable end-to-end encryption

Provide user and device-based security for data across your entire organization.

Learn More

Secure a chain of data custody

Maintain custody of data to ensure admissibility and evidence integrity.

Learn More

Optimize data protection

Leverage best practices defined by Microsoft's compliance and security.

Learn More

Enable end-to-end encryption

Stop malware and ransomware in its tracks and protect your most critical data

Cloud Fortress user-based protection encrypts all files across your hybrid network and leverages Active Directory to provide access privileges to users in need of critical resources. The Active Cypher solution integrates with Microsoft Azure cloud services seamlessly to support continued use of your organization's productivity tools, such as Microsoft Office 365, while also aligning your IT systems with Microsoft's security and compliance best practices.
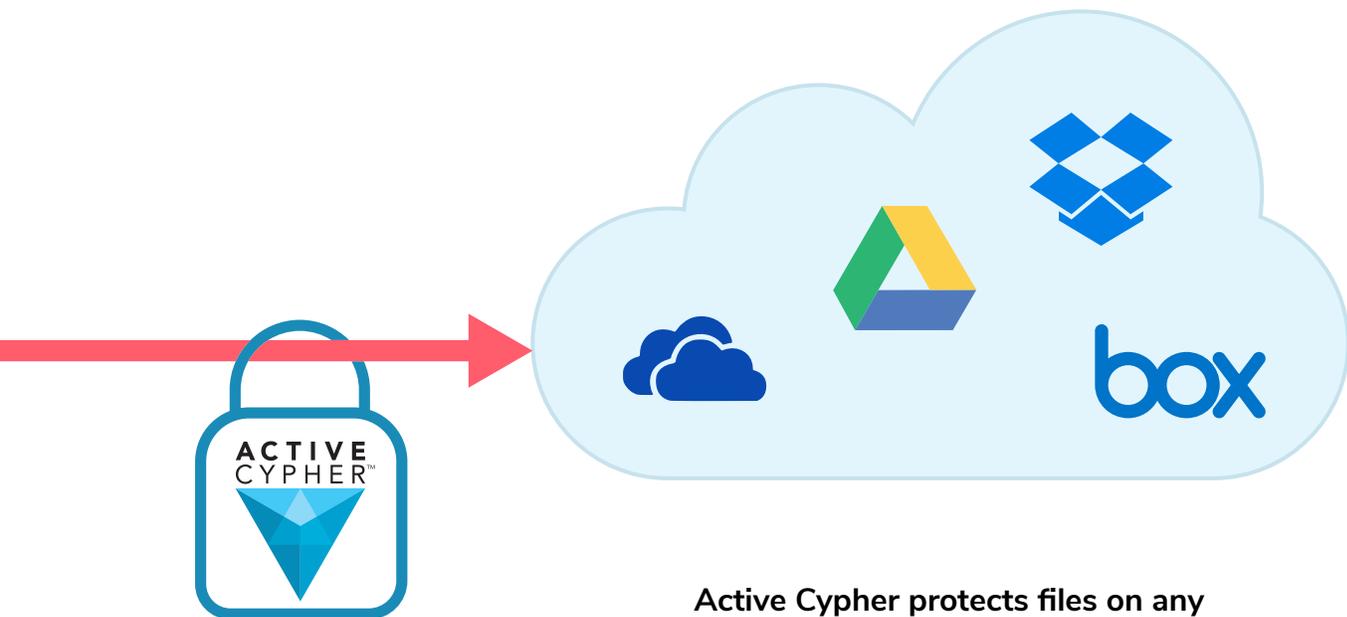
Our solution builds your security posture around the protection of your data. This revolutionary approach departs from the traditional industry focus of secure network perimeters. Rather, Active Cypher's end-to-end approach stops ransomware and malware from accessing and exfiltrating data before it's too late.

Built on Azure

Active Cypher leverages and greatly expands the strong security architecture of Microsoft Azure. All products in Active Cypher's portfolio are data-centric, policy-driven, and can be seamlessly integrated into alternative cloud solution architectures.

Azure Storage

Office 365

Azure Active Directory

Azure

Azure Virtual Desktop

Azure Key Vault

Windows Active Directory

ACTIVE CYPHER™

Privileged Access
Secured Network Resources

Active Cypher protects files on any device and anywhere they're stored.
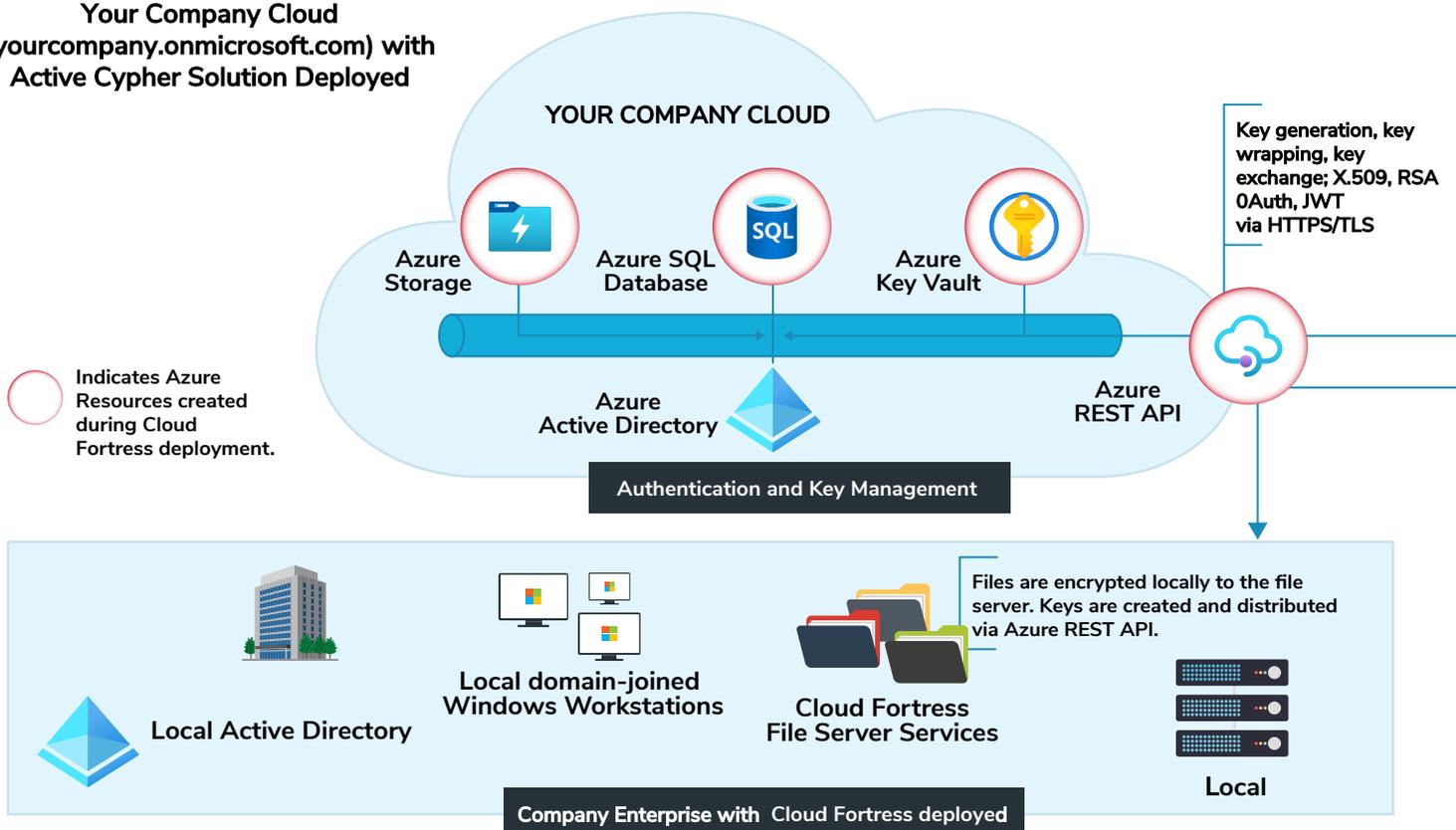
Secure a chain of data custody

Safely share and collaborate on files externally while mitigating ransomware attacks
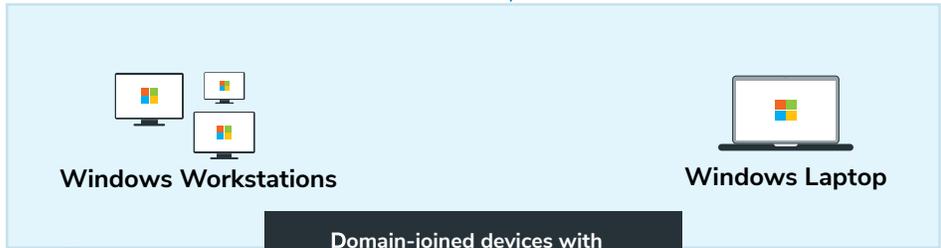
The Active Cypher Cloud Fortress device-based element, Data Guard, works against malware and ransomware while also providing control over how files are used when they are sent outside of your organization's control. Clients using Data Guard are able to fulfill chain of custody requirements with complete transparency and auditability of file activity. AI-powered sensors capture and log events such as who accessed a file, at what time, and whether a file was modified, downloaded, and/or shared.

Block ransomware and other cyber-threats from locking away company data and demanding a hefty payment. Active Cypher makes sure your files are hidden from ransomware and proactively fights threats at every stage of the attack chain.

Your Company Cloud (yourcompany.onmicrosoft.com) with Active Cypher Solution Deployed

YOUR COMPANY CLOUD

Azure Storage

Azure SQL Database

Azure Key Vault

Key generation, key wrapping, key exchange; X.509, RSA 0Auth, JWT via HTTPS/TLS

Indicates Azure Resources created during Cloud Fortress deployment.

Azure Active Directory

Azure REST API

Authentication and Key Management

Local Active Directory

Local domain-joined Windows Workstations

Cloud Fortress File Server Services

Files are encrypted locally to the file server. Keys are created and distributed via Azure REST API.

Local

Company Enterprise with Cloud Fortress deployed

Windows Workstations

Local corp. domain

Windows Workstations

Windows Laptop

Domain-joined devices with
Cloud Fortress Thin Agent deployed.

Active Cypher Thin Agent (MSI) deployed to all Users
via GPO/SCCM

Optimize data protection

Address security obstacles and align to Microsoft compliance and security best practices

Active Cypher Scout is a combination of tools that work together as a single application to check your enterprise IT configuration and help you adjust it to optimize data protection. Once the corporate IT configuration is verified, Active Cypher Scout

displays a report with its findings. Based on the results of the report, the Active Cypher team can work with you to solve any remaining obstacles to the successful protection of your data.

What's included in Active Cypher Scout?

Scouting Manager

Scouting Manager is the Azure-tenant component that collects data from the agents running on your local server. Scouting Manager performs a cybersecurity analysis and correlates this data to produce meaningful recommendations and create actionable reports.

Scouting Reports

Scouting Reports provide remediation, recommendations, and categorical reporting.

Scouting Agents

Scouting Agents are downloadable executables (.NET) that are deployed to each file server and domain collecting system data, forwarding it to Scouting Manager.
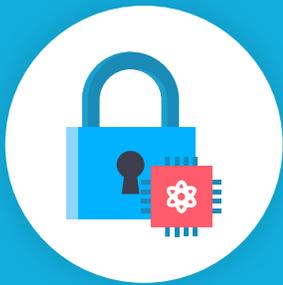
Healthcare – Data protection on any platform

The medical industry handles a wealth of extremely sensitive patient information. A data-centric security strategy improves their ability to share information in cloud collaboration platforms, while protecting against data breaches and adhering to regulatory compliance.

Local hospital uses Active Cypher to secure data in cloud collaboration tools

Data protection on any platform:

- Provides flexible data security for remote and mobile workforce.
- Protects files being accessed and shared on mobile and personal devices.
- Secures data sharing in the cloud using the Active Cypher solution.
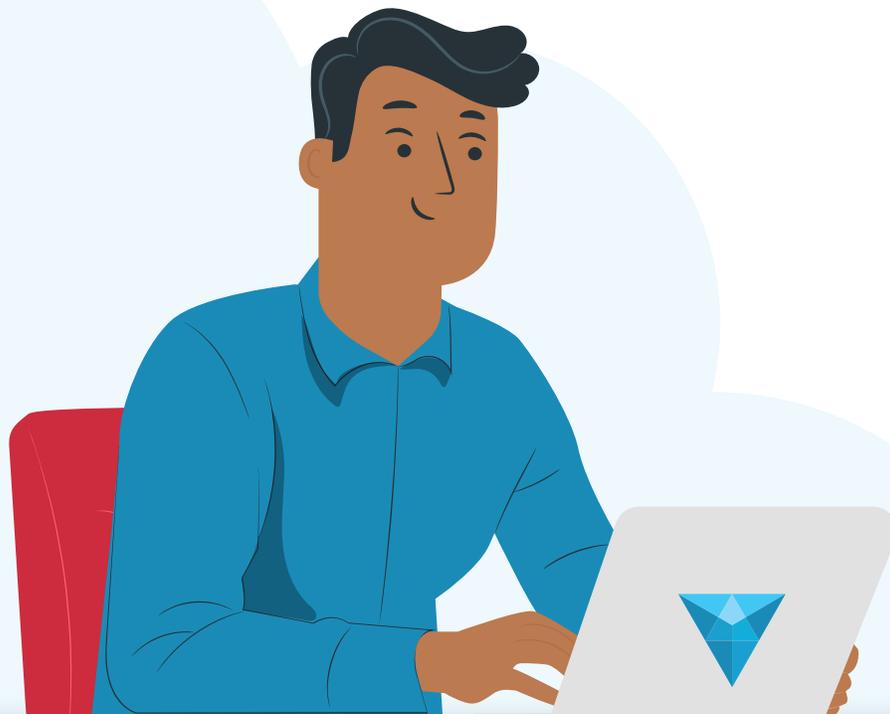
Introduction

A local hospital that recently experienced a ransomware incident turned to Active Cypher to secure their infrastructure and keep patient data private. The hospital's information security team required a data security solution that could scale across a complex ecosystem of internal departments and external stakeholders. The hospital's data is extremely sensitive, containing personally identifiable information (PII) and protected health information (PHI), which is actively targeted by hackers and subject to strict regulations. The hospital uses cloud collaboration tools to share information, and it needed a solution that ensured the highest levels of security and encryption to prevent data breaches and comply with regulatory compliance.

Active Cypher was chosen because it gave the hospital the ability to secure any type of data across multiple environments, while integrating easily with existing security technologies. The information security team could secure critical hospital and patient data through the Active Cypher platform, without slowing information sharing and collaboration workflows.

Supporting diverse technology investments

Medical institutions are experiencing a significant increase in the volume of sensitive data they collect through connected devices, driving increased use of storage, collaboration, and communication tools to meet evolving hospital demands. The challenge lies in protecting this growing volume of data without making the security systems too complex to be managed effectively.

Active Cypher works across multiple platforms, integrating with existing security solutions to help businesses maximize their existing investments.

Active Cypher delivers superior data security

- AES (Advanced Encryption Standard) 256 FIPS 140-2 encryption to protect PII and PHI
- Integrations with modern cloud collaboration applications, such as Box, OneDrive, and SharePoint
- Non-invasive thin-agent devices manage policy enforcement behind the scenes

In summary: Secure cloud collaboration

The hospital was using OneDrive to share information with external stakeholders, and it deployed Active Cypher to secure the files and data contained with that collaboration solution. This enabled the hospital to automatically secure any file with strong encryption and set policies to control access to those files. This expanded to other applications, such as SharePoint and Google Drive, offering the hospital multiple options for secure collaboration and content management. The Active Cypher solution continues to work easily with the hospital's existing security stack without interference.

Results

Using Active Cypher's solution, the hospital achieved major improvements in their processes, protecting consumer PII and PHI as it moved between internal and external teams. This data is subject to a range of regulatory compliance from state, national, and international mandates, and Active Cypher's proprietary encryption and auditing capabilities support the hospital's compliance efforts. With Active Cypher, the hospital embraces the convenience and cost efficiencies of popular cloud collaboration platforms without exposing it to the risks associated with sharing data beyond the hospital's perimeter. This, in turn, helps with employee productivity and the speed of data sharing across the institution.

# A comprehensive security solution you can trust

In an increasingly complex digital age, Active Cypher provides reliable user and device-based data protection across your entire organization to ensure your critical assets are protected against even the most sophisticated attacks.

[1] Top 5 Cybersecurity Trends 2021
[2] Ransomware, Phishing Will Remain Primary Risks in 2021
[3] 2020 World Economic Forum's Global Risk Report
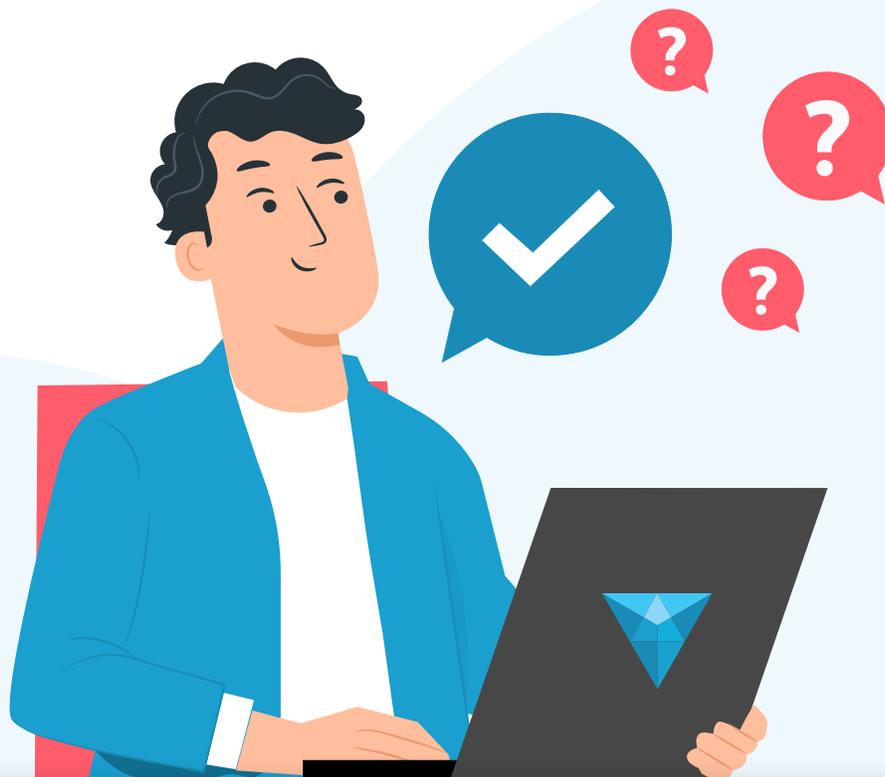
Ready to learn more?

Contact us:

Email | sales@activecypher.com

Phone | 1 (714) 477-1045

Website | ActiveCypher.com