EXECUTIVE SUMMARY

# Tackling Ransomware

An executive summary of the live webinar
*"Don't Let Ransomware Hold Your Critical Apps Hostage"*

## ABOUT THE PRESENTERS

**Gijsbert Janssen van Doorn, Technology Evangelist**

Gijsbert is a Technology Evangelist at Zerto with a focus on helping customers understand and adopt IT resilience. Before taking on the role as Technology Evangelist he spend 3 years working in the field at Zerto's Systems Engineering department. Prior to Zerto, Gijsbert was a Sales Engineer at Nexenta Systems supporting the sales of Software Defined Storage. Gijsbert has over 15 years of experience in IT infrastructure and has been involved in designing and implementing large IT infrastructures at both enterprises and large cloud service providers.

*Follow Gijsbert on LinkedIn*

**Chris Patterson, Sr. Director, Product Management**

Chris manages Navisite's Data Protection product development. Prior to Navisite, Patterson spent nine years at MTM technologies as the Director of Information Security Services, developing and consulting on security policies to the financial, retail, legal, health care, and public sectors. He holds a Bachelor's of Science in nuclear engineering from Worcester Polytechnic Institute and currently lives in Delaware.

*Follow Chris on LinkedIn*



Spectrum ENTERPRISE | Navisite

## Watch the webinar

Learn more about how managed disaster recovery can minimize downtime and protect from data loss, avoiding lost revenue and compromised internal and customer data.

Watch the full 30-minute webinar here >

## OVERVIEW

Cybersecurity remains one of the greatest IT concerns, due in part to an increased number of high profile attacks, as well as a renewed efforts by governments around the world to better regulate data use.

So what can organizations do to minimize the impact of a ransomware attack? In our webinar "*Don't Let Ransomware Hold Your Critical Apps Hostage*" Chris Patterson, Senior Director of Product Management for Navisite, and Gijsbert van Doorn, a Technology Evangelist at Zerto, consider how cloud-based disaster recovery solutions can ensure that critical data and applications are protected from ransomware and other malware attacks. We have highlighted some of the key points from the webinar below.

### THE PROBLEM: RANSOMWARE

With 60,000 ransomware infections occurring monthly, this form of malware attack is proving to be something organizations are challenged by on nearly a daily basis.

In the first quarter of 2017 alone ransomware cost organizations over $300 million – a figure which has doubled to an estimated $600 million in Q1 of 2018. On average ransoms cost $1,200 per infected machine and astonishingly over 70% of victims actually pay up – but only around half of those recover their data.

Noteworthy instances of ransomware include the 200,000 WannaCry attacks in 2017, affecting more than 150 countries worldwide and totaling more than four trillion dollars, along with attacks on Merck, law firm DLA Piper, the San Francisco Transportation System, Nayana, and most recently, the City of Atlanta.

Not infrequently, companies affected by ransomware suffer significant damage to their reputations.

**$1,200**

Average ransom cost per infected machine

### TRADITIONAL APPROACHES TO TACKLING RANSOMWARE USING BACKUPS

Obviously prevention is better than cure – basic IT housekeeping (e.g. ensuring the latest security patches have been applied) and making staff more aware of cybersecurity can stop many ransomware attacks in their tracks. However, once malware has broken into the network, effective disaster recovery methods are the best way to reclaim data that has been hijacked.

**$300 million**

Ransomware cost to organizations in the first quarter of 2017

Legacy data recovery solutions involved backups which ran relatively infrequently (e.g. once every 24 hours) due to significant impact on systems. This led to arduous recovery of data after an attack took place, taking hours at minimum, if not days or weeks. Furthermore, because data backups were done in snapshots, the recovery would only cover the time period up to the snapshot, resulting in a certain degree of data loss.

### MODERN SOLUTIONS USING DATA REPLICATION WITH ZERTO

Modern managed disaster recovery services from Navisite and Zerto now allow for more effective business continuity and disaster recovery plans. They offer

"...Once malware has broken into the network, effective disaster recovery methods are the best way to reclaim data..."

cloud based data replication solutions which ensure that data can be recovered following a ransomware attack faster, more fully and precisely, minimizing any disruption to services. Some of the benefits include:

- **Continuous data protection** – Zerto uses continuous data protection, so that systems can be rewound to their exact state seconds before the ransomware hit.
- **Minimal data loss** – because data protection is continuous, instead of potentially losing hours of data, only seconds will be lost.
- **Fast recovery** – as the process is fully automated, systems can be back up within a couple of minutes.
- **Minimal performance impact** – Zerto runs at the hypervisor level, which means it is possible to replicate workloads and set up a disaster recovery environment without having an impact on performance or production. It also allows the replication of groups of virtual machines at the same time.
- **Value** – the need for a second data center or colocation site as a replication target is eliminated.
- **Pay what you use** – with Zerto clients only pay for what they use (storage space, bandwidth), until they test or have a failover event, then they pay for what is required to restore lost data.
- **Tailored service** – Navisite offers different levels of service in managing the Zerto application according to specific client requirements, everything from a self-service option, to fully managing their replication needs.

### HOW DOES THIS HELP WITH REGULATORY COMPLIANCE (LIKE GDPR)?

Much data protection regulation requires data controllers and processors to implement protections against data loss or destruction (e.g. article 5 of GDPR). Although data recovery alone will not meet the primary objectives of data protection regulation – which is generally to avoid data being stolen or misused – it will certainly help to ensure compliance with certain elements of legislation in this area.

Other types of regulation (e.g. the SRA Handbook) may require that certain SLAs are met by service providers, thus minimizing any downtime will be critical to compliance. In this case, use of the Zerto disaster recovery application demonstrates that a robust incident response plan has been put in place. Furthermore, Zerto automatically generates reports from failover testing which can be used for compliance purposes.

### SUMMARY

Ransomware is a major, growing threat and its consequences can prove very costly to businesses which have not implemented methods to quickly restore lost data. Managed disaster recovery services from Navisite and Zerto provide a huge step forward, minimizing disruption and allowing business to continue as normal, while alleviating staffing and/or knowledge shortfalls in addressing this critical business need.

**For more information, visit navisite.com/CloudDR**

## Watch the webinar

Learn more about how managed disaster recovery can minimize downtime and protect from data loss, avoiding lost revenue and compromised internal and customer data.

Watch the full 30-minute webinar here >



Spectrum ENTERPRISE | Navisite