EGNYTE

The Ultimate Guide to Ransomware

You Can't Defend What You Don't Understand

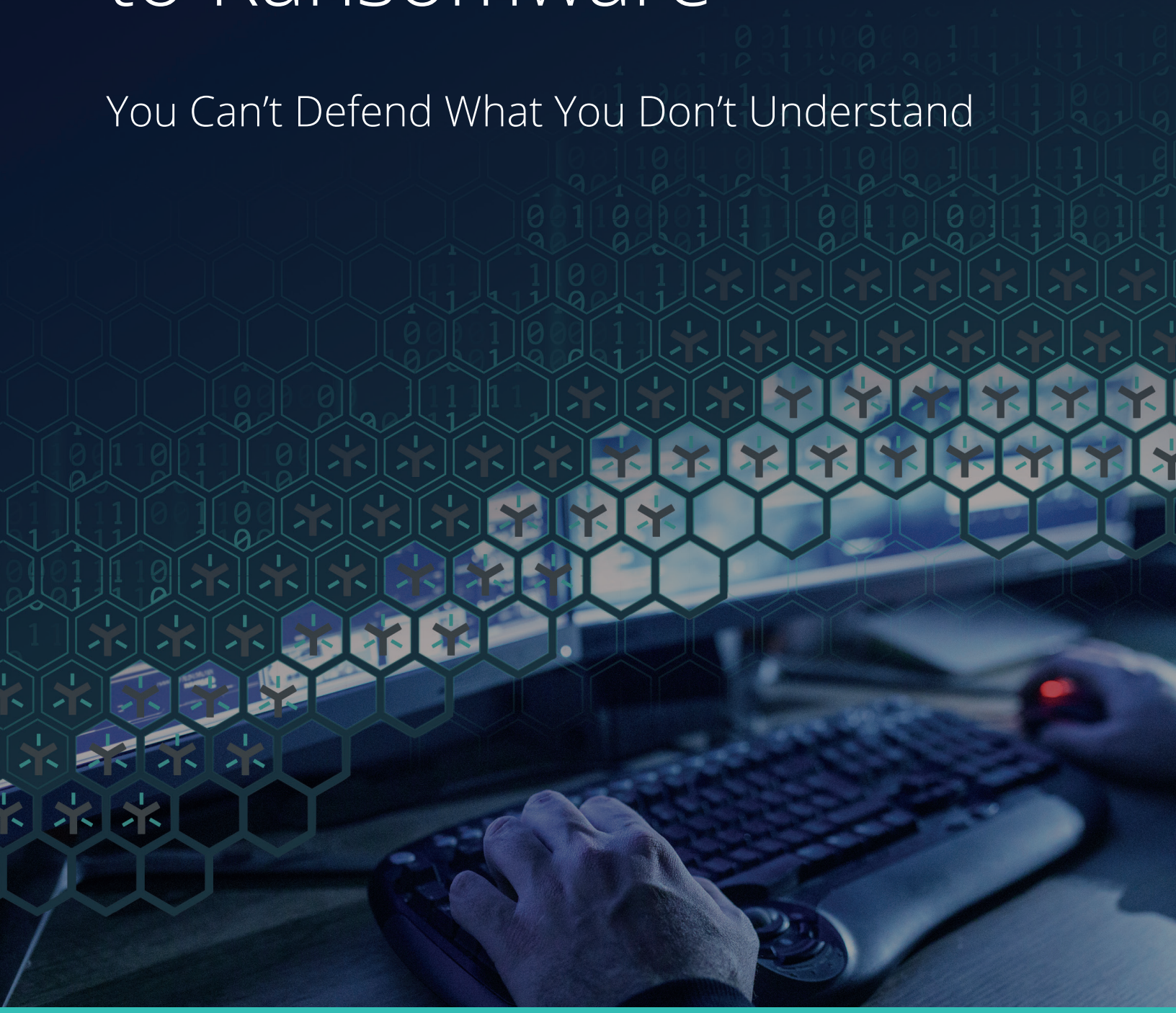
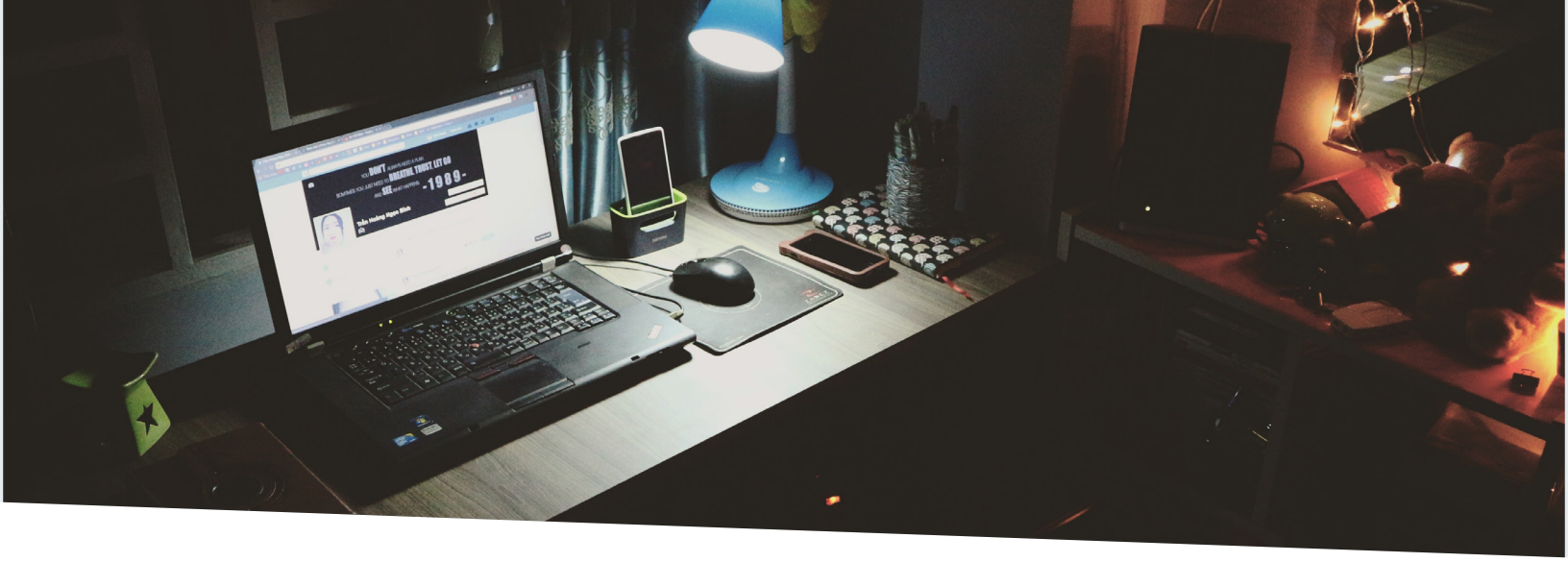


Table of Contents



You Can't Defend What You Don't Understand

Ransomware has wreaked havoc on individuals and organizations for more than 30 years. In 1989, Joseph L. Popp, a Harvard-educated biologist, introduced a Trojan by sending 20,000 compromised diskettes named "AIDS Information—Introductory Diskettes" to attendees of a World Health Organization AIDS conference. For the systems where users inserted the diskette, the Trojan encrypted file names on the computers and hid directories. A message popped up, telling users to pay $189 to PC Cyborg Corp. (by mail to a PO box in Panama) to have their systems decrypted.

Since then, ransomware and its purveyors have become far more sophisticated. The stakes have increased, and the barriers to entry have decreased. Dozens of new virulent strains of ransomware are active, and older ones are being repurposed or morphed.

Ransomware criminals are as varied as their approaches and targets. What remains consistent with ransomware is that small and medium businesses are the target of the bulk of attacks—because they lack the depth of security infrastructure that larger organizations have, making them easier targets.

Ransomware has the full attention not just of IT, but of executive teams. It ranks among the top priorities for both business and IT leaders.

To stop ransomware, organizations must understand:

- Perpetrators and how they work
- How ransomware works
- Prevention tactics
- Remediation and best practices for effective response

What is Ransomware and How it Works

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 arguably the most significant change in the malware threat landscape. IDC, Cybersecurity Threats: Eight Things CIOs Need to Know
- 1,554,669 Kaspersky users encountered ransomware between January and December 2019. Kaspersky, Ransomware 2018-2020
- 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
- Ransomware is one of the biggest security problems on the internet and one of the biggest forms of cybercrime that organizations face today. ZDNet

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.

Ransomware depends not on the complexity of its code, but the vulnerabilities of its targets. At its core, ransomware is just a worm looking for a hole. Preparation for a near-inevitable ransomware attack prevents it from becoming a breach, repelling it before it enters and closing holes.

> **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.

Ransomware Entry Points

Many organizations have porous security perimeters, especially with the spike in remote workers. However, ransomware usually takes an easier approach. It enters from a download delivered via email, because this point of entry requires the least effort on the part of the attacker. The ransomware appears as a link or attachment, often from a known source, with an enticement to click it. The attachment or link is an executable file that unleashes the ransomware.

Inadvertent downloads of malware from an infected website—sometimes executed by clicking, others by simply landing on the site—are also popular attack points for ransomware. (This includes chat and social media messaging.) This stealthy ransomware enters systems through vulnerabilities in various browser plugins, with the delivery mechanism being merely visiting a website. This ransomware, known as drive-by ransomware, is delivered in the background, often without the user being aware of it. Other entry points include good, old-fashioned social engineering and malware carried on USB drives.

More sophisticated ransomware attacks take advantage of systems' and networks' backdoors or vulnerabilities. Attackers probe targets to find weaknesses in security systems, such as lapsed patches and updates, gaps in the configuration of security tools, and insecure remote users.

Ransomware Attack Profiles

Attacks do not necessarily begin at the time of entry. Often ransomware works quietly without users noticing. It lurks in the background while it prepares for its attack on the point-of-entry system or spreads across the network to other systems before activating and making its presence known. Sometimes the ransomware lies dormant after download or downloads in segments to avoid detection. Regardless of its download timeline, once file lockdown begins, the ransomware acts quickly—taking between 18 seconds and 16 minutes to encrypt 1,000 files.

Ransomware software has two approaches to encryption. The simpler versions use the encryption functions that exist on Windows and Unix, including macOS and Linux. More sophisticated ransomware uses custom encryption implementations to bypass security software. "Off-the-shelf," open-source projects offer packaged ransomware. No matter what type of ransomware attack, once files are encrypted, no one can decrypt them without the attacker's decryption key.

After files are locked down, the ransomware presents a message (i.e., a ransom note) 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

Ransom notes usually reveal the type of ransomware used for the attack.

> "There are only two kinds of companies Those that have been hacked, and those that will be hacked."
>
> This oft-repeated saying originated at the RSA Cyber Security Conference in 2012 in a talk by **FBI Director Robert S. Mueller.**

The Ransom and Related Threats

The two main threats from ransomware attacks are that files will remain encrypted and that files will be made public. Sometimes these threats are used in tandem—pay the ransom or files will be shared—to encourage the organization to pay the ransom even if they have a backup of the encrypted files. This tactic is particularly effective when customers fear losing private data or intellectual property. Ransomware often has a built-in timer to trigger notices that the ransom has increased or delete encrypted files.

Security experts and law enforcement agencies do not support paying ransom in response to a ransomware attack. According to the FBI, "It does not guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."

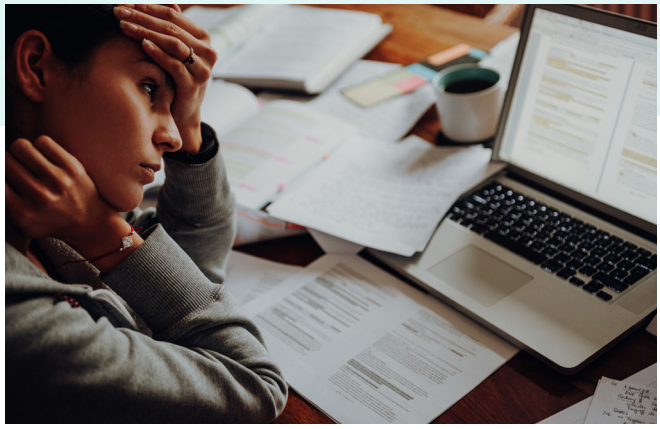
However, as Stephane Nappo said, "It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." In addition to reputation damage, loss of productivity, and the ensuing business disruption, often motivates organizations to pay the ransom. Increasingly companies are adding ransomware insurance to their coverage portfolio. Whether paid for out-of-pocket or by insurance, payments are delivered with digital currency sent to an anonymous wallet.

About the attackers

Ransomware is used by individuals, small groups, and crime syndicates. The accessibility and ease-of-use make readily accessible as would-be criminals can buy ransomware on the dark web or use ransomware-as-a-service.

The primary roles in a ransomware operation are:

- Ransomware procurement (create it or buy it) and hosting
- Campaign development and execution
- Payload collection and distribution



The more committed cybercriminals band together as part of networks to leverage reach, resources, and skills. How ransomware networks organize differs, but the three most common structures are as follows.

- **Consolidated ownership and operations -** One organization or individual controls all three operational functions and keeps 100% of the profits.
- **Channel-styled operations -** The lead organization handles ransomware procurement and hosting as well as payment collection and distribution. Campaign development and execution, or the spread of ransomware, is dealt with by a third-party organization or individual who generally receives 50-75% of the profits. This model is also known as ransomware-as-a-service.
- **Ransomware infrastructure-in-a-box -** A third-party service provider packages and sells the bundle of products and services needed to launch ransomware attacks and collect payment. Then the attacker procures the ransomware, buys the bundled solution, and keeps 100% of the profits.

For the most part, attackers can be classified into two groups.

- **Big-game hunters -** They target organizations with high-value data or assets, especially those sensitive to downtime, as these are more likely to pay a ransom. While high-profile, big-game ransomware attacks occur less often, because of the time and effort involved.
- **Spray and pray attackers**

This approach directs attacks at an acquired list of emails or compromised websites. These smaller, generic ransomware attacks are most common and cause the most harm and disruption, because of their scale.

Organizations of All Sizes Susceptible to Ransomware

Large enterprises tend to attract "big-game hunters." These cybercriminals target the organizations that have the funds or insurance to pay a ransom. Sophisticated attacks and patience are the hallmarks of big game hunters. They usually operate as a group and can spend months inside an organization preparing for a ransomware assault. The Cyber Front Lines Report says, "average dwell time grew 10 days to 95 in 2019, up from 85 in 2018. Their efforts have been lucrative, with an average payment of $41,198, as of Q3 2020, and larger enterprises facing demands over $1 million.

Small and midsize enterprises (SMEs)—from mom-and-pop businesses and small municipal agencies to multi-location companies and larger government organizations with hundreds of employees—are attractive targets to cybercriminals. This is due to the number of SMEs and their predictable cybersecurity weaknesses.

The World Bank says, "They represent about 90 percent of businesses and more than 50 percent of employment worldwide." Despite admirable achievements, SMEs generally do not dedicate IT resources to cybersecurity and inevitably have technical vulnerabilities. And, human nature is a vexing vulnerability.

SMEs become targets not only to harvest their content, but also to gain access to partners' and clients' content and systems. In May 2020, a ransomware attack on M.J. Brunner, a technical services vendor, leapfrogged to its client SEI Investments Co. Once the ransomware had moved from M. J. Brunner to SEI, it attacked SEI's clients—among them Pacific Investment Management Co. (Pimco), Fortress Investment Group LLC, and Centerbridge Partners. Although compliance agreements between clients and vendors abound, SMEs' vulnerabilities often make them the first rung on the ladder for ransomware.

> "The US was hit by a barrage of ransomware attacks in 2019 that impacted at least 948 government agencies, educational establishments and health-care providers at a potential cost in excess of $7.5 billion."
>
> "Multinational manufacturers and US city and county governments spent more $176 million responding to the biggest ransomware attacks of 2019, spending on everything from rebuilding networks and restoring backups to paying the hackers ransom."
>
> **—Michael Novinson |** CRN.

61% experienced ransomware attacks

70% paid ransom

72% said that attackers had evaded intrusion detection systems

82% said that attackers had evaded anti-virus solutions

79% said that ransomware attacks were from phishing/social engineering

The State of Cybersecurity in Small & Medium Size Businesses
Ponemon Institute

Victims of Ransomware Despite the Best of Intentions

Ransomware attacks succeed despite the numerous security tools that most organizations have in place. Cybercriminals circumvent security systems and take advantage of the inherent weaknesses of people. Attackers favor humans as the entry point because criminals of all stripes successfully exploit their vulnerabilities. Despite training, common sense, and perpetual warnings, people remain susceptible to ransomware.

Attackers use social engineering to trick people into engaging. They tap into people's weakness—lack of attention to detail, trust without verification, curiosity, and fear.

Lack of attention to detail

> At a glance, the message seems to be offering a person something that they had asked for or were interested in exploring.

Trust without verification

> The message appears to come from a trusted source with a call to action that seems reasonable.

Curiosity

> An enticing offer is presented when someone is busy overrides second thoughts about the legitimacy of the message.

Fear

> A threat, commonly related to a late payment or a law enforcement agency message, scares someone into falling for the attack.

Also, security systems require near-constant attention and maintenance to sustain an effective security posture. Even with dedicated security teams, this remains a tall order for most organizations. These weaknesses in security and IT systems are exploited to perpetrate ransomware attacks.

Three Ways Ransomware Attacks People

Attackers favor email and pop-up ads to deliver ransomware.

Malicious Pop-Ups

More insidious are malicious advertising and pop-ups delivered while a person browses a website—even legitimate ones. Again, targeting people's inherent vulnerabilities, these ads can trick even the most vigilant. Malicious ads are often disguised as legitimate ads or, ironically, a security notification. Triggers to start the ransomware download can also be sneaky, such as click the "x" to close the pop-up or even roll over the ad.

In 2017, a ransomware named Bad Rabbit infected websites and asked visitors to click to install Adobe Flash. Kaspersky Labs describes the attack. "While the target is visiting a legitimate website, a malware dropper is being downloaded from the threat actor's infrastructure."

Infected USB Memory Sticks

Perpetrators also use Infected USB memory sticks to deliver ransomware to a device. A busy person grabs a USB flash drive that carries the ransomware, and the spread starts—from the first system to any subsequent ones and systems connected to the network.

Try2Cry, launched in July 2020, initially looked for connected removable drives and inserted itself into the root folder of the USB flash drives. Malware Guide calls this crytpo ransomware, that compromises all kinds of content, "a dangerous and lethal file-encrypting virus that has been created to intimidate and receive ransom money from victimized users."

Malicious Email

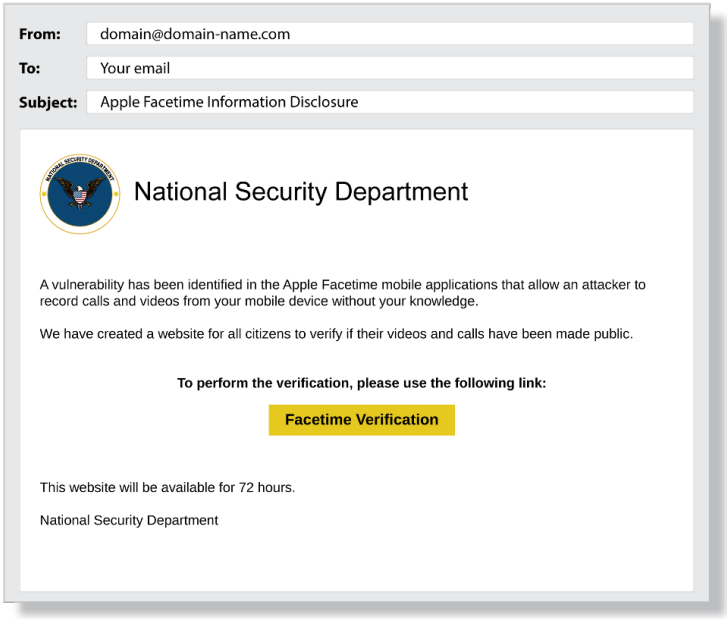
The social engineering ploys noted above lure people into clicking and unwittingly unleashing ransomware via email. An unsolicited message delivers ransomware through infected attachments or links to malicious websites.

> Seventy-six percent of IT executives are concerned about unstructured data sprawl, and more than half say remote work is the main culprit.
>
> Away from the office, nearly a third of employees are accessing corporate files through unsecured WiFi networks and on personal devices with no password requirements. This is a big problem because a large portion of these files
>
> contain sensitive information.
>
> **Egnyte, Fall 2020 Data Governance Trends Report.**

Sprawling Ransomware Attack Surface

Ransomware targets any vulnerable device, but it focuses on those connected to networks. This increases the reach of the ransomware and the potential size of the demand.

People get hit on their commonly used connected mobile devices, primarily desktops, laptops, phones, and tablets. The recent spike in the number of connected devices, often used on unsecured home networks, creates an enticing attack
surface for ransomware as organizations struggle to provide adequate security. And, they suffer knowing that behind this porous perimeter lies the content that organizations depend on for day-to-day use, compliance, and back up.



Types of Ransomware

Content and systems mostly fall prey to two types of ransomware-locker ransomware and crypto ransomware. Others include scareware and doxware.

Locker Ransomware

Locker ransomware takes over an operating system then locks the device's user interface to prevent access to computing resources—except for a communication channel with the attacker. WannaCry, a locker ransomware that spread across 150 countries in 2017, was estimated to have caused $4 billion in financial losses.

Crypto Ransomware

With crypto ransomware, the impacted device can be accessed, but the files are encrypted. The attacker threatens that all content in the files and folders will remain encrypted until they receive the ransom payment. UCSF networks within the School of Medicine IT environment were attacked in June 2020, and data described as "important to some of the academic work we pursue as a university serving the public good" was encrypted. The university paid $1.4 million to recover the data.

Scareware

Scareware commonly appears as a warning from security software that payment must be made to fix or remove a problem. Unlike locker ransomware or crypto ransomware, scareware only presents annoying pop-up messages. Below is an example of scareware from "SpySherriff."

DoxwareMemory Sticks

Also referred to as extortionware, doxware encrypts personal content (e.g., contacts, photos, messages, files) then threatens to make it public unless the attacker receives the ransom payment. In July 2020, the University of Utah paid $457,000 ransom to prevent the release of student and employee information.

Reach of Ransomware Continues to Grow. Ransomware cases doubled in the first quarter of 2020.

Out of 121.2 million recorded ransomware attacks, 79.9 million were recorded in the US and 5.9 million in the UK

Channel Pro Fall 2020 Data Governance Trends Report.

Ransomware-as-a-Service (RaaS)

Based on the SaaS model, RaaS offers criminals the use of ransomware tools for a fee. Cybercriminals create ransomware then provide access to it along with tools and instructions to launch attacks.

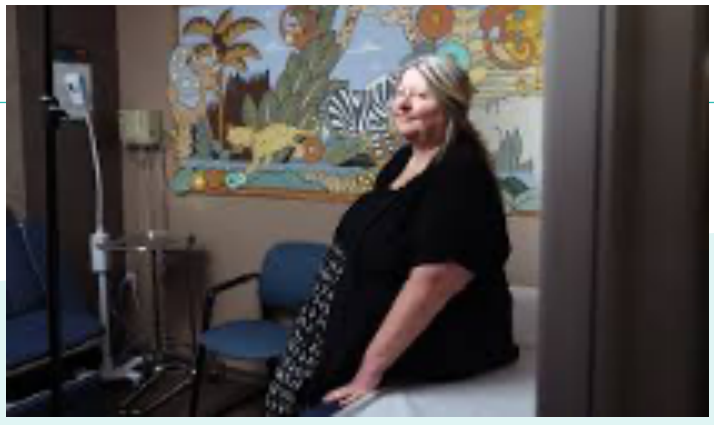
Depending on the RaaS provider, criminals pay for the use of the ransomware and share a portion of the ransom-service fees can be high. The RaaS crypto ransomware, Satan, takes 30% of the ransom collected.

RaaS makes ransomware easily accessible to criminals with novice hacker resources. Would-be cybercriminals find RaaS options, such as Satan, on the Dark Web and sign up to join the platform just as they would with legitimate SaaS solutions. Once their subscription is set up, they gain access to the malicious code as well as instructions on how to execute their ransomware attack. With the ready availability of RaaS offerings, there is little to no barrier to entry-any organization's content and systems can be targeted.

Ripple Effect of a Ransomware Attack

In Simi Valley, California, Wood Ranch Medical (WMR) was delivered a death blow by a ransomware attack in August 2019. A month later, with her patients' health records encrypted and no way to restore them, Dr. Shayla Kasel (founder and owner of WMR) announced that she would permanently close WMR's doors on December 17. (Happy holidays to the patients and employees of WMR—NOT.)

Dr. Kasel, along with her staff, lost their jobs and patients found themselves without a healthcare provider for their families. And while it is believed that no personally identifiable information (PII) was taken, almost 6,000 patients had to interrupt their holiday season to find a new doctor and set up monitoring services to protect themselves. Another blow was that patients lost their health records.



The Ransom and Related Threats

The two main threats from ransomware attacks are that files will remain encrypted and that files will be made public.

Sometimes these threats are used in tandem—pay the ransom or files will be shared—to encourage the organization to pay the ransom even if they have a backup of the encrypted files. This tactic is particularly effective when customers fear losing private data or intellectual property. Ransomware often has a built-in timer to trigger notices that the ransom has increased or delete encrypted files.

Security experts and law enforcement agencies do not support paying ransom in response to a ransomware attack. According to the FBI, "It does not guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."

However, as Stephane Nappo said, "It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." In addition to reputation damage, loss of productivity, and the ensuing business disruption, often motivates organizations to pay the ransom. Increasingly companies are adding ransomware insurance to their coverage portfolio. Whether paid for out-of-pocket or by insurance, payments are delivered with digital currency sent to an anonymous wallet.

About the Attackers

Ransomware is used by individuals, small groups, and crime syndicates. The accessibility and ease-of-use make readily accessible as would-be criminals can buy ransomware on the dark web or use ransomware-as-a-service.

The primary roles in a ransomware operation are:

- Ransomware procurement (create it or buy it) and hosting
- Campaign development and execution
- Payload collection and distribution

The more committed cybercriminals band together as part of networks to leverage reach, resources, and skills. How ransomware networks organize differs, but the three most common structures are as follows.

- **Consolidated ownership and operations**
  One organization or individual controls all three operational functions and keeps 100% of the profits.
- **Channel-styled operations**
  The lead organization handles ransomware procurement and hosting as well as payment collection and distribution. Campaign development and execution, or the spread of ransomware, is dealt with by a third-party organization or individual who generally receives 50-75% of the profits. This model is also known as ransomware-as-a-service.
- **Ransomware infrastructure-in-a-box**
  A third-party service provider packages and sells the bundle of products and services needed to launch ransomware attacks and collect payment. Then the attacker procures the ransomware, buys the bundled solution, and keeps 100% of the profits.

For the most part, attackers can be classified into two groups.

1. Big-game hunters
They target organizations with high-value data or assets, especially those sensitive to downtime, as these are more likely to pay a ransom. While high-profile, big-game ransomware attacks occur less often, because of the time and effort involved.

2. Spray and pray attackers
This approach directs attacks at an acquired list of emails or compromised websites. These smaller, generic ransomware attacks are most common and cause the most harm and disruption, because of their scale.

Ransomware Stands Ready to Attack

Three Things to Stop It

Deploy an effective defense against ransomware with:

1. Prevention

Have systems in place that protect the essential assets—content. Prevention goes beyond firewalls and anti-virus solutions. It includes data protection, regardless of where it resides (e.g., file storage, applications, devices), and data governance to maintain data stores' health and safety.

2. Remediation

Be prepared to act as soon as an issue is detected. Neutralize the attack and restore systems and data without additional disruption—surgical restoration rather than a blanket rollback.

3. Monitoring and Maintenance

Early detection can stop an attacker before damage is done or minimize the impact of an attack. Monitoring should leverage machine learning to analyze user behavior, and it should include signature-based detection. Maintenance should encompass both systems and content. Only content in-use should be accessible. Once it has served its purpose, content should be permanently deleted or encrypted and archived.

Be proactive and assess the state of your security profile to identify the gaps. Find a solution that addresses deficiencies in a way that does not overburden your IT staff or require workflow changes from other team members.

Ransomware Prevention Considerations

Benjamin Franklin's cautionary words still ring true, "An ounce of prevention is worth a pound of cure."

When considering ransomware, prevention should focus on the essential asset in all organizations—content. Prevention must go beyond infrastructure protection. It needs to protect content wherever it resides, including PCs, desktops, mobile devices, file storage, and cloud applications.

Like all effective security, ransomware prevention must take a holistic approach and incorporate multiple tools and tactics to protect potential targets. Ransomware protection strategies should include:

- **Content protection**
- **Identity management policies**
- **Early threat detection**
- **Compute layer security**
- **Cybersecurity awareness and training**
- **Continuity planning**
- **Ransomware insurance**

Prevention | Content Protection

Backup is at the core of any content protection plan. Systems should be backed up locally and using cloud storage.

The cloud backups provide redundancy and add an extra layer of protection. 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.

Backup Policies

- Have multiple backups in case the last backup gets overwritten with encrypted ransomware files
- Keep a backup of sensitive data offsite in data centers with strictly limited access
- Separate backups from production systems—not connected to the computers and networks they are backing up
- Backup frequently and provide granular rollback capabilities

Backup Policies

- Limit access to areas where valuable data and content are stored
  - Enable or deny permissions by:
    - Account
    - User
    - Specific elements, such as date, time, IP address, or whether requests are sent with SSL/TLS
- Use the principle of least privilege—only give users access to the accounts, systems, and data they require

Network Segmentation

- Limit data access
- Prevent lateral movement
- Defend Active Directory
- Segregate networks into distinct zones and require different credentials for each
- Implement Dynamic Access Control in Windows

Encrypt

- Encrypt metadata to make it more difficult to identify types of data stored in different applications
- Establish policies to encrypt data in transit and at rest

Logging and Versioning

- Use versioning to enable preservation, retrieval, and restoration of data
- Maintain access logs to provide an audit trail
- Create restore and recovery points

Rights Management

- Give users the lowest system permissions needed
- Turn off admin rights for users who do not require them
- Restrict write permissions on file servers
- Set up roles that do not allow certain users to delete any data and enforce no-delete rules by requiring a code to delete any version of data

Prevention | Content Protection

Backup is at the core of any content protection plan. Systems should be backed up locally and using cloud storage. The cloud backups provide redundancy and add an extra layer of protection. 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.

Backup Policies

- Have multiple backups in case the last backup gets overwritten with encrypted ransomware files
- Keep a backup of sensitive data offsite in data centers with strictly limited access
- Separate backups from production systems—not connected to the computers and networks they are backing up
- Backup frequently and provide granular rollback capabilities

Encrypt

- Encrypt metadata to make it more difficult to identify types of data stored in different applications
- · Establish policies to encrypt data in transit and at rest

Data Access Policies —for Internal and Remote Users

- Limit access to areas where valuable data and content are stored
- Enable or deny permissions by:
  - Account
  - User
  - Specific elements, such as date, time, IP address, or whether requests are sent with SSL/TLS
- · Use the principle of least privilege—only give users access to the accounts, systems, and data they require

Network Segmentation

- Limit data access
- Prevent lateral movement
- Defend Active Directory
- Segregate networks into distinct zones and require different credentials for each
- Implement Dynamic Access Control in Windows

Logging and Versioning

- Use versioning to enable preservation, retrieval, and restoration of data
- Maintain access logs to provide an audit trail
- Create restore and recovery points

Rights Management

- Give users the lowest system permissions needed
- Turn off admin rights for users who do not require them
- Restrict write permissions on file servers
- Set up roles that do not allow certain users to delete any data and enforce no-delete rules by requiring a code to delete any version of data

Prevention | Identity Management Policies

Impersonation persists as the most common entry point for cybercriminals. 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.

Strong Passwords

- Establish policies that require complex passwords—the National Institute of Standards and Technology's (NIST) Digital Identity Guidelines suggests no fewer than eight characters, and passwords should use mixed case letters, numbers, and special characters (e.g., P@ssw0rd$)
- Mandate that passwords are changed regularly—as frequently as every month
- Implement a password management strategy

Multi-Factor Authentication (MFA)—Require It everywhere

- Use this second validation or authentication method to provides another layer of protection
- Enhance logins with a credential from a physical token, a personal smartphone, or a unique biometric signature
- Ensure that even if an attacker gets their hands on a weak or stolen employee password, they cannot log in

Actively Manage Users' Accounts and Applications

- Eliminate accounts when an employee leaves, including access to:
  - Databases
  - Applications
  - Other repositories
- Ensure that all keys are rendered unusable
- Remove outdated or unnecessary programs from user devices
- Ensure that all software and firmware on all devices are updated and patched automatically

Prevention | Early Threat and Infection Detection

Monitor and analyze systems to detect suspicious activity. This allows for preemptive threat neutralization. Stop threats before they become attacks with these solutions.

- Utilize machine learning algorithms, bot detection solutions, and proxy analysis to detect and alert for unusual behavior—continuously
- Identify abnormal file sharing
- Monitor for anomalies, such as inconsistent file types
- Alert admins about irregularities
- Flag file extensions that have changed or contain known ransomware signatures
- Look for rapid, successive encryption of files
- Detect known ransomware using a "signature-based" approach

Entry-Point Protection

- Prevent unauthorized access using perimeter controls, such as firewalls, secure email and web gateways, and intrusion prevention/detection systems (IPS, IDS)
- Filter web content and block sites that may introduce malware
- Reject addresses of known spammers and malware
- Block unknown email addresses and attachments on the mail server
- Deploy anti-virus, anti-malware, anti-phishing tools at the end-user and email-server level—and keep them up to date

Prevention | Compute Layer Security

A secure compute layer ensures the availability of systems and data as well as keeps cybercriminals from using compute power to spread the ransomware further. Consider the following to reexamine and harden the compute layer, including mobile devices, and reduce attack surfaces.

- Assess and secure remote entry points with endpoint security software installed on external devices, such as laptops and mobile devices
- Apply software and OS patches as soon as they are available and keep service packs and patches up to date
- Delete stale DNS to protect against DNS protocol attacks, such as DNS spoofing, DNS ID hacking, and DNS cache poisoning
- Adjust hypervisor firewall rules to manage both ingress and egress traffic
- Enable secure login to keep assets protected when users move across unsecured networks by issuing SSH keys
- Deploy a VPN to protect connections between devices and the Internet
- Implement SIEM solutions to monitor and log network activity, then analyze log and memory data identify unusual activity on the system to pinpoint an attack
- Use a jump host (also known as a jump server) as an intermediary host or SSH gateway to a remote network when connecting to another host in a dissimilar security zone that is outside the firewall or in a demilitarized zone (DMZ)
- Set up viewable file extensions to identify executables, such as a .exe, vbs, or .scr
- Use Group Policy (in Windows) to block the execution of files from local folders
- Scheduled frequent security scans
- Uninstall PowerShell or, if it is required, track every single script that is running and monitor PowerShell closely with endpoint detection and response systems
- Block vulnerable plugins, such as WordPress related ones
- Limit Internet connectivity for highly-sensitive, critical data—in some cases, it may make sense to disconnect completely

Prevention | Cybersecurity Awareness and Training

Create a cyber-resilient organization with security awareness training to help employees learn to avoid ransomware and malware traps as well as recognize signs of an attack or potential attack. Invest in educational programs and regular training that teach employees about common ransomware delivery techniques and red flags. Consider the following recommendations for areas to focus on cybersecurity education and training.

- Provide easily accessible channels for reporting and getting help with suspicious activity
- Make it clear that anyone reporting suspicious activity does not have to be positive that a problem exists—better a false positive, since waiting until an attack is happening can mean responding too late
- Remind users that ransomware preys on their inattentiveness and that no technology can protect a system like human vigilance
- Warn employees about clicking links or attachments that come within unsolicited emails
- Institute a policy never to use public WiFi
- Stress the importance of examining links and attachments to make sure they are from a reliable source
- Ensure that users know not to click on executable files or unknown links
- Incorporate regular practical tests that entice users into clicking on would-be malicious links or downloads
- Keep users apprised of the latest malware and ransomware attacks
- Warn staff about the dangers of giving out company or personal information in response to an email, text, or phone call
- Teach users to recognize the signs of a phishing attack

Prevention | Use Red, Blue, and Purple Teams to Test Security

Simulated attacks help detect security weaknesses before cybercriminals do. Issues uncovered are often related to misconfigurations and coverage gaps in existing security products. When run with internal teams, the "attacks" also can enhance understanding and cooperation among the IT and security teams.

Red Teams

Red teams play offense. They are comprised of internal security professionals or consultants who are experts in attacking systems and bypassing defenses. They use real attack techniques to identify vulnerabilities across infrastructure, systems, and applications by performing vulnerability scanning and penetration testing. Red teams also ferret out weaknesses in processes and users' behavior.

Blue Teams

Blue teams take defense. They are usually the analysts and engineers responsible for maintaining the organization's security systems. Blue teams use a combination of threat prevention, detection, and response to thwart attacks by red teams. Blue teams receive no warnings about attacks and must react without preparation to demonstrate their defensive capabilities.

The Rise of Purple Teams

Purple team assessments can help an organization identify its vulnerability to cybercriminals' latest tools and tactics. These assessments help to improve threat hunting, monitoring, and incident response.

Unfortunately, red and blue teams often do not work together, since blue teams are mostly internal and red teams are consultants. In these cases, the blue team does not get continuous feedback or an opportunity to engage with the red team. This is a lost opportunity to improve overall operations rather than uncover issues.

Companies form purple teams that bring red and blue together to share insights and develop a feedback loop and knowledge transfer to resolve this. Purple has red and blue teams work for a common cause rather than as adversaries.

> All organizations should consider red, blue, and purple teams a must-have regardless of size, industry, or resources.

Prevention | Ransomware Insurance

Another defensive move that companies are making to minimize the risk of ransomware is cyber liability insurance. Ransomware insurance is a cyber liability specialty insurance that offers damage protection should an attack occur. It protects businesses and related individuals. Ransomware insurance is meant to reduce the financial burden of recovery after a ransomware attack—restoring data and dealing with stolen or leaked data. Also, while paying a ransom is frowned upon by security experts and law enforcement, ransomware insurance can cover that cost.

Remediation

Remember the "five Ps"—**Prior Planning Prevents Poor Performance**. Have a plan in case a ransomware attack occurs. With ransomware, prior planning and the plan's efficacy can determine an attack's impact. Expedite neutralization and reduce the lifecycle of an attack by considering the following as part of remediation planning.

Remediation | Continuity Planning

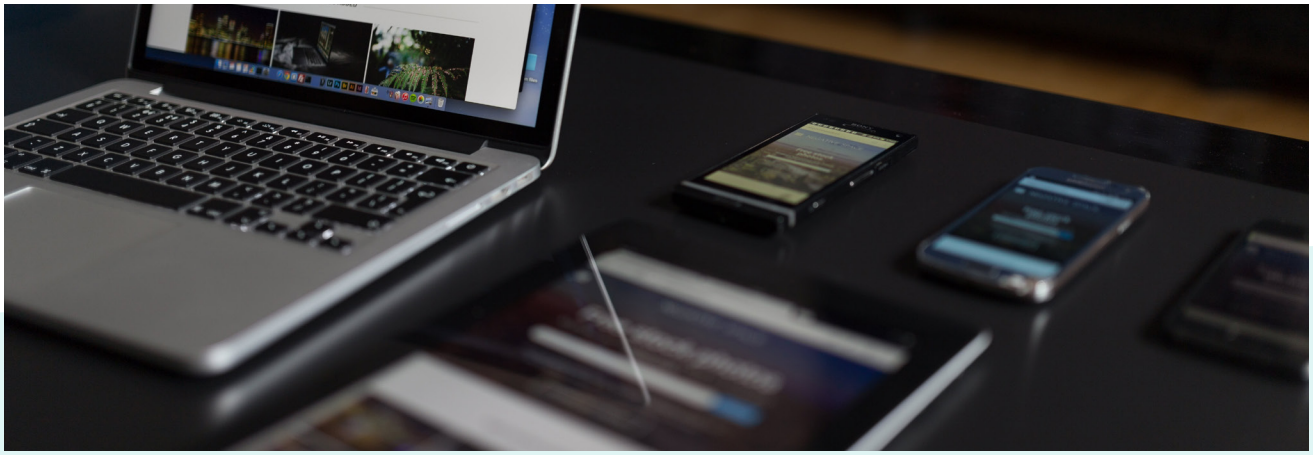
A continuity plan plays a critical role in ransomware remediation. It should explain, in detail, what steps to take to resume operations as quickly as possible. The plan should include different responses based on threat levels. And, the plan should be tested regularly to incorporate updates and ensure preparedness.

High Threat Level	Ransomware has been successfully deployed and poses a direct threat or suspicious activity points to an immediate threat.
Medium Threat Level	Ransomware has been detected on an endpoint, but does not pose an immediate threat, or suspicious activity has been flagged for review to determine if it is a threat.
Low Threat Level	Unwanted software, such as adware, has been detected. It can cause issues, including changing browser settings, redirecting search results, and displaying ads. The problem should be addressed, but it does not warrant an accelerated response.

For each threat category, develop an incident response team that will follow remediation guidelines based on the kind of ransomware attack and its severity.

First responses should include:

- Block all affected user accounts to contain ransomware before it spreads
- Identify every encrypted file
- Trace the ransomware infection back to its source
- Analyze the extent of the damage
- Consider remediation options



Remediation | Common Post-Attack Mistakes

Review these common mistakes in handling a ransomware incident to help avoid them.

Restarting Infected Devices

A restart could result in retaliation. Often, ransomware detects attempts to reboot and penalizes victims. These penalties include corrupting the device's Windows installation so that the system will never boot up again and deleting encrypted files at random. Also, rebooting clears the machine's memory, eliminating information that could be useful for future analysis. It is best to put the system into hibernation, so all data saved in memory.

Connecting to External Backup Systems and Storage Devices

This gives the ransomware access to even more content. Only connect to backup systems and storage devices after neutralizing the ransomware

Communicating on a Network Impacted by Ransomware

Depending on the strain of ransomware, attackers could intercept communications sent or received on a compromised network. Until remediation is complete, use alternate networks or communication channels.

Never Delete Files During a Ransomware Attack

Some ransomware includes decryption keys in the infected files. If the file is deleted, the key is too, and the file cannot be decrypted. Also, files can contain information that is helpful for attack analysis.

Remediation | What to Do after Ransomware Detection

Isolate Systems Impacted by the Ransomware

Prevent the ransomware from spreading by disconnecting all infected devices from each other, shared storage, and the network—both wired and WiFi. This disconnection must be automated. When an infection is identified, infected files isolated should be automatically isolated, and any suspicious executables removed.

Also, remember the ransomware may have entered through multiple systems, and some of the ransomware may remain dormant. In the case that ransomware is detected, all connected and networked computers should be scanned.

Identify the Ransomware Strain

Generally, ransomware can be identified by the message that it presents. Understanding the type of ransomware used in the attack reveals propagation methods and targeted files. Knowing the strain of ransomware can also help select the best options for remediation.

It is also essential to determine if the ransomware includes persistence mechanisms. In this case, after the ransomware process is stopped, it will reactivate after a period of time or after a reboot. Knowing if the ransomware utilizes persistence mechanisms is critical. Without this knowledge, remediation is undermined.

Trace the Attack

Identifying the entry point of ransomware helps track its spread and, potentially, stop it. The attack can be traced from the last modified user account with information found in audit logs. Work backward, being sure to include remote users and partners to find the point of origin.

Report the Ransomware Attack to the Authorities

Many compliance regulations require disclosure in the event of a breach. A ransomware attack is considered a breach that must be reported to regulatory and law enforcement agencies. The FBI's Internet Crime Complaint Center should be alerted immediately, followed by local law enforcement. Disclosures to law enforcement help them track down the individual or group behind the ransomware attack and prevent future attacks.

Assess the Impact of the Ransomware Attack

Before launching into defensive and corrective action, stop to assess the damage and understand the situation in its entirety. Then, armed with information, make decisions about remediation.

Evaluate Ransomware Recovery Options

Ransomware recovery options come down to three choices.

1. **Pay the ransom.** As noted earlier, this is not recommended by security experts or law enforcement agencies. However, in some circumstances, it is the best of bad options.

2. **Attempt to remove the ransomware.** Some ransomware can be neutralized with a decryptor that has been created using information from prior attacks. For newer ransomware, the likelihood that a decryptor is available diminishes. Even with a decryptor, security experts question if it is even possible to delete the ransomware.

3. **Reinstall from the last clean point.** Starting from a clean point is generally accepted as the best solution to remedy a ransomware attack. However, according to a Forrester survey of IT infrastructure and operations decision makers, 54% responded that their backups are fragmented. Even when backups are pristine, the disruption caused by an organization-wide rollback increase exponentially with users' numbers.

A surgical rollback approach should be taken to reduce the impact and cost of the ransomware attack. Infected machines only should be rolled back to the last point in time before the attack.

Notify Affected Customers

Regardless of how unpleasant it is, sometimes, legal and compliance regulations require that customers be notified about a ransomware attack. If notification is needed, promptly explain the situation and the remediation plans. Expediency and transparency are always the best approaches and give customers confidence that the organization has the matter under control.

Plan to Prevent Recurrence

When the ransomware has been neutralized, and business operations are back to normal, the next round of work begins. A full assessment must be completed to understand how the ransomware entered, was activated, and what it did. This will help prevent future attacks. Red, blue, and purple teams are great resources to help with the ransomware attack analysis.

Monitoring and Maintenance

The prevention best practices outlined previously should drive monitoring and maintenance. These include:

- Content protection
- Identity management policies
- Early threat detection
- Compute layer security
- Cybersecurity awareness and training
- Continuity planning
- Ransomware insurance

Monitoring and maintenance should encompass both systems and content. **Regular monitoring** is mandatory, since ransomware does not adhere to a schedule. **Smart, continuous backup** is also a must and should provide the capability for nuanced rollbacks-by the user and by a specific time-to minimize data and productivity losses.

A World of Potential Solutions

There are many ways to attack the ransomware problem, and many vendors that will tell you their solution is best. However, there are pros and cons to every solution on the market, and the winners will need to deploy a comprehensive approach across multiple vectors of defense. To help you understand the market, we have detailed the major types of solutions and where they fit on the spectrum of defense.

Solution Type	Example Vendors	Prevention	Remediation	Monitoring & Maintenance
Anti-malware	McAfee, Bitdefender, Kapersky, Malwarebytes, Webroot, Norton, Checkpoint,	X		X
Identity & Access Management	Cisco Duo, Idaptive, Oracle, Okta, IBM, Ping, OneLogin, Symantec, Centrify, Microsoft Active Directory, VMware, LastPass, Optimal IdM, Bitium	X		
Endpoint Protection	Avast, ESET, Bitdefender, Trend Micro, Panda, Sophos, F-Secure, Kapersky, Vipre, McAfee	X		X
Multi-Factor Authentication	RSA, WatchGuard, Microsoft Authenticator, HID DigitalPersona, Duo, RSA, Authy, Google Authenticator, andOTP, LastPass	X		
Advanced Encryption	Folder Lock, AxCrypt, CryptoExpert, CertainSafe, VeraCrypt, NordLocker, CryptoForge, Steganos Safe, Cypherix	X		
Threat Detection & Response	CrowdStrike, CheckPoint, SentinelOne, F-Secure, Palo Alto Networks, Kapersky, Microsoft Defender, Trend Micro, VMware Carbon Black, Symantec, Bitdefender, Blackberry Cylance, Cybereason, Infocyte, ESET, Sophos	X	X	X
Backup & Recovery	IDrive, Arcserve, Backup Radar, Livedrive, Ashampoo, ElephantDrive, Carbonite, Acronis, SOS Online Backup, Backblaze, CheckPoint, SpiderOak, OpenDrive, Zoolz BigMind, StorageCraft, Paragon, NovaBackup, NovaStor, NTI, Retrospect, Synametrics, NAKIVO, Unitrends, AOMEI,		X	
Employee Training	Barracuda Networks, Cofense, HoxHunt, KnowBe4, Lucy, PhishLabs, Securementum, Proofpoint, Webroot			
Managed Security Service Providers (MSSPs)	Cipher, SecureWorks, IBM, Rackspace, Verizon, Symantec, Trustwave, AT&T, CenturyLink, AlertLogic, Rapid7, BlueVoyant	X	X	X

Vendor Evaluation Questions

Whatever solution direction you decide to go, you should employ a decision framework that analyzes vendors on four major areas: File Access, Threat Detection, File Protection & Restoration and Deployment & Support.

Use these evaluation questions when reviewing ransomware protection 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?

Conclusion:
Beating Ransomware by Protecting Content

A proactive approach to ransomware prevention can significantly reduce the risk of infection. However, in the event of a ransomware attack, planning is the best front-line defense. Effective response procedures expedite containment of the incident, prevent data loss, and streamline the recovery process.

Assessing security as it relates to ransomware 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. Securing content and proving granular access if a rollback is required ensures business continuity after a ransomware attack.

About Egnyte

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?

www.egnyte.com

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