EGNYTE

Ransomware Primer for IT Leaders

Ensuring your content survives an attack.

Table of Contents

> There are only two kinds of companies. Those that have been hacked, and those that will be hacked.
>
> **— Robert S. Mueller |** FBI Director, 2012 RSA Cyber Security Conference

The ways organizations get hacked vary, but analysts, press, and vendors agree - ransomware leads the pack of security threats. Studies consistently show that the scale and cost of ransomware continue to grow.

- Ransomware is one of the biggest security problems on the internet and one of the biggest forms of cybercrime that organizations face today. ZDNet
- 73% of ransomware attacks resulted in criminals encrypting data. Sophos, The State of Ransomware 2020--5,000 IT Managers Across 26 Countries
- Downtime costs are up by 200% year-over-year, and the cost of downtime is 23X greater than the average ransom requested in 2019. Datto's 2019_State of the Channel Ransomware report
- 1,554,669 Kaspersky users encountered ransomware between January and December 2019. Kaspersky, Ransomware 2018-2020
- 500% increase in attacks on enterprises in the past year with cost of these attacks projected to be $11.5 billion, in addition to loss of customer and partner trust. Forrester, Ransomware Report
- Ransomware is arguably the most significant change in the malware threat landscape. IDC, Cybersecurity Threats: Eight Things CIOs Need to Know

Quick Review: What Is Ransomware

Ransomware software encrypts the data on or blocks access to computers and networks. It can also exfiltrate data. The perpetrator demands a ransom payment to decrypt data, remove the block, or stop the publication of data for public access.

How Ransomware Attacks Happen

Ransomware attacks vary as far as entry point, but the goal is the same – block access. The most common attacks use encryption to:

Block Access

Prevent employee access to content, especially files that are sensitive or valuable property of the company or customer.

- Encrypt files e.g., REvil
- Encrypt and exfiltrate data e.g., Clop
- Encrypt hard drive e.g., Petya
- Encrypt machines e.g., Ekans

Present Ransom Note

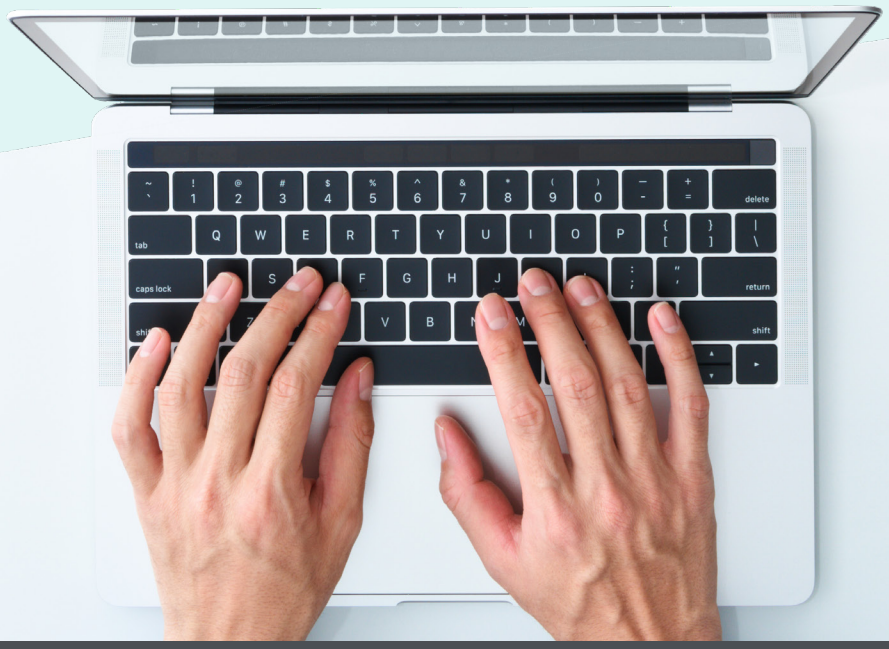
Once access is blocked, the ransomware presents a message that tells users:

- What has happened.
- How much to pay to undo it.
- Where to send the payment.
- What happens if the payment is not received.

Remediate

Once the damage has been assessed, ransomware recovery options come down to three choices.

- Pay the ransom.
- Attempt to remove the ransomware.
- Reinstall from the last clean point-ideally by file rather than blanket rollback.



Components of an Effective Ransomware Defense

Like all effective security, ransomware defense must take a holistic approach and incorporate multiple tools and tactics to protect potential targets.

Prevention must move beyond infrastructure protection, and towards protecting content, wherever it resides, including PCs, desktops, mobile devices, file storage, and cloud applications.

Ransomware protection strategies should include:

Identity and Access Management

Early Threat Detection

Continuity Planning

Content Protection and Restoration

Identity and Access Management (IAM)

Pretending to be a legitimate user makes it easier for cybercriminals to perpetrate malicious activities and harder to detect them. The following policies help reduce the risk of impersonation.

- Apply centralized policies to ensure that authorized users can only access content.
- Actively manage users' accounts and applications with updates and patches on all software and firmware, removing unused programs along with revoking keys and eliminating accounts when users leave.
- Implement a strong password strategy that dictates criteria for passwords and how frequently to update them.
- Require multi-factor authentication (MFA) everywhere to enhance logins with a credential from a physical token, smartphone, or biometric signature.

> It's important to maintain appropriate governance to keep your [IAM] program on track and avoid many pitfalls.
>
> **— Gartner Guide to Initiating and Running an Effective IAM Program**

Early Threat Detection

Preemptively neutralize threats by continuously monitoring and analyzing systems to detect suspicious activity. Stop threats before they become attacks with these solutions.

- Monitor for anomalies, such as inconsistent file types, abnormal file sharing, and accelerated encryption of files.
- Proactively identify suspicious login behavior.
- Protect entry points from unauthorized access using perimeter controls, such as firewalls, secure email and web gateways, and intrusion prevention/detection systems (i.e., IPS, IDS).
- Filter web content, email addresses, and attachments to block sites, messages, and content that may introduce malware or expose users to attackers.
- Deploy anti-virus, anti-malware, and anti-phishing tools at the end-user and email-server level—and keep them updated.
- Flag file extensions that have changed or contain known ransomware signatures.

> The critical benefit of threat detection and response is to respond to threats in real-time automatically.
>
> **— CIOReview |** An Overview of Threat Detection and Response

Continuity Planning

A continuity plan plays a critical role in ransomware remediation. It should explain, in detail, what steps to take to resume operations as quickly as possible. The plan should include different responses based on threat levels. And, the plan should be tested regularly to incorporate updates and ensure preparedness. To be prepared for a smooth recovery in the event of an attack, businesses should:

- Maintain visibility for all content and have the ability to discover sensitive files across cloud repositories and apps, device storage, and on-prem file shares.
- Set up automated ransomware detection and workflows to mitigate damage.
- Monitor content viewing, uploading, editing, sharing, and deletion at the company, team, and individual level to have early warning of suspicious activities.

Remember the **"Five Ps":** Prior Planning Prevents Poor Performance.

Content Protection and Restoration

While backups remain a crucial part of content protection, more must be done. The following best practices ensure that content survives a ransomware attack intact.

- Implement strict data access policies for internal and remote users based on role, location, and security tags.
- Provide file and folder permissions at a person-level.
- Use advanced encryption to protect content in transit and at rest as well as to obscure metadata that could make it easier for attackers to identify sensitive files.
- Sync files and backup to cloud and local storage.
- Maintain logs of which users uploaded, downloaded, or deleted files and folders.
- Backup frequently and provide granular rollback capabilities.

> We wanted to make sure that the data itself can be encrypted. As we did our analysis, we came up with the conclusion that Egnyte was the only one. It was designed from the ground up to handle enterprise-grade files. The others are not.
>
> **— Vimal Thomas VP** | Information Technology Yamaha Corporation of America

Solution Evaluation Questions

Use these questions when reviewing ransomware defense solutions. A vendor with strength in these areas will help effectively deflect ransomware attacks, minimize the impact of a ransomware attack, and expedite recovery and remediation from a ransomware attack.

File Access

Can file governance policies control access, at person-level, for internal and remote users based on role, location, and type of content (e.g., sensitive)?

Do file access restriction policies apply to all storage and apps across cloud and on-prem repositories as well as mobile devices?

How is two-factor authentication addressed?

How is encryption used to protect content?

Early Threat Detection

Is suspicious login and access behavior proactively monitored to flag known threats, inconsistent file types, abnormal file sharing, and accelerated encryption of files?

Can vulnerabilities be tracked in real-time?

How does the solution handle dormant ransomware and ransom notes?

File Protection and Restoration

Can files and backups be synced between cloud, on-prem, and local storage?

Is content recovery a blanket rollback to date, or can it be rolled back, by user, in a granular way?

What automation is included with regards to ransomware detection and response?

Deployment and Support

Can the solution support on-prem and cloud deployments across all devices and apps?

How long does it take to get up and running?

What infrastructure is required to support the solution?

What is the cost of ongoing maintenance and support services?

According to a recent Forrester report,

The number of ransomware attacks on enterprises is up 500% over the past year, and these attacks are projected to cost businesses $11.5 billion, in addition to the cost of loss of customer and partner trust.

Beat Ransomware By Defending Content

Remember content protection and governance when assessing ransomware solutions. This demands a shift in focus from protecting files and applications to safeguarding what is inherent in them—content. If content is protected, the enterprise is protected.

Egnyte's cloud-native solution leverages the industry's leading content intelligence engine to provide unparalleled protection from ransomware with proven content security and governance solutions. Egnyte delivers a simple, secure, and vendor-neutral foundation for ransomware prevention and remediation across applications and storage repositories.

Why do more than 16,000 companies choose Egnyte to protect their content?

Read more about Ransomware.

Learn More

EGNYTE

In a content critical age, Egnyte fuels business growth by enabling content-rich business processes, while also providing organizations with visibility and control over their content assets. Egnyte's cloud-native content services platform leverages the industry's leading content intelligence engine to deliver a simple, secure, and vendor-neutral foundation for managing enterprise content across business applications and storage repositories. More than 16,000 companies trust Egnyte to enhance employee productivity, automate data management, and reduce file-sharing cost and complexity. Investors include Google Ventures, Kleiner Perkins, Caufield & Byers, and Goldman Sachs. **For more information, visit www.egnyte.com**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com