IMPERVA®

E-BOOK

Insider's Guide to Defeating Ransomware: Protect Your Data at its Source

Content

Moving Onto the Most-Wanted List

As if your cyber security team doesn't have enough to worry about with serious threats such as distributed denial of service attacks and advanced persistent threats, now you need to add another class of cyber-attack to your list of top concerns. No longer content with small payoffs from consumers, cybercriminals are increasingly using ransomware to attack companies and organizations like yours.

Surging in popularity, ransomware is now the most profitable type of malware attack in history. Cybercriminals have discovered how financially rewarding–and easy to use–it can be, especially against larger targets with business-critical data stored on file shares. Consider this:

- Nearly 40 percent of businesses got hit by ransomware in 2015.[1]
- More than 2,400 complaints regarding ransomware were received by the U.S. Federal Bureau of Investigation (FBI) in 2015, with a reported loss of more than $24 million.[2]
- 4,000 ransomware attacks per day (a 300 percent increase compared to 2015) were seen in the first quarter of 2016.[3]

Don't underestimate the impact of ransomware across the organization as a whole. Even if only one endpoint is infected, ransomware can encrypt files both locally and on corporate file shares. This not only holds data hostage for the infected user, but also for all other users that need to access the compromised file store. An active ransomware attack can bring all business operations to a halt until systems and files are restored.

Given the speed at which ransomware impacts organizations, security teams need solutions in place to detect ransomware at the earliest stage possible. Monitoring access to data on corporate file shares in real time to detect suspicious file modifications is the most efficient and effective way to detect–and block–a ransomware attack on unstructured data stored in file servers.

This e-book sounds the alarm about the threat of ransomware for businesses and public sector organizations, equips security professionals with the facts about the risks and consequences of ransomware, and presents an approach to protect enterprise data from ransomware attacks.

Nearly 40 percent of businesses got hit by ransomware in 2015.

SOURCE: OSTERMAN RESEARCH

[1] "State of Ransomware," Osterman Research, August 2016.

[2] Anderson, Vicki, "Ransomware: Latest Cyber Extortion Tool," U.S. Federal Bureau of Investigation, April 26, 2016.

[3] Otto, Greg, "Ransomware attacks quadrupled in Q1 2016," FedScoop, April 29, 2016.

RAnSoMWarE

Ransomware offers quick and easy profits for hackers and can result in significant losses for victim organizations

$1 BILLION

FBI estimate for losses expected in 2016 due to ransomware

$17,000 ₿

Ransom paid in Bitcoin by Hollywood Presbyterian Medical Center to clear its network of a ransomware infection and regain access to vital patient files

$337,607

Ransom paid to cybercriminals via Bitcoin over the course of three CryptoWall ransomware campaigns during May, June, and July of 2015. This figure represents only a fraction of the total CryptoWall payments thought to have been received.

Sources: Herjavec Group, Imperva Hacker Intelligence Initiative, ZDNet.

Ransomware 101

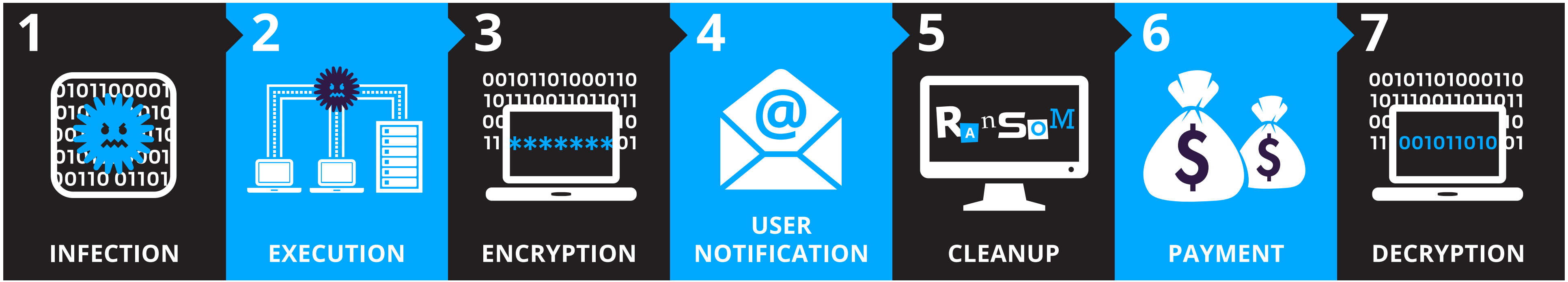
What is Ransomware?

Ransomware is a type of malware that holds data (or sometimes devices) hostage, typically encrypting files and rendering them inaccessible to end users. Cybercriminals demand payment from victims to regain access to the data or device.

How do ransomware infections happen?

- Phishing (93% of phishing emails now contain ransomware[4])
- Email attachments
- Infected programs
- Malicious advertisement (malvertisement)
- Self-propagation[5]
- Traffic Distribution Systems (TDS)[6]
- Drive-by infections on compromised websites

How does it work?



1 INFECTION

Ransomware runs on the infected endpoint.

2 EXECUTION

It scans and maps locations containing targeted file types. This not only includes locally stored files, but also mapped and unmapped network-accessible systems—including major file stores. Some ransomware deletes or encrypts any backup files and folders it has found.

3 ENCRYPTION

The ransomware performs a key exchange with the command and control server and uses this encryption key to encrypt all of the files it discovered while scanning.

4 USER NOTIFICATION

Once encryption is complete, the ransomware adds files that contain information about payment and decryption, then uses those files to display a ransom note to the victim with payment instructions.

5 CLEANUP

The ransomware usually terminates and deletes itself, leaving only the instruction files.

6 PAYMENT

Clicking on a link in the payment instructions takes victims to a webpage with further information about how to pay. Hidden TOR services are often used to encapsulate these communications in layers of obfuscation to avoid being discovered by network traffic monitoring.

7 DECRYPTION

Once a victim has paid the ransom, usually via an attacker's Bitcoin address, the victim may be given the key to decrypt the files. However, there is no guarantee that the cybercriminal will deliver the key as promised.

[4] "Q1 2016 Sees 93% of Phishing Emails Contain Ransomware," PhishMe, June 4, 2016.
[5] The malware spreads copies of itself within the network or via flash drives.
[6] A buyer and seller of web traffic generated from links on websites that sell the clicks on those links to a TDS. Some hackers have been known to buy traffic from TDS vendors.

Why are the number of ransomware attacks increasing?

1. Better encryption:

   The use of strong encryption methods makes it far more difficult for a victim to directly obtain the decryption key on their own.

2. Digital currency:

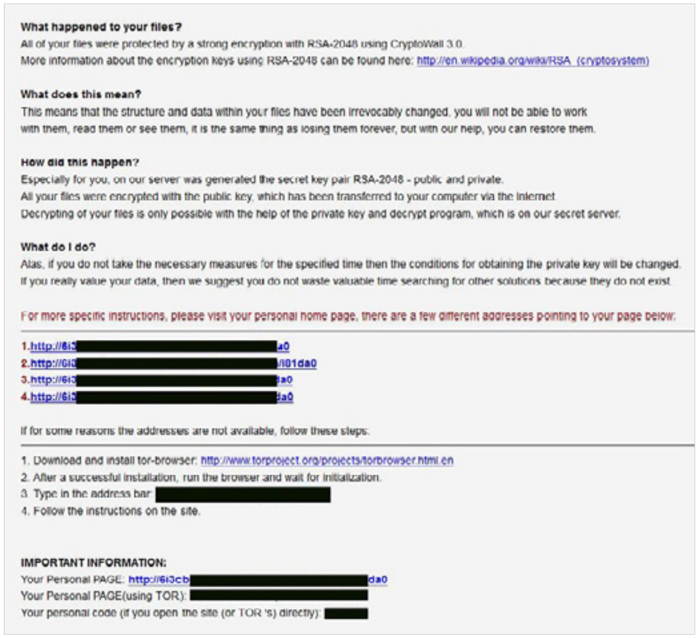
   Bitcoin and other digital currencies make it easier for attackers to get paid while remaining anonymous. Using Tor networks also helps maintain anonymity.

3. Ransomware-as-a-service (RaaS):

   Ransomware authors provide customized, on-demand versions of malware to distributors. The author collects the ransom and shares it with the distributor in a classic affiliate distribution model. With RaaS, ransomware attacks become accessible and profitable for any potential threat actor, which is helping drive an increased volume of attacks .

How do you know if your organization is infected?

Rapid file overwriting is one of the clearest markers of ransomware on your network. Monitoring access and modifications to data on your file servers in real time can help you stop the attack and contain the damage. Otherwise, as soon as ransomware finishes its activity, it will display a ransom note on the infected endpoint–at which point, it's often too late to prevent downtime and extensive remediation efforts.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http://6i3[redacted]a0
2.http://6i3[redacted]/i01da0
3.http://6i3[redacted]a0
4.http://6i3[redacted]a0

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: http://6i3cb[redacted]da0
Your Personal PAGE(using TOR): [redacted]
Your personal code (if you open the site (or TOR 's) directly): [redacted]

CryptoWall 3.0 Instruction Screen (Source: Imperva Hacker Intelligence Initiative)

Who is at risk?

Consumers, businesses, and public-sector organizations

Top sectors targeted:

38% Services (including technical, scientific, and professional services as well as healthcare, education, and arts and entertainment)

Manufacturing **10%**

Finance, insurance, and real estate **17%**

Public administration **10%**

Bringing Business to a Standstill

The damages caused by ransomware go far beyond the cost of paying a ransom (and it's not recommended that you do pay). In fact, the biggest impact to the business is downtime, which can easily stretch from hours to days or even weeks depending on the extent of the attack. Productivity and revenue losses alone can be substantial, not to mention the damage to brand or reputation that can occur during a prolonged business outage or interruption.

Additionally, organizations incur hefty costs to recover files, restore or replace systems and endpoints, and identify and remove ransomware infections from all affected endpoints. Without a way to detect and stop ransomware before it encrypts critical data, organizations can incur these costs over and over again as endpoints continue to become infected and corporate file shares held hostage.

To Pay or Not to Pay

It's tempting for organizations to pay the ransom as quickly as possible; however, that's no guarantee that you'll get your company's files or access back. In fact, in an alert dated September 15, 2016, the FBI states: "The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom."[8]

Paying a ransom also helps perpetuate the problem by incenting cybercriminals to expand their use of ransomware. It can also make your organization a greater target for cybercriminals because you've shown a willingness to pay.

The Cost of Ransomware

Source: Intermedia.

72% Companies affected by ransomware that could not access data for at least 2 days following an attack

32% Companies that lost access to their data for 5 days or more following an attack

[8] "Ransomware Victims Urged to Report Infections to Federal Law Enforcement," U.S. Federal Bureau of Investigation, Alert Number I-091516-PSA, September 15, 2016.

Understanding Why Common Security Solutions Aren’t Enough

Many organizations have inadequate protection against ransomware despite expending significant cost and effort to implement layers of security solutions that can help prevent and detect malware infections. With these tools in place, the security team receives automated alerts about suspected attacks and infections. In the event that a ransomware attack initially evades detection, best practices dictate that organizations have file backup and recovery systems to prevent data loss and reduce downtime.

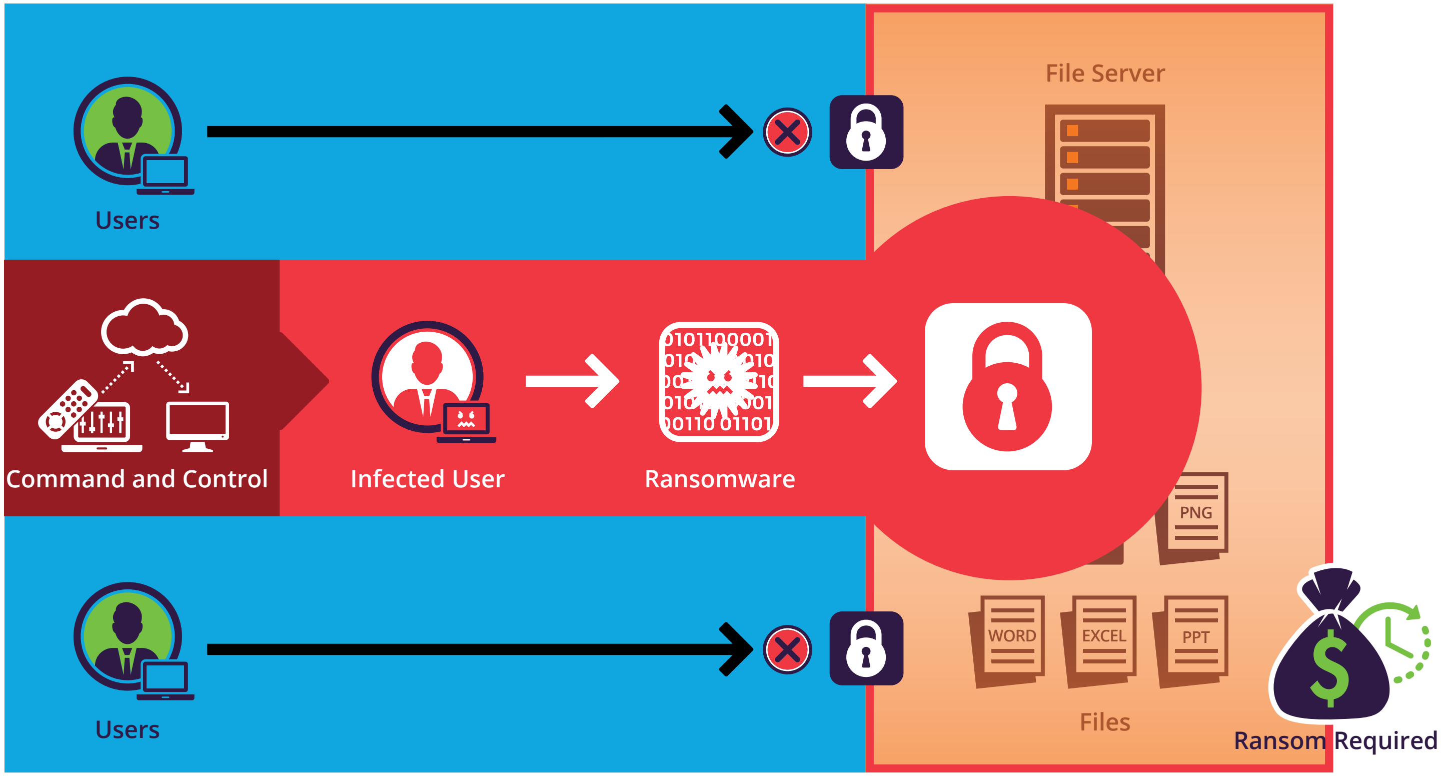
Unfortunately, these measures haven’t been all that effective at protecting companies from downtime and losses due to ransomware. Instead, many organizations have resorted to paying the ransom because their businesses have been crippled by the lack of access to critical data and devices.

Why—despite our best cyber security efforts—are cybercriminals able to use ransomware against us successfully? Here’s some insight into why standard defenses and after-the-fact remediation simply aren’t enough.

SECURITY SOLUTIONS	HOW RANSOMWARE WINS
Prevention-only solutions including anti-virus endpoint protection and advanced malware detection and prevention systems	• Signature-based endpoint protection can only detect malware that it already knows. Malware code changes very rapidly to evade signature-based detection. • While advanced malware detection/prevention solutions can help detect new and unknown malware using capabilities such as sandboxing, modern malware is aware of sandboxing technologies and has incorporated methods to evade it. • With widespread adoption of user mobility solutions and bring-your-own-device (BYOD) practices, end-user computing devices do not always benefit from corporate endpoint and network-based defenses. This leaves the organization susceptible to attack when these unprotected devices later connect to the corporate network.
Detection-only solutions such as SIEM systems and user behavior analytics (UBA) tools	• Analysis of event and traffic data can help identify potential threats, but can miss the signs of ransomware infection, providing false negatives and the illusion that everything is normal. • These solutions on their own do not take into account granular information about how users access files, which is essential to accurately pinpoint ransomware attacks while minimizing false positives. • Even when anomalous traffic or behavior is detected, it can go uninvestigated due to the sheer volume of alerts that security teams must handle and prioritize. Additionally, these systems do not offer mitigation, nor do they alert security teams to ransomware after the fact.
Response-only solutions such as file backup and recovery systems	• Your data recovery process can have gaps, such as infrequent backups or critical files missing from the backup plan. Despite the fastest, most problem-free recovery technology, organizations still face hours of costly downtime if backup and recovery is central to an organization’s ransomware mitigation plan. • Anticipating businesses’ response to ransomware, cybercriminals are adapting ransomware to look for backups on all attached drives and encrypt those as well. • Finally, measures that repair and respond after the attack don’t prevent attacks from happening over and over again in the future.

How Ransomware Infects a File Share

Without protections in place, ransomware avoids detection, infects an endpoint and then encrypts corporate file shares. Even if only one user is infected, all users are impacted because the files are rendered unusable.



Protecting Data at the Source

When it comes to ransomware, time is of the essence. The good news is that there is a more effective way to defend your organization. Real-time file access monitoring detects and blocks ransomware before it does widespread damage. It automates identification of ransomware based on file-access activity patterns and applies policies to block that behavior and protect your files.

Imperva SecureSphere File Security products deliver real-time file monitoring, detailed auditing, and security for files stored on file servers and network attached storage (NAS) devices. Imperva SecureSphere File Firewall offers a unique solution to combat ransomware by detecting and blocking infected users or devices based on file access behavior. It uses a combination of real-time capabilities to help security teams detect, block, investigate, and report on ransomware infections:

Real-time Alerting and Blocking:

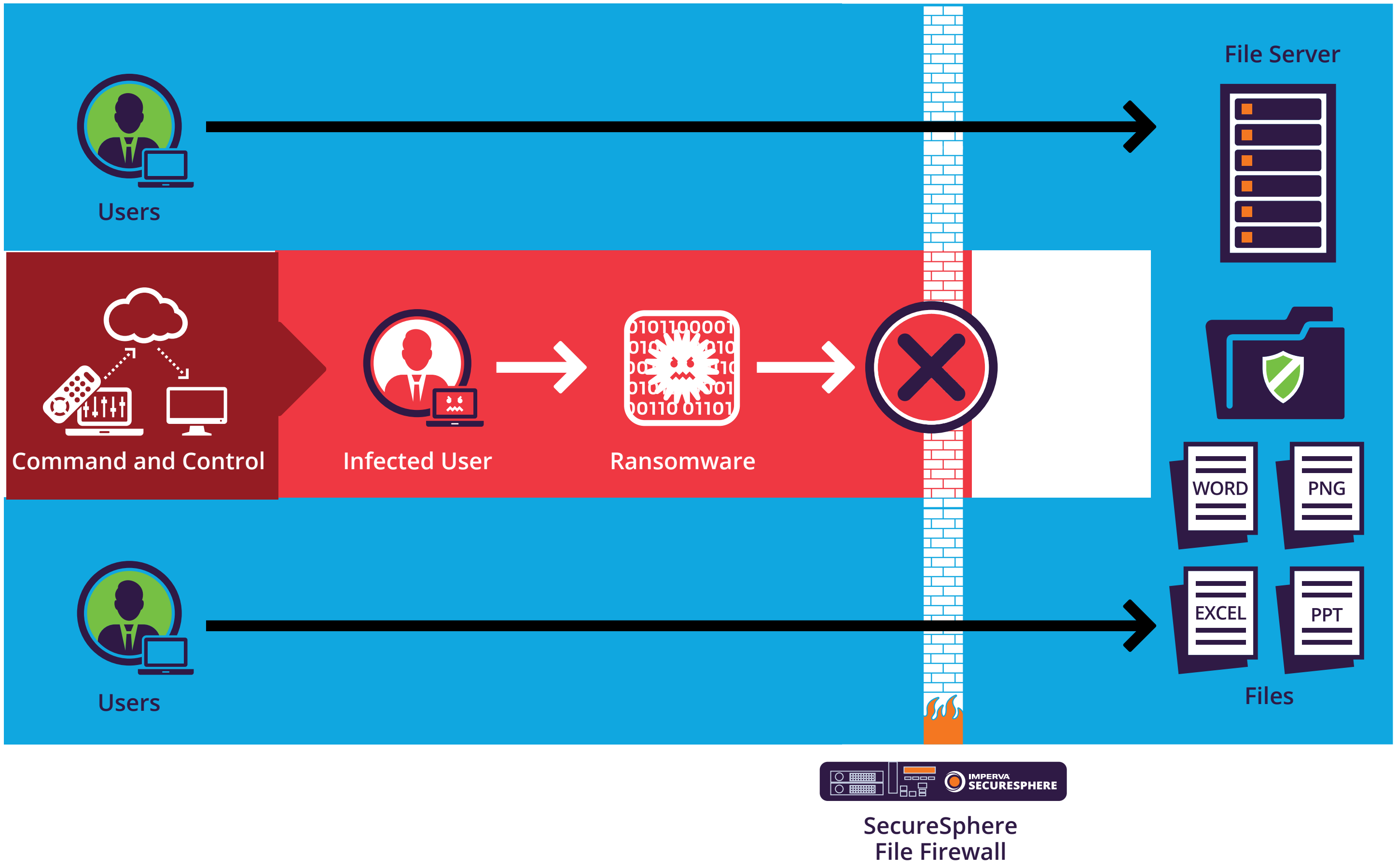
- Policy-based detection identifies ransomware-specific read/write behavior and blocks users and endpoints from further file access.
- Deception-based detection uses strategically planted, hidden files on file storage systems to identify ransomware at the earliest stage of the attack. Any write/rename actions on these hidden files trigger automatic blocking of the infected user or endpoint.

Granular Reporting and Analysis:

- A detailed audit trail supports immediate forensic investigation to answer who, what, where, when, and how users access files.
- Interactive audit analytics accelerate investigations, letting you quickly drill down into the audit trail.
- Easy reporting helps you document any security incidents.

How SecureSphere File Firewall Protects File Shares

SecureSphere File Firewall detects and blocks ransomware attacks before the file share is encrypted. The infected endpoint is blocked, while other users can continue to access files.



Essential capabilities for a real-time file access monitoring solution

- Real-time monitoring and analysis of user file access behavior
- Granular visibility into who, what, when, where, and how files were accessed
- Alerting when suspicious behavior is detected
- Detection and blocking of unauthorized/ransomware access
- Analytics to accelerate investigation of security incidents
- Backed by ongoing research dedicated to understanding how ransomware behaves

SecureSphere File Firewall

Real-time ransomware detection and mitigation

STEP 1 Monitor and Audit Activity

SecureSphere File Firewall monitors all user file access in real time. It also provides an audit trail of file access activity showing who, what, when, where, and how data was accessed.

STEP 2 Detect Ransomware-specific Behavior

SecureSphere File Firewall uses policy-based detection to identify distinctive behavior patterns associated with ransomware, such as rapid file overwriting and repeated use of the rename operation. Any user file access that violates policies triggers automatic blocking of the infected user or endpoint.

The solution also identifies ransomware with deception-based detection capabilities. This method leverages strategically planted, hidden files on file storage systems to identify ransomware at the earliest stage of the attack. Any write/rename actions on these hidden files trigger automatic blocking of the infected user or endpoint.

STEP 3 Block File Access

Once suspicious behavior is detected, SecureSphere File Firewall policies can restrict access to the file share by blocking access from endpoints and users with suspected ransomware infections. It also alerts administrators so that infected endpoints can be quarantined and the infection remediated.

Architectural Firm Prevents Millions of Dollars in Downtime

A Desirable Ransomware Target

One of the largest architectural firms in the U.S. stored 200 terabytes of work-in-progress files such as diagrams, blueprints, and 3D models in file shares on two network-attached storage devices.

Multiple Infections = Massive Productivity Loss

After malware infected a user's device within the organization, it accessed the file share, encrypting the majority of the firm's files and rendering them unusable. After remediating the infection and restoring the files, it happened again. The two major ransomware outbreaks eventually cost the company more than $500,000 in billable hours.

The Solution

To prevent ransomware from taking its files hostage and negatively impacting productivity in the future, the firm now has Imperva SecureSphere File Firewall for real-time monitoring of all user access to file shares. With Imperva, the firm can immediately detect ransomware and block attacks to protect the company's files.

Nearly 40 percent of businesses got hit by ransomware in 2015.

SOURCE: OSTERMAN RESEARCH

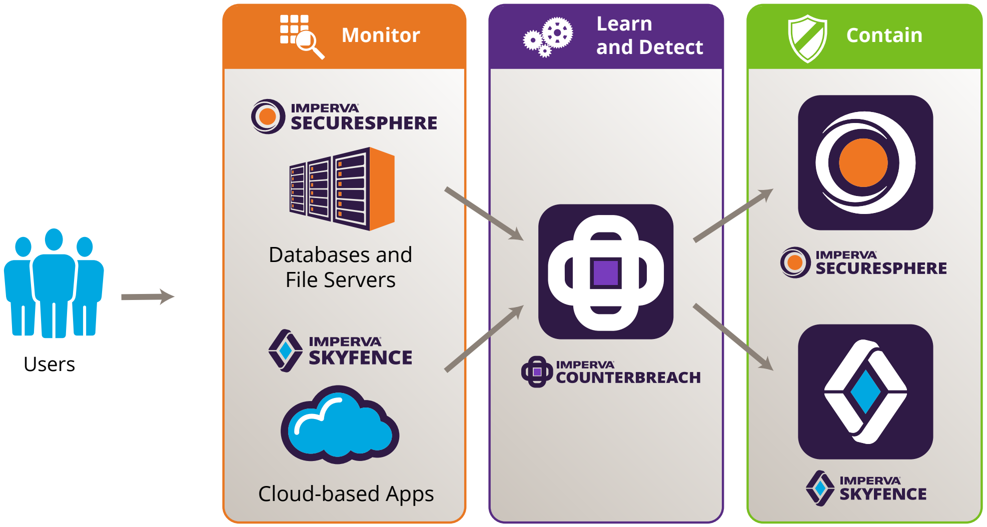
Extending Your Data Defense Beyond Ransomware

Protect Files from Insider Threats

While defending against ransomware is a critical capability, a real-time, file activity monitoring solution is also essential for mitigating other security threats. If a cybercriminal can successfully introduce ransomware into your organization, other security threats can get past your defenses and put the organization at risk.

In addition to being exposed to ransomware extortion, your business could also be exposed to data theft caused by malicious or careless insiders. It only takes one curious insider to jeopardize your intellectual property, financial data, business plans, and other business-critical data.

To safeguard organizations from the theft and loss caused by insider threats, the Imperva CounterBreach solution leverages advanced, machine learning technology to protect enterprise data stored in file shares, SaaS applications, and enterprise databases. By dynamically learning users' normal data access patterns and then identifying inappropriate or abusive access activity, CounterBreach proactively alerts IT teams to dangerous behavior. CounterBreach also uses deception technology to deterministically identify endpoint devices that have been compromised by external attackers, adding additional context to user-data-access learning. To learn more about CounterBreach, visit **imperva.com/breach-prevention.**



Learning More

Find out more about how to protect your critical and sensitive data against ransomware and other security threats against. Check out the following resources:

Webpage: SecureSphere File Firewall

Datasheet: Imperva SecureSphere File Security

White Paper: How Malware and Targeted Attacks Infiltrate Your Data Center

Playbook: Top 10 Indicators of Data Abuse

About Imperva

Imperva® (NYSE:IMPV) is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere, CounterBreach, Incapsula and Skyfence product lines enable organizations to discover assets and risks, protect information wherever it lives–in the cloud and on-premises–and comply with regulations. The Imperva Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the-minute threat intelligence, and publishes reports that provide insight and guidance on the latest threats and how to mitigate them.
Imperva is headquartered in Redwood Shores, California.

imperva.com

IMPERVA®