EGNYTE

Ransomware Defense

Content visibility, control and remediation to combat ransomware.

Content has never been more critical to companies' success than ever before. It houses the data, information, knowledge and wisdom created by your organization to support growth and competitive advantage.

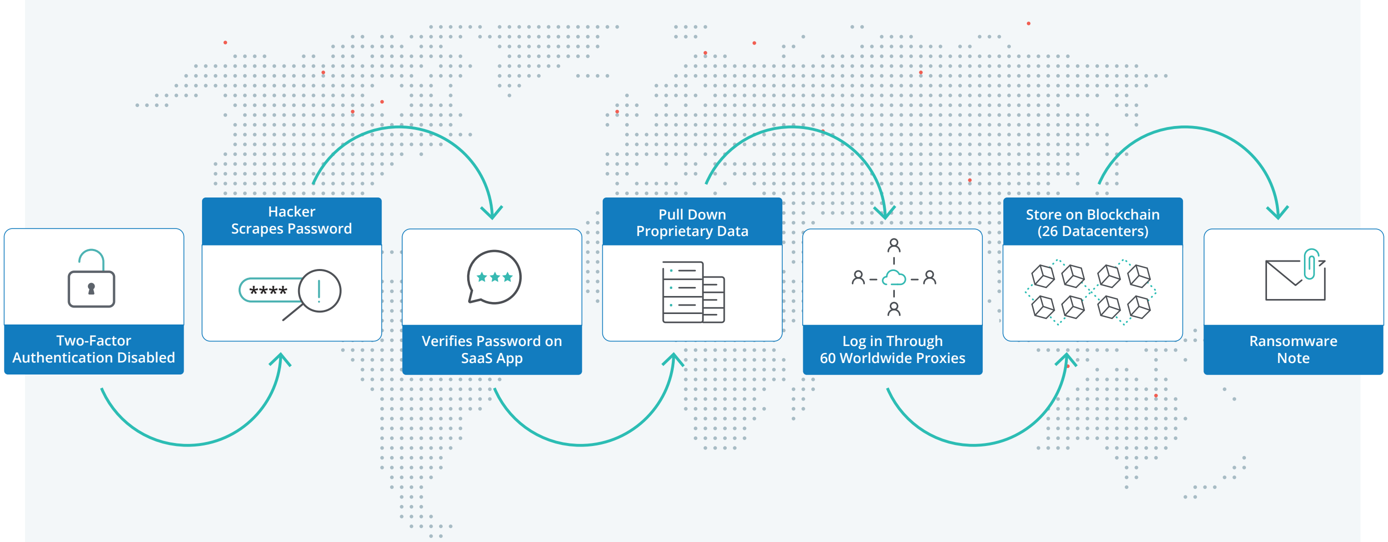
As such, the stakes are high. Risks to your content are threats to the entire business. Content governance is not only about securing enterprise files and data; it's about protecting the business itself.

The Challenge

Most companies house hundreds of thousands, even millions, of files - with employees accessing and sharing in more places than ever before. Now imagine those files locked and potentially gone forever.

Ransomware, malicious cyber threats that request victims to pay a ransom to retrieve stolen and encrypted data, are now the most prevalent cybersecurity threats for companies large and small. These types of attacks routinely cripple businesses and often result in huge financial losses.

Anatomy of a Ransomware Attack


Two-Factor Authentication Disabled
Hacker Scrapes Password
****
Verifies Password on SaaS App
Pull Down Proprietary Data
Log in Through 60 Worldwide Proxies
Store on Blockchain (26 Datacenters)
Ransomware Note

A good ransomware defense starts with full visibility of content, control over access to files, resources and data, and remote remediation capabilities, including the possibility of quarantining or blocking access to infected files.

The Egnyte Solution

Prevention

Egnyte provides advanced access controls to assign and manage folder and sub-folder permissions, two-factor authentication, and password management to prevent over-sharing and unnecessary access to sensitive information. These advanced access controls are critical to the implementation of data structure and hierarchy. Access permissions are always uniformly enforced, irrespective of location and access method.

Egnyte also provides tools for data minimization, to decrease your attack surface, along with a centralized dashboard to control and monitor all employee devices, and data governance tools to reduce content exposure.

Detection: monitoring and management

When an authorized user solicits content from an unlicensed, external party, that content is scanned for malware signatures upon upload, including known bad file extensions. Egnyte's signature-based ransomware detection runs a deep scan of all content in Egnyte and Windows File Server to detect known patterns of ransomware such as the presence of “ransom notes” in your content. As a first line of defense, signature-based ransomware is excellent at detecting known file types associated with ransomware.

For ransomware that has never been seen before, Egnyte includes behavior-based ransomware detection, which helps find previously unknown types of ransomware that can ravage your system. A proprietary machine-learning model looks for patterns of user activity associated with ransomware such as the rate of file rename, creation, deletion, and encryption, and alerts you to potential threats.

Remediation

Administrators can remediate issues by disabling links to content in Egnyte that contains sensitive data, taking action on compromised accounts, forcing password resets, adding user exceptions, deleting empty or unused groups, or moving or deleting sensitive content that is being shared too broadly or stored in unauthorized locations.

In the event of a ransomware attack, Egnyte can help identify affected files and roll back to the last good version.

By baking ransomware detection into the content environment, Egnyte makes it easier to discover and contain ransomware so it can be easily and quickly eradicated from your system before you go through the process of data restoration.

Conclusion

Ransomware is one of the top threats to individuals and businesses in recent history. Not only does it put sensitive, private information at risk, it has a noticeable impact on the pace and progress of businesses of all sizes.

Egnyte provides a comprehensive and intuitive solution for ransomware defense with:

- Granular folder and subfolder permissions
- Advanced password management
- Zero-day detection to mitigate the attack surface (blocking offending endpoints/users)
- Selective restoration
- Versioning and event-history auditing to isolate infected users
- Built in two-factor authentication
- Breach reporting
- Dormant ransomware and notes search
- ML-based data classification
- Data minimization and policy-based Redundant, Obsolete, Trivial (ROT) removal and archival

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. **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