ACTIVE™ CYPHER

MSSP USE CASE

How a National Managed Security Service Provider Removed Human Error From Customer Communications and Protected Their Business From Data Loss

ACTIVE CYPHER™

Simplifying Data Protection

Managed Security Service Providers Can Use Active Cypher to Secure Data in Cloud Collaboration Tools

MSSP Use Case

Managed Security Service Providers (MSSP) are extensions of their customers' I.T. departments. They are trusted to manage the safety and integrity of an organization's most sensitive information, such as strategic plans, financial reports, sales plans, customer information, and more.

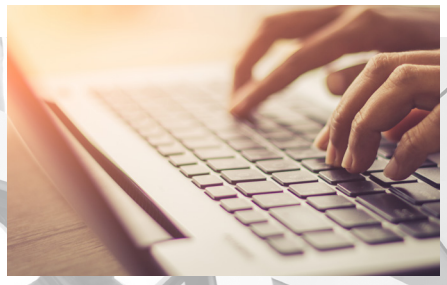
The trusted nature of MSSP's work makes them targets of cybercrime because they hold the keys to many customers' digital assets. As a result, they must continue to stay at the forefront of protection to maintain the integrity of their business.

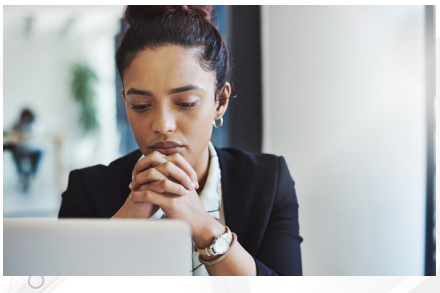
MSSPs struggle with the familiar business problems:

- Competitors trying to gain intelligence
- Random and targeted cybercrime
- Human errors
- Disgruntled employees

The difference for MSSPs is that, if they are compromised, so are their customers. which could be hundreds of businesses.

- Cyberattacks against Managed Service Providers, including MSSPs, jumped 67% in 2022.
- 90% of MSPs have been hit by a successful cyberattack since the COVID pandemic began.
- MSSP monitoring and security management tools are the primary targets of cybercriminals.
- By 2025, 60% of all organizations will use cybersecurity risk as primary factor in conducting third-party transactions





Challenges

The Chief Information Security Officer was concerned that his MSSP Security Operations Center (SOC) was introducing too much risk to their customers when they emailed monthly reports about security operations, architecture vulnerabilities, and incidents.

Their standard practice was that SOC Security Analysts emailed monthly reports to customers with sensitive information about their environments. They were concerned that email was not secure enough for this information. Security Analysts had also accidentally sent reports to the wrong customer on occasion.

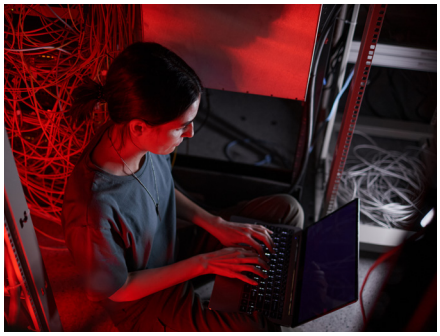
The MSSP had employees quit the company after they downloaded strategic plans for product infrastructure, business roadmaps, existing architectures, and customer information to their personal machines. Unfortunately, the MSSP had no way to stop this illegal and inappropriate breach.

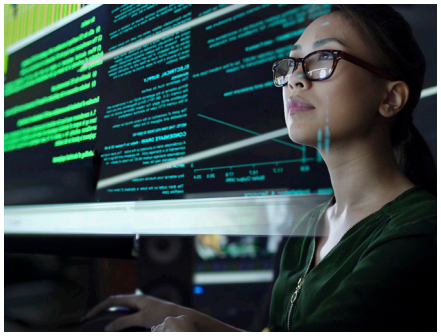
Most Data Protection solutions require trusted third-party custodianship of data, encryption keys, or both. Unfortunately, the MSSP has lost confidence in trusted third-party environments and needs complete control over its security environment.

Results

The MSSP implemented Active Cypher's Cypher Cloud solution to secure external data sharing with customers and for internal data protection. Cypher Cloud is wholly contained in its environment and requires no third-party influence on the data or encryption keys. All files are dynamically encrypted based on business policy and do not change the security analysts' workflow. Azure Active Directory privileges control access using known and available tools.

Monthly security reports are now shared with customers in secure SharePoint enclaves and leverage Active Cypher's unique protection to share files with users outside their organization while requiring user validation. As a result, the information is protected from human error or theft throughout the data supply chain.





4299 MacArthur Blvd
STE 104 Newport Beach CA 92666
(714) 477-1045

Highlights

Difficulties

- Securely sharing confidential information with external customers
- Employees taking intellectual property and leaving the company
- MSSPs are targeted because of their customers' information and access
- Crisis of trust with third-party providers

Solutions

- Protect data at the asset level
- Secure information dynamically
- Safely share information
- Able to revoke access remotely
- Ensures security entirely within customer environment

Results

- Reduced human error
- No trusted third-party relationship
- Reduced administrative burden

Microsoft Azure MARKETPLACE

Member of Microsoft Intelligent Security Association
Microsoft

Microsoft Silver Partner