

# End-to-End Protection Against Ransomware

## Prevention, Detection, and Recovery Designed for Mission-Critical Applications

Ransomware and cyber threats compromise organizations through a growing number of avenues, inflicting a wide range of damage. One of the biggest drivers behind the rise is ransomware as a service (RaaS). RaaS allows developers to sell their services using subscription models for plug-and-play ransomware. Cyberattacks are big business with evolving ways to capitalize on the crime. Enterprises need an end-to-end strategy to protect their mission-critical applications and prevent, detect, and recover from attacks.

The first half of 2022 saw a **2X growth of ransomware variants.**

[Fortinet Global Landscape Report, 1H 2022](#)

## Protecting What Matters Most

Zerto, a Hewlett Packard Enterprise company, and Fortinet are collaborating to deliver increased value to enterprises. We know acquiring technology is only the first step in achieving a business goal. The technology pieces need to work together and supply rich functionality quickly and effectively, so you can concentrate on your business needs.

With a focus on mission-critical applications that cannot tolerate disruption or downtime, Zerto and Fortinet provide best-of-breed prevention and recovery from any cyber threat or ransomware attack across virtual and cloud environments.

## Together we help businesses



### Proactively Reduce Threats

Discover and control rogue devices and applications based on risk mitigation policies.



### Stop Attacks in Their Tracks

Instantly stop breaches and prevent data loss and ransomware damage with no dwell time.



### Detect and Defuse in Real Time

Automatically detect and defuse potential threats in real time—even on compromised devices.



### Act Swiftly

Enable swift and effective response and remediation while keeping systems online.



### Automate Incident Response

Use customizable contextual incident response playbooks that automate response.



### Get Back to Business

Recover mission-critical systems fast and mitigate data loss to a few seconds.

## End-to-End Strategy Aligned with NIST Framework

Zerto continuous data protection, and Fortinet endpoint, detection, and response (EDR) solutions, align with the NIST (National Institute of Standards and Technology) Cyber Security Framework to provide a comprehensive strategy to mitigate the threat and impact of a ransomware infection. Following the framework helps organizations understand, manage, and reduce cybersecurity risks.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Continuously scan for unmanaged devices and apps and proactively minimize unprotected endpoints to reduce attack surface.	Leverage ML and granular security policies to protect against ransomware and zero-day malware across a broad variety of endpoints.	Rely on behavior-based detection to identify and defuse potential threats (even fileless malware) automatically.	Automate response while getting intelligence-infused guidance on alerts and investigation next steps. Safely test remedies in isolated sandbox.	Recover using granular control and speed, with the ability to return to a safe state from seconds before an attack was executed.

FortiEDR delivers innovative endpoint security with real-time visibility, analysis, protection, and remediation. It proactively shrinks the attack surface, prevents malware infection, detects and defuses potential threats in real time, and automates response and remediation procedures with customizable playbooks as well as through third-party connectors.

When coupled with Fortinet Security Fabric, you get heightened visibility, real-time threat intelligence, more opportunity for automated response from other Fortinet solutions, and a broad ecosystem of third-party integrations.

Zerto provides a foundation for continuous data protection (CDP) which is critical to the data recovery process—and the most effective method of ransomware mitigation. Zerto CDP delivers industry-leading, granular RPO and RTO and can ensure minimal data loss with pinpoint recovery.

Zerto offers the rapid maturity of a data protection and recovery solution that integrates cyber resilience, continuous data protection, and sandbox architecture that provides network isolation and enables data forensics that won't impact production.

## Serving Industries



### Financial Services

Modernizing banks need to digitize services without fear of disruption that could affect the bottom line. Ensure availability and access while reducing the likelihood of an attack.



### Healthcare

Modern digital strategies such as virtual care, telemedicine, and online collaboration underscore the need for endpoint protection and recovery strategies that safeguard patient data and access to critical systems.



### Public Sector

From military and defense to local agency response and civil services, people rely on their government to deliver essential services while moving modernization efforts forward.

## Get Started

For more information, or to start understanding how Fortinet and Zerto can help protect your data and applications, please reach out to [sales@zerto.com](mailto:sales@zerto.com).