CloudFirst
Flagship Solutions

# Threats, Vulnerabilities, and Solutions

## How CloudFirst Protects Your Business and Your Data

# TODAY'S BUSINESSES ARE UNDER CONSTANT THREAT OF CYBER ATTACKS

Today's businesses are under constant threat of cyber attacks. The famous last words "It could never happen to us" are famous for a reason. An organization that doesn't prioritize cybersecurity paints a target on its back.

The first step to protecting your company is understanding what you're up against.

That's why we've broken it down, threat by threat. This guide brings you up to speed on the top three threats—the bad actors and malicious programs—that are after your data and IT systems. We'll show you how they exploit vulnerabilities in their victims' defenses to steal sensitive information, extort money, destroy property, and more.

The good news is that you can protect yourself. CloudFirst has solutions that combine state-of-the-art cybersecurity technologies with around-the-clock professional defense teams to stop threats in their tracks. ezSecurity focuses on IBM i Systems, and ezProtect is designed to protect multiple platforms, including end-user devices.

Don't leave it up to chance. Implement CloudFirst's premier solutions and rest assured that your data and IT systems are safe and secure.

## THREAT 1: RANSOMWARE & MALWARE

Companies paid over $1.1B in ransom in 2023.1 This trend is only accelerating. Once ransomware infects a system, it encrypts everything, rendering your files a jumbled mess. Only by paying the ransom do you get the key to de-encrypt it. And ransomware is only one type of malicious program that threatens your business. Anything from spyware to remote access takeover can wreak havoc.

## THREAT 2: INSIDER THREATS

Whether through user error or willful misconduct, insiders can inflict massive damage. This is especially true for users with administrator or superuser privileges.

## THREAT 3: SOCIAL ENGINEERING

Click this link. Download this attachment. Enter your username and password here. I'm wearing a reflective vest and hard hat, so let me into your data center. What all of these have in common is that they're deceptive techniques hackers use to trick people into helping them.

THREAT 1

# RANSOMWARE & MALWARE

## Vulnerability

**Network**
An unprotected network is the equivalent of an airport with no security. You need to lock it down and monitor movement across it.

**ezProtect Patch Management**
With automated patch management, never worry about forgetting an update again. The ezProtect Patch Management solution proactively monitors and manages operating system and application level patches.

**ezProtect Device Hardening**
Measures include managing antivirus software, using CIS Benchmarks[3] or other standards for system configuration guidance, and putting a monitoring system in place to measure the compliance of those systems.

## Solution

**ezProtect Security Information and Event Management (SIEM)**
By collecting and aggregating network logs, SIEM provides constant surveillance for your network. It combines AI pattern recognition with realtime reporting to scan network traffic, flag anomalies, and detect suspicious behaviors. That means we can recognize and stop malicious code before it takes hold. CloudFirst partners with IBM's QRadar, Splunk, and others for SIEM, allowing flexibility in meeting your needs.

**ezProtect Managed Firewall**
Block malicious IP addresses. Configure changes to stop threats in their tracks. Implement an intrusion prevention system (IPS). Especially when combined with a SIEM, managed firewalls block bad traffic at the source, preventing ransomware and other attacks from infecting your network.

**ezSecurity Exit Point Monitoring**
This security gate is standard in ezSecurity. Everything that goes in or out has to pass through it. Keep a close eye on IBM i Systems exit points to prevent unwanted intruders from getting access to critical business data.

**ezProtect Patch Management**
With automated patch management, never worry about forgetting an update again. The ezProtect Patch Management solution proactively monitors and manages operating system and application level patches.

**ezHost to Escape End of Life (EOL)**
Every technology eventually reaches EOL, meaning the vendor no longer updates it. CloudFirst decommissions all EOL tech to close these vulnerabilities with lifecycle management built in to ezHost and all other cloud solutions we offer.

**ezProtect Device Hardening**
Measures include managing antivirus software, using CIS Benchmarks[3] or other standards for system configuration guidance, and putting a monitoring system in place to measure the compliance of those systems.

**ezProtect Security Operations Center (SOC)**
Measures include managing antivirus software, using CIS Benchmarks[3] or other standards for system configuration guidance, and putting a monitoring system in place to measure the compliance of those systems.

This SOC capability is bundled with ezProtect Endpoint Security, giving you complete antivirus, antimalware, and SOC with Managed Detection and Response (MDR). Monitor and respond to threats across endpoints in real time with ezProtect Managed Security Services (MSS).

THREAT 2

# INSIDER THREATS

## Vulnerability

### Escalated Privileges
Prevent users from accessing information they shouldn't and stop them from running commands above their level of trust.

### Stolen Credentials
Getting ahold of another user's login information is a common exploit for all hackers. Insiders are particularly dangerous in this regard.

### Corrupted or Lost Data
If a "disgruntled IT admin" takes the nuclear option and wipes the databases, what happens next?

## Solution

### ezProtect Security Information and Event Management (SIEM)
Control who has access to what, how they access it, and how the system makes sure they are who they say they are.

### ezProtect Managed Firewall
Users should only be able to access data and perform actions necessary for their jobs.

### SezProtect and ezSecurity Multi-Factor Authentication (MFA)
ezSecurity includes MFA by default in its Ransomware Defense and Access Control (RDAC) or higher packages for high-privilege users and shared network drive access, making it impossible for one user to impersonate another through stolen credentials alone.

### ezRecovery/ezAvailability Disaster Recovery and Business Continuity Planning (DR/BCP)
When a crisis strikes, you need a plan. Restoring lost data from offsite backups is often the only way to recover from a severe attack.

### ezVault Automated Backups on the Cloud
ezVault automatically backs up and encrypts all your data to our secure cloud and includes a second immutable copy at another location for ultimate data protection. Then you can quickly restore that data to the original system, an alternate system, or standby ezRecovery systems in the cloud.

THREAT 3

# SOCIAL ENGINEERING

## Vulnerability

### Email Phishing

If you've ever gotten a fake email pretending to be your bank or the IRS, you've seen phishing. When phishing is highly targeted to individuals, it's called spear phishing. This makes it more difficult to spot.

### Users

There's an old adage in cybersecurity that users are the weakest link. Without proper training and controls, unaware users pose a major vulnerability.

## Solution

### Email Filtering and Gateway Protection

ezProtect prevents most phishing emails from ever hitting your employee's inboxes. It also blocks malware and spam.

### Cloud Email Backup for Evidence Trail

In addition to filtering out spam and phishing attempts, CloudFirst's email archiving with email backup provides a full audit trail and method for recovery in case something does go wrong.

### Digital Hygiene Training

Regular training sessions should cover safe web browsing, responsible downloading, and password management.

### Multi-Factor Authentication (MFA)

If a user does accidentally let their password slip, MFA can save the day. CloudFirst's ezProtect solution includes MFA by default.

### Policies

Policies for responsible computer use should include provisions for installing software, changing default passwords, and reporting incidents.

### Managed Detection and Response (MDR)

If all else fails, MDR can see and stop incidents before they get out of hand with 24-7 monitoring and realtime response.

THE COMPLETE SOLUTION

# DEFENSE IN DEPTH

## ezProtect

The best protection against cyber attacks is defense in depth. This cybersecurity strategy involves layering defenses on top of each other.

That way, even if one defense falls, another can protect you. The ezProtect solution itself uses a defense-in-depth approach. Then, by combining ezProtect, ezSecurity, ezAvailability, ezRecovery, and ezVault into a single holistic solution, you can safeguard your valuable data and IT systems.

Don’t leave cybersecurity to chance. CloudFirst’s comprehensive solutions will protect you from today’s biggest cyber threats.

### ezSecurity

Securtiy-as-a-Service

### ezAvailability

High-Availability-as-a-Service

### ezRecovery

Disaster-Recovery-as-a-Service

### ezVault

Backup-as-a-Service


631.608.1200

www.cloudfirst.host

AIX IBMi Linux Windows