AI EDGE LABS

RETAIL IOT CYBER SECURITY

Retail IoT Devices Under Attack

GPS Tracker

Video surveillance

RFID Tag

Barcode reader

Cyber Threats at a Glance

44% Retail organizations were hit by a ransomware attack in 2020

54% Cyber criminals were successful in encrypting data

32% Retailers paid ransom

An average ransom bill for rectifying a ransomware attack **$1.97M**

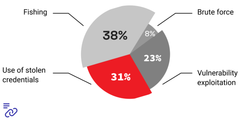
Top Attack Types:

Credential harvesting	30.43%
Malware	22%
Ransomware	13%
DDoS	10%

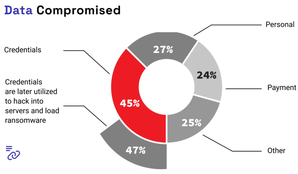
Top Breach Patterns:

- System Intrusion
- Basic Web
- Social Engineering
- Application Attacks

Top Attack Vectors:



Data Compromised



Actor Motives:

- Financial (98%)
- Espionage (2%)

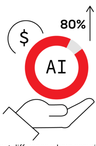
Threat Actors:

- External (87%)
- Internal (13%)

Why AI Security Matters

78%

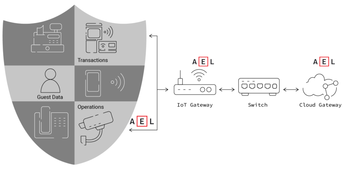
Retailers cite concerns about data privacy and security regulations in their annual financial performance reports.

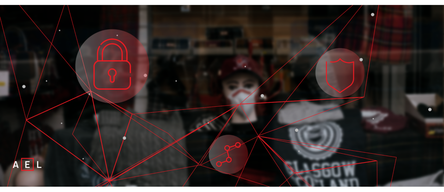


Cost difference where security AI and automation was fully deployed vs. not deployed

Average Cost of a Data Breach **$3.27M**

Retail AI-driven Network Security





AI EdgeLabs is an AI-powered platform that brings advanced network visibility, early threat detection, automated incident response and remediation vital for the newest technologies for the retail and any industry. Edge Labs Threat Intelligence ensures:

- Threat detection for IoT Equipment in the store.
- Hidden and unknown threat and abnormal activity detection.
- Smart firewalling with automated response.
- Assets management inside the retail ecosystem.
- Mitigation actions for incidents

PROTECT YOUR EDGE & IOT ENVIRONMENT

AI EDGE LABS