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.

Ransomware Realities

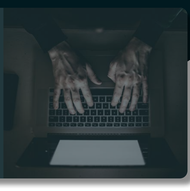
There are **significant ransomware risks** with vulnerabilities, misconfigurations, and open-source and third-party code.

Vulnerabilities account for 42% of the most common attack vectors according to a 2020 Forrester Research study.

Open-source and third-party code can be flawed and is sometimes intentionally tainted with malicious code.

Misconfigurations accounted for 65% of publicly disclosed cloud security incidents according to Palo Alto Networks.

Most threats today originate with highly trained, experienced, and **sophisticated threat actors**, often operating with the support of nation states or skilled crime gangs.



Recent Dramatic Increase in **Ransomware Attacks**

93%
increase in first six months of 2021

148%
increase between 2019 and 2020

$1.16M
average cost per ransomware attack according to the DBIR.

There is no single solution that stops **ransomware.**

Remediate Ransomware with **Three Key Components**

Prevention Strategies

Stop ransomware from establishing a foothold.

- Data Governance & Backups
- Training & Assessments
- Email Security & Other Technologies
- Identity and Access Management Methods
- Vulnerability Management

Detection Strategies

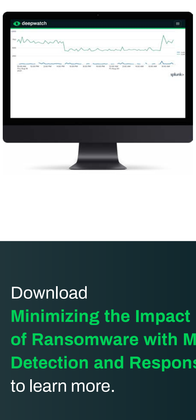
If ransomware gets in, detect the threat fast.

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

Response Strategies

If ransomware or anomalous data is found, rapidly respond.

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



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

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.