deepwatch

Three Key Steps to

Reducing Ransomware

Ransomware is a global scourge damaging businesses of all types and sizes around the globe. The dramatic impact from attacks can be felt in everything from energy and food supplies to health services and education. Organizations need to quickly advance their security profile using three key steps to ensure they are prepared to prevent and remediate attacks.

$4.35 Million

AVERAGE COST OF A DATA BREACH REACHED AN ALL-TIME HIGH LAST YEAR, USD 4.35 MILLION.

This figure represents a 2.6% increase from the previous report, when **the average cost of a breach was USD 4.24 million**. The average cost has climbed 12.7% since the 2020 report.

-IBM Cost of a Data Breach 2022

In April 2022, **THE FIRST NATIONAL EMERGENCY DUE TO A RANSOMWARE ATTACK** was declared in Costa Rica. It shut down many government functions for five days.

-Bleeping Computer

In their 2022 Global Threat Report, Crowdstrike identified an **82% INCREASE IN RANSOMWARE-RELATED DATA LEAKS IN 2021.**

-Crowdstrike Global Threat Report 2022

According to the FBI, **A CYBERCRIME WAS REPORTED EVERY 37 SECONDS IN 2021,** with ransomware losses from reported incidents reaching $50 million in the US.

-FBI IC3 2021

RANSOMWARE-AS-A-SERVICE PROVIDERS MAKE ATTACKS EASIER, spreading the work and risk by renting or selling their tools for a portion of the profits. There is a continuously evolving, connected ecosystem of ransomware attacker

-Microsoft Security

+13%

Increase in ransomware attacks 2021

-IBM Cost of a Data Breach 2022

40 Billion

Records were exposed due to breaches in 2021

-Tenable 2021 Threat Landscape Retrospective

+34%

Increased Cyber insurance premiums in Q4 2021 alone

-Fitch Ratings

Remediate Ransomware with

Three Key Strategies

Prevention Strategies

Stop ransomware from establishing a foothold.

- Data Governance & Backups
- Training & Assessments
- Identity & Access Management Methods
- Vulnerability Management

Detection Strategies

If ransomware gets in, detect the threat fast.

- Endpoint Detection and Response
- Threat Hunting
- Log Collection & SIEM Monitoring
- Machine Learning & Artificial Intelligence

Response Strategies

If ransomware or anomalous data is found, rapidly respond.

- Incident Response
- Attack Planning & Tabletop Exercises
- Response Technologies & Services
- Remediation

Managed Detection and Response (MDR) Can Help Implement These Three Key Strategies

With MDR, organizations can gain greater visibility into the detection and response process; augment in-house staff with security experts; expand existing solution capabilities to maximize ROI; integrate seamlessly with a SEIM; and optimize security investments.

Download **Minimizing the Impact of Ransomware with Managed Detection and Response** to learn more.

deepwatch

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

CONTACT US

sales@deepwatch.com
4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
855.303.3033
www.deepwatch.com