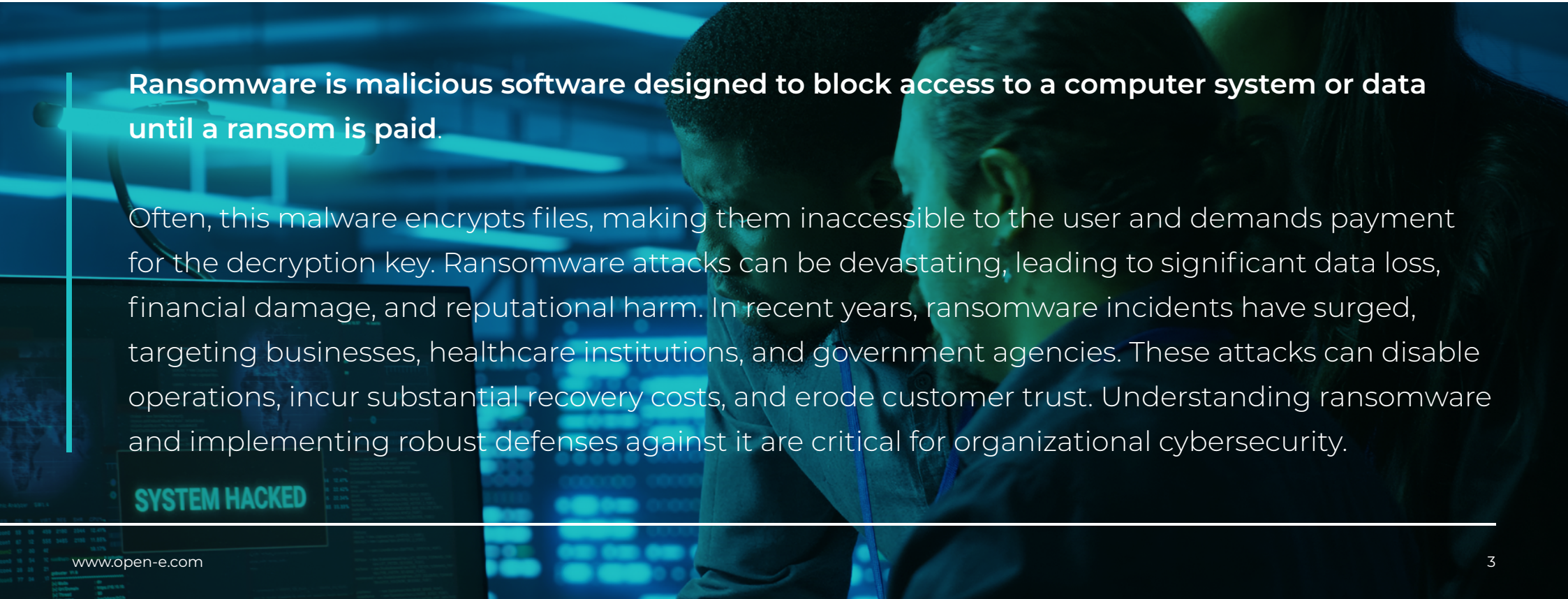
Next-Gen Defense:

How Open-E JovianDSS Protects Against Ransomware Attack Consequences

Table of contents

Introduction



Ransomware is malicious software designed to block access to a computer system or data until a ransom is paid.

Often, this malware encrypts files, making them inaccessible to the user and demands payment for the decryption key. Ransomware attacks can be devastating, leading to significant data loss, financial damage, and reputational harm. In recent years, ransomware incidents have surged, targeting businesses, healthcare institutions, and government agencies. These attacks can disable operations, incur substantial recovery costs, and erode customer trust. Understanding ransomware and implementing robust defenses against it are critical for organizational cybersecurity.

Major Cybersecurity Threats in 2024 and Beyond

Emerging Threats Identified by Open-E:

Emerging threats include AI-driven malware, deep fake scams, and increased targeting of IoT devices. Staying informed about these threats is essential for proactive defense.

- **AI-driven Malware**

  AI-driven malware represents a sophisticated evolution in malicious software, leveraging Artificial Intelligence to enhance its capabilities. These threats can adapt in real-time to security measures, which makes them more difficult to detect and neutralize. Artificial intelligence-driven malware can perform complex tasks such as evading detection systems, automating the exploitation of vulnerabilities, and even learning from the AI's environment to improve attack vectors over time.

- **Deep Fake Scams**

  Deep fake technology uses AI to create highly realistic fake images, audio, and videos, posing significant risks to individuals and organizations alike. Deep fake scams can be used for multiple malicious purposes, including identity theft, financial fraud, and spreading misinformation. The ability of deep fakes to convincingly mimic real people makes them a potent tool for social engineering attacks, potentially compromising sensitive information or causing reputational damage.

- **Increased Targeting of IoT Devices**

  The proliferation of Internet of Things (IoT) devices has created a vast and often insecure network of connected devices, ranging from smart home gadgets to industrial control systems. Cybercriminals are increasingly targeting these devices due to their weak security measures and critical roles in personal and organizational contexts. Compromised IoT devices can be exploited to carry out large-scale attacks, like Distributed Denial of Service (DDoS) attacks, or to obtain unauthorized access to sensitive networks and information.

Predictions for the Future Landscape of Cybersecurity

The cybersecurity landscape will continue to evolve, with attackers becoming more sophisticated. It is the reason for organizations to adopt agile and adaptive security measures to stay ahead:

Advanced Persistent Threats (APTs)

APTs are long-term, targeted cyber-attacks typically orchestrated by skilled and well-funded adversaries. They aim to steal sensitive data or disrupt operations without detection. Organizations must continuously monitor and adapt their security measures to effectively detect and mitigate these stealthy intrusions.

AI and Machine Learning in Cybersecurity

AI and machine learning technologies enhance cybersecurity by automating threat detection and response. They analyze vast amounts of data to identify patterns and anomalies indicative of cyber threats. This proactive approach enables organizations to anticipate and counteract sophisticated attacks more efficiently.

Regulatory Changes and Compliance

As governments and industry bodies update and introduce new cybersecurity regulations, organizations must adapt their security practices to remain compliant and avoid penalties. Staying abreast of these changes is essential to ensure data protection and maintain customer trust in an increasingly stringent regulatory environment.

Zero Trust Architecture

Zero Trust Architecture is a security model that assumes no entity, inside or outside the network, is trustworthy by default and requires continuous verification for access to resources. This approach minimizes the risk of data breaches by strictly enforcing access controls and monitoring all network activities.

Importance of Staying Ahead with Proactive Measures

Proactive measures, such as regular security assessments and adopting cutting-edge technologies, are crucial for maintaining robust cybersecurity:

Regular Security Assessments

Regular security assessments involve systematically evaluating an organization's security posture to identify vulnerabilities and weaknesses before attackers can exploit them. These assessments ensure that security measures are up-to-date and effective, allowing organizations to proactively address potential threats.

Adopting Cutting-edge Technologies

Embracing the latest cybersecurity technologies, such as advanced encryption, blockchain, and next-generation firewalls, enables organizations to fortify their defenses against emerging threats. Leveraging these innovations ensures that security systems can adapt to and mitigate sophisticated cyber attacks.

Continuous Monitoring and Threat Intelligence

Continuous monitoring involves real-time surveillance of network activities to detect and respond to threats swiftly. Integrating threat intelligence helps organizations stay informed about the latest cyber threats and vulnerabilities, allowing them to proactively anticipate and counteract potential attacks.

Employee Training and Awareness

Regular training programs and awareness campaigns educate employees about the latest cyber threats and best practices for preventing them. A well-informed workforce is crucial for maintaining robust cybersecurity, as human error is often a significant factor in security breaches.

Developing and Testing Incident Response Plans

Creating and routinely testing incident response plans ensures organizations can react quickly and effectively to cyber incidents. These plans provide a structured approach to managing and mitigating the impact of security breaches, minimizing downtime and data loss.

PROTECT YOUR BUSINESS FROM RANSOMWARE CONSEQUENCES

WITH OPEN-E JOVIANDSS! BREAK FREE IN 2024!

Welcome to the future of data protection — 2024 is the year of hypervisor-agnostic data storage! Choose your hardware, select your hypervisor, and pair it with Open-E JovianDSS for complete freedom from vendor lock-in. Scale your storage, boost performance, and protect your data without disrupting your operations. Don't wait for a ransomware attack to strike. Protect your data and ensure business continuity with Open-E JovianDSS! Contact us today to learn more or to schedule a demo. Let's secure your data future together! Act Now!

Advanced Snapshot Technology:

Stop ransomware in its tracks! Open-E JovianDSS takes instant snapshots of your data, preserving it in secure, isolated, and immutable recovery points. Should an attack occur, simply roll back to a clean snapshot and restore your data — fast and easy!

Smart Retention Plans:

Say goodbye to storage waste and hello to efficiency! Customize your snapshot retention plans to keep your critical data safe for as long as you need while freeing up valuable space. Protect your data without breaking the bank!

SED Encryption for Maximum Security:

Lock down your data with Self-Encrypting Drives (SEDs)! Open-E JovianDSS works seamlessly with hardware-level encryption, keeping your data secure, even in the event of a ransomware attack. When your data is encrypted, hackers don't stand a chance.

Business Continuity & Disaster Recovery:

Keep your business running no matter what! Open-E JovianDSS delivers rock-solid High-Availability (HA) clusters and on-/off-site backups, ensuring your data is always accessible — even during attacks or hardware failures. Recover quickly and get back to business!

Scalable, Hypervisor-Agnostic Data Storage:

Future-proof your storage infrastructure! Scale your storage needs effortlessly as your business grows with no vendor lock-in. Choose the hypervisor that works for you and enjoy total freedom to build the system that suits your needs!

Understanding Ransomware – History and Types

It's worth learning a bit about ransomware's history and types of ransomware that have evolved over the years to better understand how big a threat it has been and how fast cybercriminal groups' activities are growing. Here are the most important events that have significantly influenced how cyberterrorism works today and how it is forging ahead in the field of ransomware.

History

1989: The AIDS Trojan (PC Cyborg)

- **Origin:** Created by Joseph Popp, the AIDS Trojan is considered the first known ransomware.
- **Mechanism:** Distributed via floppy disks to attendees of a WHO conference. The malware encrypted file names on infected computers, demanding a ransom of $189 sent to a PO box in Panama for the decryption key.
- **Significance:** This early form of ransomware used simple encryption and demonstrated the potential for financial extortion using malware.

Early 2000s: Evolution of Ransomware

- **Innovation:** After the AIDS Trojan, there was a lull in ransomware activity. However, the early 2000s saw the emergence of more sophisticated ransomware attacks.
- **Mechanism:** Variants like GPCoder began to appear, using more advanced encryption techniques to lock files and demand ransom payments.

2005: GPcode

- **Innovation:** GPcode was an early example of ransomware that used RSA encryption.
- **Mechanism:** It encrypted files on the victim's computer and demanded a ransom for the decryption key. The encryption was relatively weak, allowing some researchers to break it, but it marked the beginning of more sophisticated encryption use in ransomware.

2011: WinLock

- **Innovation:** WinLock represented a significant evolution in ransomware tactics.
- **Mechanism:** Instead of encrypting files, WinLock locked users out of their computers entirely by displaying a full-screen image demanding payment. This variant targeted users in Russia and demanded payment via premium SMS services.

2017: WannaCry

- **Innovation:** WannaCry exploited a vulnerability in Windows systems, known as EternalBlue, to spread rapidly across networks.
- **Mechanism:** It propagated using worm-like behavior, encrypting files and demanding a Bitcoin ransom. WannaCry affected over 200,000 computers in 150 countries, including critical infrastructure like the UK's National Health Service (NHS), highlighting the devastating potential of ransomware combined with unpatched software vulnerabilities.

2022: Conti

- **Innovation:** Conti ransomware operated as a ransomware-as-a-service (RaaS) model, with affiliates carrying out attacks in exchange for a share of the profits.
- **Mechanism:** It used a combination of phishing emails and remote desktop protocol (RDP) exploits to gain access to networks, encrypting files and demanding payment.

2013: Cryptolocker

- **Innovation:** Cryptolocker was a major milestone in ransomware's history due to its strong encryption and widespread impact.
- **Mechanism:** It spreads via phishing emails containing malicious attachments. Once executed, it encrypted files on the victim's computer using RSA-2048 encryption and demanded a ransom in Bitcoin. Cryptolocker infected over 250,000 systems, generating millions of dollars in ransom payments.

2020: Maze

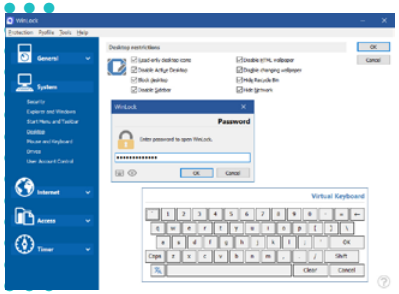
- **Innovation:** Maze ransomware popularized the tactic of double extortion, in which attackers encrypted data and threatened to leak it if the ransom was not paid.
- **Mechanism:** It spreads through phishing emails and exploit kits, encrypting files and exfiltrating sensitive data.

Types

Crypto Ransomware

Mechanism: Encrypts files on a victim's system, rendering them inaccessible without the decryption key.
Examples: Cryptolocker, Locky, and WannaCry.
Impact: This is one of the most common types and typically targets critical data, demanding payment for the decryption key.

Source: www.wikipedia.org



Locker Ransomware

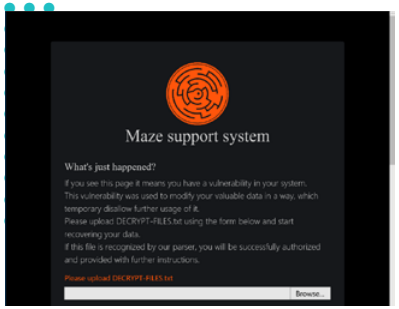
Mechanism: Locks the victim out of their entire system or device, preventing access to files and applications.
Examples: WinLock.
Impact: Unlike crypto-ransomware, locker ransomware doesn't encrypt files but locks the user interface, displaying a ransom note demanding payment to unlock the system.

Source: www.crystaloffice.com

Scareware

Mechanism: Uses fake threats and alerts to scare victims into paying a ransom. Often masquerades as antivirus or system optimization tools that claim the system is infected or compromised.
Examples: Fake antivirus software that displays continuous pop-up warnings.
Impact: It is generally less harmful as it doesn't encrypt files or lock the system, but it can still cause significant annoyance and lead to financial loss if victims pay the ransom.

Source: signal.avg.com



Doxware (Extortionware)

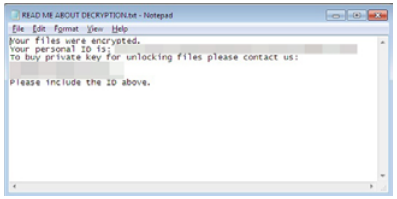
Mechanism: Threatens to publish or leak sensitive data unless a ransom is paid. Combines data encryption with the threat of data exposure.
Examples: Maze ransomware.
Impact: This type leverages the potential damage to the victim's reputation or privacy, often targeting businesses with sensitive customer data.

Source: media.kasperskycontenthub.com

RaaS (Ransomware as a Service)

Mechanism: A business model in which ransomware developers sell or lease their tools to affiliates, who then carry out the attacks. The profits are shared between the developers and the affiliates.
Examples: Sodinokibi (REvil), GandCrab.
Impact: This model has democratized ransomware attacks, making them accessible to less technically skilled criminals and increasing the overall volume of attacks.

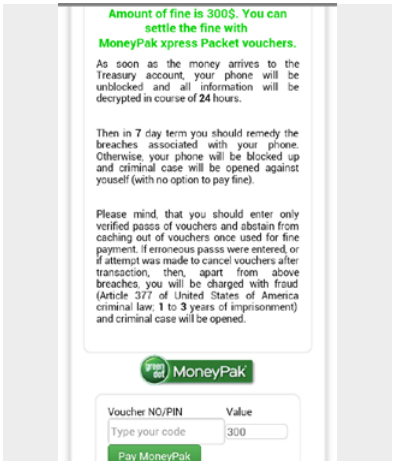
Source: www.pcrisk.pl



Fileless Ransomware

Mechanism: Operates entirely in the system's memory and uses legitimate system tools to carry out attacks, leaving no traditional malware files on the disk.
Examples: Sorebrect.
Impact: This type is harder to detect and remove because it doesn't leave a typical malware footprint on the hard drive.

Source: www.trendmicro.com



Mobile Ransomware

Mechanism: Targets mobile devices, locking them or encrypting stored data.
Examples: Koler and Simplocker.
Impact: Mobile ransomware can be particularly disruptive with the increasing use of mobile devices for sensitive transactions.

Source: www.webroot.com

The Process – How Ransomware Attacks You

Understanding how ransomware operates is key to defending against it. By knowing the various stages of an attack victims can better prepare, prevent, and recover from these incidents. Below is an overview of the common stages of a ransomware attack, detailing the tactics used by attackers and the impact on affected systems.

Initial Access

- **Exploit Kits**
  Attackers may use exploit kits to take advantage of software or the operating system vulnerabilities, enabling them to gain access and deploy ransomware. Remote Desktop Protocol (RDP): Attackers might exploit weak RDP configurations to gain remote access to a system and manually deploy the ransomware.
- **Phishing Emails**
  The most common method is phishing emails containing malicious attachments or links. When a user opens the attachment or clicks the link, the ransomware is downloaded onto their system.

Encryption

- **File Encryption**
  The ransomware begins encrypting files on the infected system, often targeting documents, databases, and other critical data. Encrypted files are typically renamed with a specific extension to indicate they are locked.
- **System Lockdown**
  In some cases, ransomware also locks the entire system, displays a ransom note on the screen, and prevents the user from accessing their files or system.

Ransom Note Delivery

Ransom Demand

The ransomware displays a ransom note, usually as a text file or a screen message, instructing the victim on how to pay the ransom to decrypt their files. This note often includes payment instructions, typically involving cryptocurrency, to maintain the attacker's anonymity.

Communication Channels

The note might provide a method for the victim to contact the attacker, such as an email address or a dark web site, to negotiate or confirm payment (IBM — United States) (McAfee).

Payment

Decryption Key

After payment, the attacker may (but is not guaranteed to) provide a decryption key or a tool to unlock the encrypted files. However, there's no assurance that paying the ransom will result in the restoration of files, and it encourages further criminal activity.

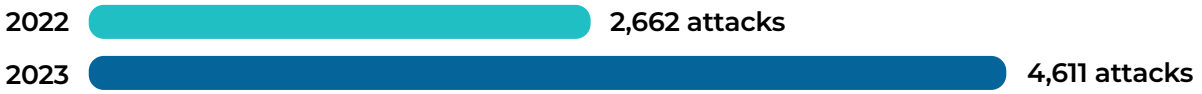
Ransom Payment

If the victim decides to pay the ransom, they follow the instructions to transfer the specified amount, usually in Bitcoin or another cryptocurrency.

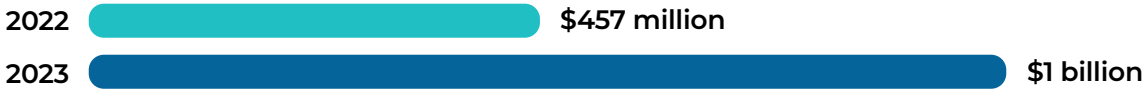
Ransomware Statistics and Trends 2022 – 2025

Ransomware attacks have seen significant fluctuations and trends between 2022 and 2023, with early indicators for 2024 suggesting continued escalation. Here's a detailed overview of the statistics and trends surrounding ransomware attacks during these years.

Overall number of attacks:



Average ransom payment ($):



% of Businesses impacted (approximately):

Cyberattacks Leading to Data Loss

The 2023 Data Health Check report found that cyberattacks were the leading cause of IT downtime and data loss. Hardware failures and cyber incidents accounted for a substantial proportion of these issues. **Many businesses overestimated their preparedness, with 62% believing they could only survive for less than a day without their IT systems**. This gap in preparedness often led to severe consequences when backups failed to deliver during a crisis.

Long-term Impact of Data Loss

Data loss can have long-lasting effects on businesses. **Statistics show that 51% of companies closed within two years of a significant data loss incident, and 43% never reopened. Small businesses were particularly vulnerable, with nearly 70% closing within a year after a major data loss**. These figures underline the need for robust, reliable backup and recovery systems to ensure business continuity.

Ransomware Predictions in 2025

Ransomware attacks are expected to become more sophisticated in 2025, exploiting cloud and VPN infrastructure vulnerabilities and using double extortion. The emergence of Ransomware-as-a-Service (RaaS) is spreading access to powerful ransomware tools, increasing the frequency and variety of attacks. Attackers will continue to exploit the anonymity of cryptocurrency payments, and artificial intelligence will enable more sophisticated phishing and ransomware campaigns, making defense more difficult

Key Trends and Observations

- **Shift in Targeting Strategies:** Ransomware groups increasingly adopt a „big game hunting" strategy, focusing on fewer but more lucrative targets. This approach has led to a rise in ransom demands exceeding **$1 million**.
- **Sector Vulnerability:** The healthcare sector has emerged as a primary target, especially in 2023, due to the urgency of potential ransom payments in life-critical situations. Other heavily targeted sectors include education, government, and business services.
- **Geographical Impact:** The United States remains the most affected country, with **574 victims** reported in just the second quarter of 2023.
- **Recurrence of Attacks:** A troubling trend is that **80%** of businesses that paid a ransom experienced another attack, highlighting organizations' persistent vulnerability.
- **The Emergence of New Threat Actors:** The landscape is becoming increasingly crowded with new groups, which accounted for **17%** of all ransomware incidents in 2023, indicating a growing pool of threat actors entering the field. Human error is often a significant factor in security breaches.

Sources: Statista, Security Magazine, TrueList, Invenio IT, and TechRadar.

Main Challenges in Ransomware Protection

Attack Methods & Strategies

Advanced Encryption Techniques

- **Caused by:** Modern ransomware uses strong encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), making it nearly impossible to decrypt files without the attacker's key. This level of encryption ensures that once the files are locked, they cannot be accessed without paying the ransom.
- **Example:** Cryptolocker, which uses RSA-2048 encryption, was one of the first ransomware strains to employ strong encryption, setting a precedent for future attacks.
- **Solution**: Implementing snapshots.

Exploitation of Zero-Day Vulnerabilities

- **Caused by:** Ransomware often exploits zero-day vulnerabilities, which are previously unknown flaws in software that are exploited before developers can release patches. This allows ransomware to bypass traditional security measures and infiltrate systems unnoticed.
- **Example:** WannaCry exploited the EternalBlue vulnerability in Microsoft Windows, a zero-day exploit that allowed it to spread rapidly across networks.
- **Solution**: Updates on each level.

Sophisticated Delivery Methods

- **Caused by:** Attackers use sophisticated methods such as spear phishing, drive-by downloads, and malvertising to deliver ransomware payloads. These methods are designed to trick users and evade detection by security software.
- **Example:** Phishing emails that appear to be from trusted sources can contain links or attachments that download ransomware when opened.
- **Solution**: Top-notch antivirus.

Common Vulnerabilities and Attack Vectors

Phishing Emails, Following Security Protocols, and Risk Awareness

- **Caused by:** Phishing is one of the most common methods of delivering ransomware. Attackers send emails that appear legitimate, encouraging recipients to click on malicious links or download infected attachments.
- **Example:** Locky ransomware was often distributed through emails containing Word documents with malicious macros.
- **Solution**: Employee awareness training and proper firewall configuration.

Unpatched Software Vulnerabilities

- **Caused by:** Ransomware exploits vulnerabilities in unpatched software to gain access to systems. Keeping software up to date is crucial to prevent these exploits.
- **Example:** The NotPetya attack leveraged a vulnerability in the Windows SMB protocol, which had not been patched in many systems despite a known fix being available.
- **Solution**: Regular updates and operating in heterogeneous environments.

Remote Desktop Protocol (RDP)

- **Caused by:** Weak RDP configurations and credentials can be exploited to gain remote access to systems and deploy ransomware.
- **Example:** Dharma ransomware uses brute force attacks on RDP to gain access and deploy the ransomware payload.
- **Solution**: Strong RDP or its alternatives.

Weaknesses in Data Protection

Inadequate Snapshot Strategies

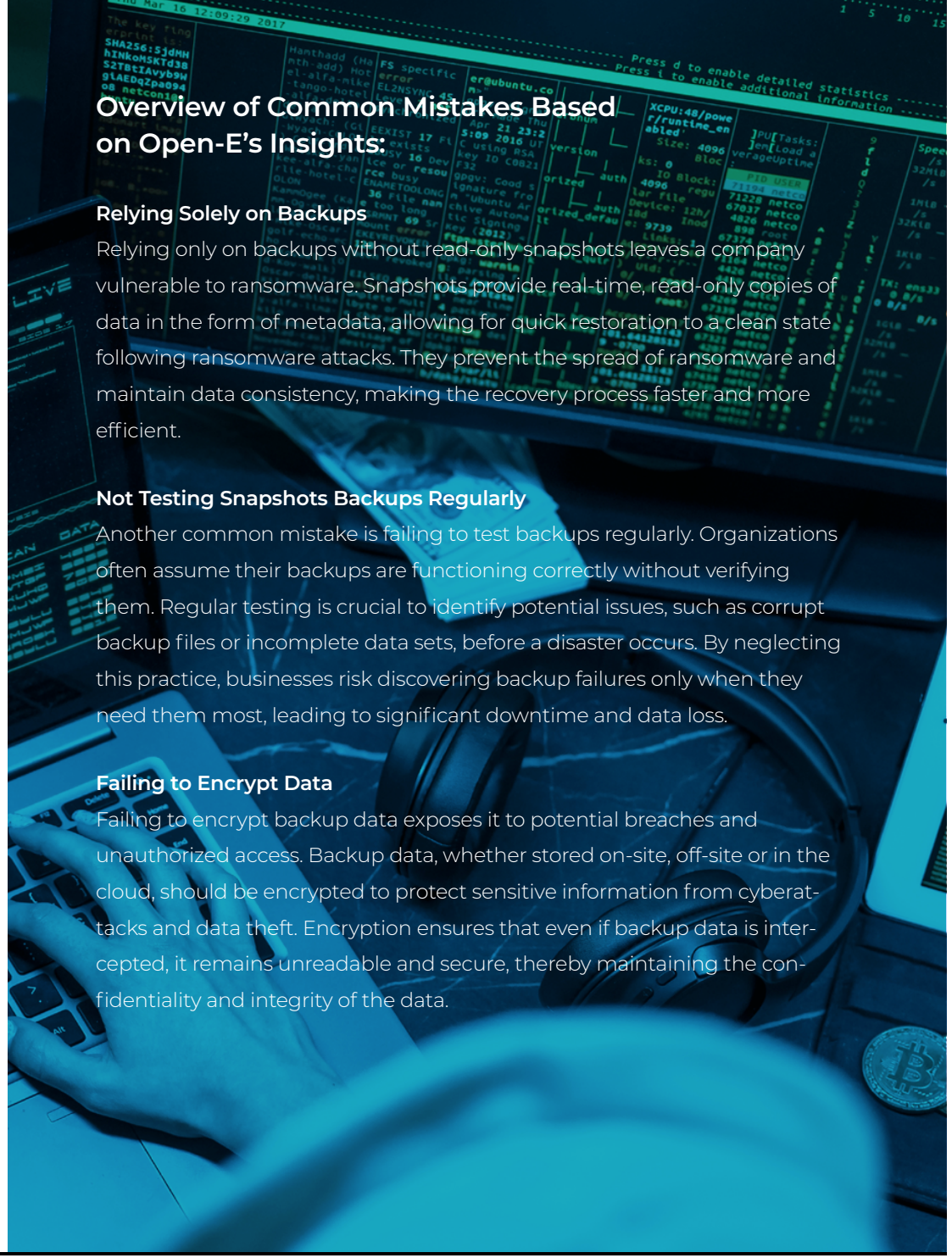
- **Caused by:** Not having regular and secure snapshots can lead to significant data loss if ransomware encrypts critical files.
- **Example:** Organizations hit by ransomware like CryptoWall without adequate read-only snapshots often have no option but to pay the ransom or lose their data. By integrating snapshots into their backup strategy and using retention plans, organizations can ensure data integrity and availability, enhance their resilience against ransomware, and reduce recovery time.
- **Solution**: Custom retention plans.

Lack of Data Encryption

- **Caused by:** Not encrypting sensitive data can increase the impact of a ransomware attack, as attackers can threaten to publish the data.
- **Example:** Maze ransomware, which combines file encryption with data theft, increases pressure on victims to pay the ransom by threatening to release sensitive information.
- **Solution**: Using SED and other encryption methods.

Common Mistakes in Data Backup and Recovery

In the field of ransomware protection, many cases are unique, depending on the business type of company that suffered the attack. **However, based on our experience on the subject, we can highlight some common mistakes in data protection that make it easier for cybercriminals to attack.**



Overview of Common Mistakes Based on Open-E's Insights:

Relying Solely on Backups

Relying only on backups without read-only snapshots leaves a company vulnerable to ransomware. Snapshots provide real-time, read-only copies of data in the form of metadata, allowing for quick restoration to a clean state following ransomware attacks. They prevent the spread of ransomware and maintain data consistency, making the recovery process faster and more efficient.

Not Testing Snapshots Backups Regularly

Another common mistake is failing to test backups regularly. Organizations often assume their backups are functioning correctly without verifying them. Regular testing is crucial to identify potential issues, such as corrupt backup files or incomplete data sets, before a disaster occurs. By neglecting this practice, businesses risk discovering backup failures only when they need them most, leading to significant downtime and data loss.

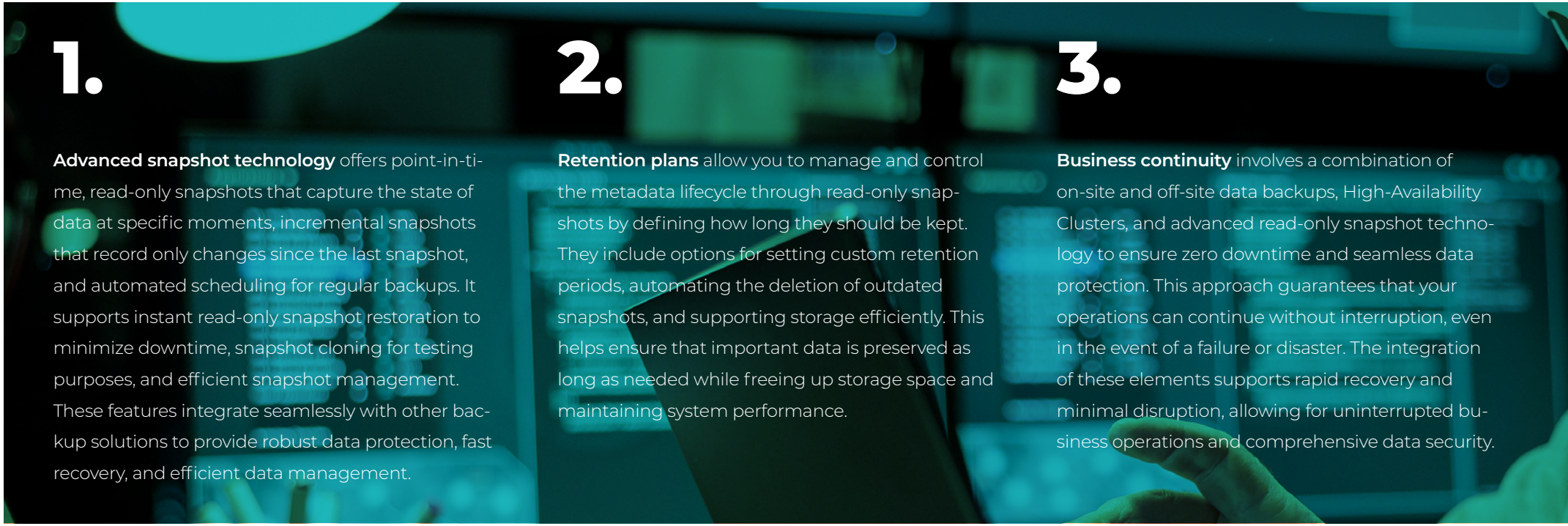
Failing to Encrypt Data

Failing to encrypt backup data exposes it to potential breaches and unauthorized access. Backup data, whether stored on-site, off-site or in the cloud, should be encrypted to protect sensitive information from cyberattacks and data theft. Encryption ensures that even if backup data is intercepted, it remains unreadable and secure, thereby maintaining the confidentiality and integrity of the data.

Open-E's Pro Tips to Avoid Ransomware Consequences

Multi-Layered Security Approaches

Employing a multi-layered approach, including firewalls, antivirus software, and intrusion detection systems, enhances overall security and reduces the risk of ransomware attacks. Open-E JovianDSS is a robust data storage software solution offering high availability, data integrity, and efficient data management. Key features include:



1.

Advanced snapshot technology offers point-in-time, read-only snapshots that capture the state of data at specific moments, incremental snapshots that record only changes since the last snapshot, and automated scheduling for regular backups. It supports instant read-only snapshot restoration to minimize downtime, snapshot cloning for testing purposes, and efficient snapshot management. These features integrate seamlessly with other backup solutions to provide robust data protection, fast recovery, and efficient data management.

2.

Retention plans allow you to manage and control the metadata lifecycle through read-only snapshots by defining how long they should be kept. They include options for setting custom retention periods, automating the deletion of outdated snapshots, and supporting storage efficiently. This helps ensure that important data is preserved as long as needed while freeing up storage space and maintaining system performance.

3.

Business continuity involves a combination of on-site and off-site data backups, High-Availability Clusters, and advanced read-only snapshot technology to ensure zero downtime and seamless data protection. This approach guarantees that your operations can continue without interruption, even in the event of a failure or disaster. The integration of these elements supports rapid recovery and minimal disruption, allowing for uninterrupted business operations and comprehensive data security.

4.

Disaster recovery solution provides comprehensive protection by enabling quick recovery from catastrophic events. It includes automated failover and failback processes to switch operations seamlessly between primary and secondary systems. The solution features real-time data replication to off-site locations, ensuring data consistency and minimal data loss. With automated testing and validation, you can ensure your recovery plans work effectively. This approach guarantees minimal downtime and rapid restoration of services, safeguarding business continuity in the face of disasters.

5.

Encryption techniques:

- Open-E JovianDSS supports Self-Encrypting Drives (SED), which provide hardware-based encryption. These drives automatically encrypt and decrypt data without impacting system performance. SED feature ensures that even if drives are physically stolen, the data remains inaccessible without proper authentication, adding an extra layer of security against physical data breaches and complementing ransomware protection.

- While encryption alone doesn't prevent ransomware attacks, it ensures attackers cannot read any stolen data. Coupled with other security measures, such as firewalls, antivirus software, and intrusion detection systems, this encryption strengthens the overall security posture, enhancing protection against ransomware.

Open-E JovianDSS Data Security Features

Ransomware-proof Data Safety Levels

A company's business needs can determine its data storage infrastructure's appropriate business continuity procedures. **Before selecting various data storage functions, it is crucial to understand the potential risks and be aware of every detail in the infrastructure**. Start by analyzing and realizing how and why your company stores data, then document all business processes related to data storage to ensure a comprehensive understanding of data management practices.

Basic ZFS Data Protection

To protect your data storage from cyberattacks, silent data corruption, and human errors, it is essential to use ZFS-based software with self-healing features to mitigate corruption risks, while also employing snapshots that allow you to restore the system to a previous state in the event of security breaches, accidental deletions, or modifications.

+ **Fast recovery with snapshots**
+ **Retention plans**
+ **Self-healing**

ZFS Data Protection with Data Redundancy

By using snapshots, self-healing, and RAID configurations, you can effectively secure your data against ransomware attacks, silent corruption, and drive failures, as RAID provides data redundancy and allows recovery of lost information through parity data, enhancing the resilience of your storage system.

+ **Basic ZFS Data Protection**
+ **Data redundancy — RAID rebuild**

High-Availability Cluster

To safeguard against data loss from server failure, industries such as retail, hospitality, and small-to-medium-sized businesses use High-Availability Clusters with two or more connected nodes. These clusters, which can utilize shared or non-shared data storage architectures, ensure Business Continuity by maintaining uninterrupted access to data, even in the face of ransomware attacks or hardware failures.

+ **Basic ZFS Data Protection**
+ **Data redundancy — RAID rebuild**
+ **High-Availability Clusters — shared and non-shared**

Open-E JovianDSS On- & Off-site Data Protection

On-site Data Protection with Open-E JovianDSS stores backups locally on both the production server and a secondary local server, allowing for quick system restoration and minimal downtime in the event of a ransomware attack. Off-site Data Protection adds an extra layer of security by storing backups on a remote server, ensuring that critical data remains safe and recoverable even if ransomware compromises on-site systems.

+ **Basic ZFS Data Protection**
+ **Data redundancy — RAID rebuild**
+ **On- & Off-site Data Protection**

Maximum Data Security

To maximize data security combine previous methods. You can use Open-E JovianDSS with on-site and off-site backups and a high availability cluster. While costs may be a concern, they are far less than the price of data loss or ransom, and expensive hardware isn't necessary for effective security.

+ **Basic ZFS Data Protection**
+ **Data redundancy — RAID rebuild**
+ **High-Availability Clusters — shared and non-shared**
+ **On- & Off-site Data Protection**

SEAGATE EXOS X24 24TB HDD

Ransomware-Proof Your Business with Cutting-Edge Encryption from Open-E and Seagate

Introducing Seagate Exos X24 SEDs with Open-E JovianDSS

Protect Your Business:

When Seagate's hardware encryption protects your data, ransomware, and cyber threats won't stand a chance. **Your encrypted data remains safe and secure even if your network is compromised**. Open-E JovianDSS ensures a seamless experience, automatically encrypting your information on the fly.

Speed Without Sacrifice:

Encryption doesn't have to slow you down. With Seagate Exos X24 SEDs, encryption is handled at the hardware level, enabling **ultra-fast data performance** without compromising security. Power up your operations with **secure, high-capacity drives** designed for performance.

Built-In Data Compliance:

Meet your industry's strict data security and privacy regulations effortlessly. With automatic encryption using Seagate Exos X24, Open-E JovianDSS helps you ensure that all data, whether at rest or in transit, is protected and compliant with GDPR, HIPAA, and more regulations.

Power Up Your Storage with Exos X24's Massive 24TB Capacity!

Why choose between performance and security when you can have both? Seagate Exos X24 delivers **up to 24TB of storage per drive**, so you can scale your infrastructure without worrying about data exposure. Combined with Open-E JovianDSS, you get **fast, reliable, fully encrypted, scalable, and ransomware-resistant storage**.

Your data deserves the best protection — start now!

open-e

Founded in 1998, Open-E is a well-established developer of IP-based storage management software. Its flagship product, Open-E JovianDSS, is a robust, award-winning storage application that offers excellent compatibility with industry standards. It's also the easiest to use and manage. Additionally, it is one of the most stable solutions on the market and an undisputed price-performance leader.

Thanks to its reputation, experience, and business reliability, Open-E has become the technology partner of choice for industry-leading IT companies. Open-E accounts for over 40,000 installations worldwide.

+40000 software implementations

+120 countries worldwide

+25 years of experience

+800 certified engineers and sales professionals

Open-E, Inc. | +1 (678) 666 2880 (US) | +49 (89) 800777 0 (Europe) | info@open-e.com