Ransomware is Here: What you can do about it?

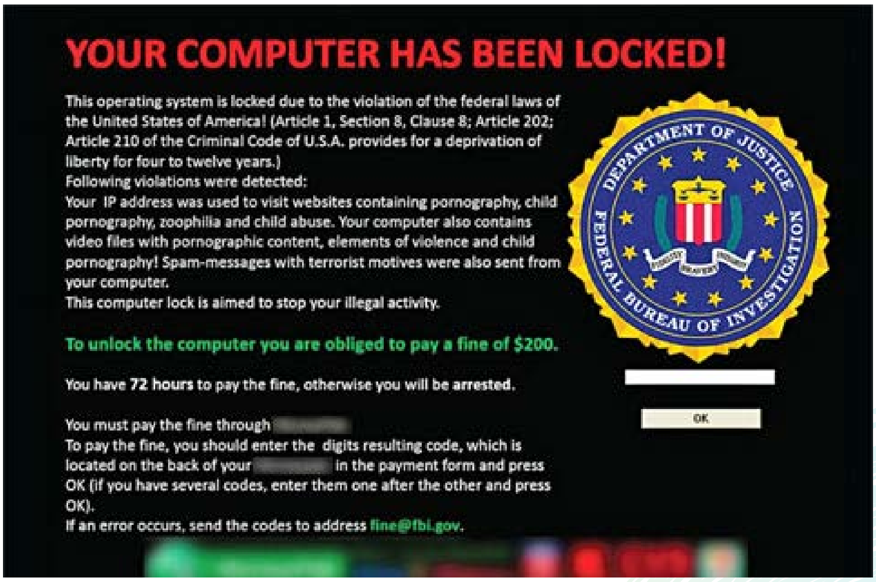
Whitepaper

SentinelOne

Overview

Over the last few years, ransomware has emerged as one of the most devastating and costly attacks in the hacker arsenal. Cyber thieves are increasingly using this form of attack to target individuals, corporate entities and public sector organizations alike by holding your system or files for ransom. Unlike other forms of cyber theft that often involve stolen financial or healthcare information, ransomware cuts out the middleman. In cases where an attacker steals health or financial documents, they must sell them on to third parties to make money. As far as ransomware is concerned, the money comes directly from the victim.

Ransomware is a quickly growing threat vector. According to the FBI's Internet Crime Complaint center (IC3), infected users made complaints about ransomware 2,453 times in 2015—nearly double the figure for 2014. What's more, these figures most likely represent only the tip of the iceberg, as many users pay their ransom without making a report to the authorities. A recent survey conducted by a Cyber Security Research Center at the University of Kent found that over 40% of those infected with CryptoLocker actually agreed to pay the ransom demanded, which is a big incentive for hackers to target more systems.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Fig 1. Reveton ransomware taking over an endpoint, with removal instructions

Lastly, hackers are rapidly iterating both malware and distribution techniques.
In early Q2 of 2016, a new variant of ransomware, known as CryptXXX, emerged on the scene. This program is packed in such a way that users and antivirus software may initially confuse it for a Windows DLL file. Further layers of code are deliberately designed to obfuscate the functionality of the program and thwart security researchers. According to research from SentinelOne, this functionality includes the ability to deliberately hunt down and steal bitcoin wallets, as opposed to simply waiting for a ransom.

CryptXXX has since evolved its abilities even further since detection. A new version of the virus now includes the ability to steal network access credentials and search for and encrypt shared drives attached to the initially-infected endpoint. The implications are ominous. Most ransomware authors don't know whether the data they're encrypting is actually of value to their targets. By adding the ability to spread in this manner, cyber-criminals have drastically increased their odds of winning a payday.

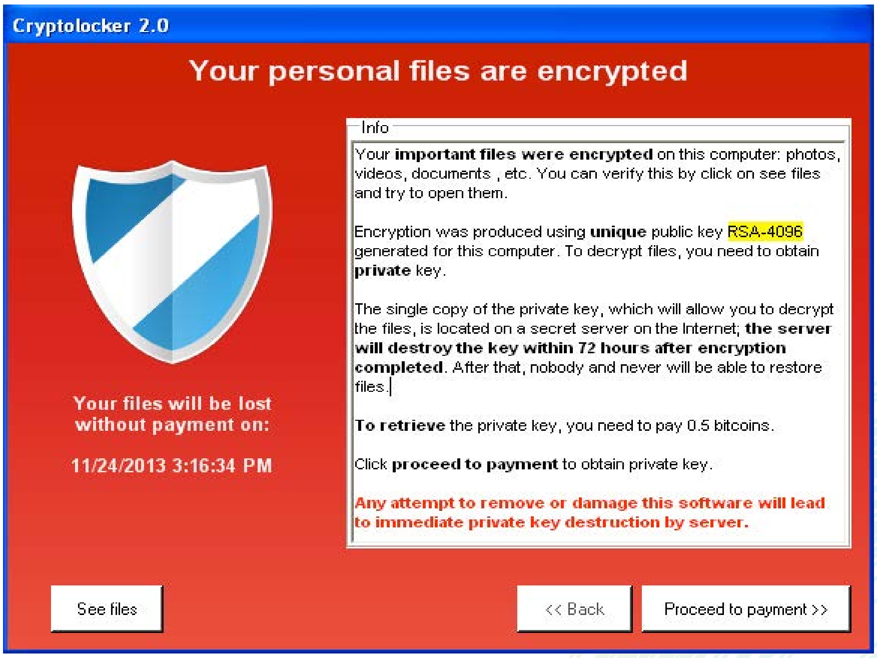
Other attackers are swiftly refining their toolkit in order to hit specific targets as well. SamSam, for example, bypasses the process of infecting users via a phishing attack or drive-by-download, and goes straight for unpatched vulnerabilities in JBoss. KeRanger diversified to begin infecting OS X users. Most ransomware is less creative than one might assume, given the breathless reports of its efficacy. However, even the most basic attacks have shown an alarming ability to bypass traditional security measures.

While many endpoint security products including traditional antivirus, host IPS, clustering and sandbox technologies have tried to prevent ransomware attacks, none of these solutions have been successful in preventing this latest form of attack. SentinelOne is the only vendor to provide "Next Generation" Endpoint and Server Protection to successfully detect and prevent ransomware-based attacks. We'll now discuss in more depth how ransomware works and how SentinelOne protects against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects a computer and takes control of either the core operating system using lockout mechanisms or possession of data files by encrypting them. The program then asks the user to make a "ransom" payment to the malicious individual or organization in order to remove the locks and restore the user's endpoint or files.

Less sophisticated malware simply locks the user out of the system, preventing them from logging in and accessing programs and data on their device. More advanced forms of ransomware will target specific data files such as sensitive documents, spreadsheets, PDF files, pictures and videos. These files are encrypted with advanced cryptographic techniques so that they become inaccessible for use. This more advanced mechanism may also traverse network shares and hold hostage data files that are present on shared drives and online file storage/sharing services. The malware will also use very long encryption keys making it virtually impossible for the user to circumvent the extortion demands. In either case, once infected, a computer or the data files cannot be used without the decryption key. In many cases, even when the ransom has been paid the ransomware will remain, lying dormant on the hard drive which makes this threat even more concerning.



Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

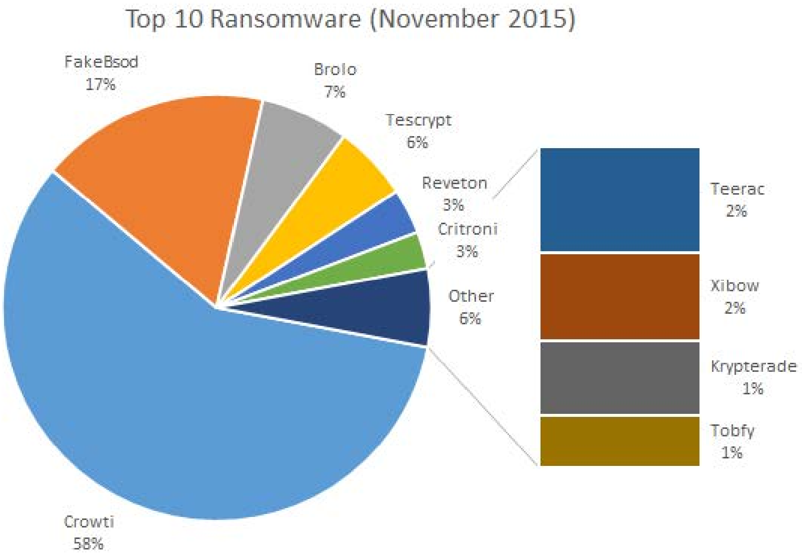
Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Fig 2. CryptoLocker is more sophisticated ransomware that selectively encrypts data files

TECHNIQUES

Every week appears to bring with it a new strain of ransomware. Although truly creative variants such as CryptXXX tend to stand out, the vast majority of new ransomware (and new malware in general) is merely an iteration of what has come before. Thus, most ransomware variants attack their targets using a few narrowly-defined methods.



SHOTGUN STRATEGY

While some ransomware has shown a nascent ability to seek out valuable data, and specifically target it for encryption, most malware has no idea what it's trying to hold for ransom. It could end up targeting vital patient records—or a couple of photos from the last company outing. With this in mind, hackers are going for volume, rather than precision.

Exploit kits are one way to hack users en masse. Criminals will typically purchase advertising space, allowing them to host banner ads on various sites. The ads themselves contain exploit kits, such as Angler, that execute inside a user's browser when they detect certain vulnerabilities. Angler then downloads and installs ransomware in turn. This strategy, known as a drive-by-download, can infect hundreds of people with just a single ad.

Spear phishing campaigns are another way to target either individual users, or large classes of users within a single enterprise. In a failure that speaks volumes about the effectiveness of security awareness training, many users will still download and enable macros on suspect Word documents. Other strains, such as Petya, may require users to enable User Access Control.

An emerging category of malware, including the previously-mentioned SamSam, finds specific unpatched vulnerabilities to exploit. They can use pen-testing tools to seek out known vulnerabilities. Given the ease with which other categories of malware are finding their targets, it's unclear as to whether this technique will ever become the norm.

And lastly, a more concerning infection technique is through compromised remote access servers. Hackers can launch brute force attacks to gain access to systems connected to the internet, and then use privilege escalation techniques to gain admin rights to servers with sensitive information. Once they have control of these high-profile systems, they can hold the data for ransom.

PERSISTENCE PAYS OFF

Most ransomware uses certain techniques that prevent both average and advanced users from ever reversing the infection. Although Petya has a relatively crude infection vector, it persists in a user's system by overwriting the Master Boot Record. Other malware hides out in traditional locations such as the registry.

Also of importance is preventing the user from ever restoring an infected endpoint to a pristine state. Ransomware will contain additional functionality, apart from encryption, to seek and destroy system restore files known as Shadow Copies. It will also disable Windows backup tools and mess around with other systems that may restore or defend the system's integrity, such as Safe Mode, Recovery Mode, and Windows Defender.

This behavior—disabling backups and crippling Windows—is clearly threatening, and yet most traditional endpoint protection fails to notice it. That's because most endpoint protection is signature-based. It tries to identify malware based on its file structure. Most malware authors, however, are wise to this method. They know that changing even a small detail of their programs will cause them to slip past traditional endpoint protection unnoticed—which is why, paradoxically, there's been little real innovation in evasion or infection methods.

SentinelOne changes the game by bringing in behavioral detection. Instead of trying to identify malware that may have been obfuscated using several techniques, it looks at what it's actually doing. Is a program creating new executables without authorization, disabling key windows features, or otherwise taking actions to perturb the integrity of a computer or server? Then it may be malware, and SentinelOne will chart this history of the suspect program as it goes through a network, allowing administrators to understand its attack path and reverse its changes at any point. SentinelOne offers next-generation protection on both endpoints and servers – both.

RANSOMWARE EXAMPLES

Some notable examples of ransomware are:

Reveton – This malware did not encrypt files, but rather blocked internet access with a fake law enforcement warning demanding payment to restore access. Reveton falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites and other illegal online activity.

CryptoLocker – This malware has surfaced in many different variations, and is one of the most recognizable examples of this ransomware attack. CryptoLocker was first reported in late 2013 and was one of the first to employ the encryption/ransom technique. Originally, it also claimed to only allow 72 hours before the decryption key was permanently deleted.

Cryptowall/Crowti – This is a recent CryptoLocker variant in this family, and Cryptowall first appeared in 2014. This variant employed more sophisticated attack methods and techniques to hide itself from traditional antivirus software. Cryptowall also attempts to delete shadow copies of files eliminating a common method of lost data recovery and thus making it even more damaging and resistant.

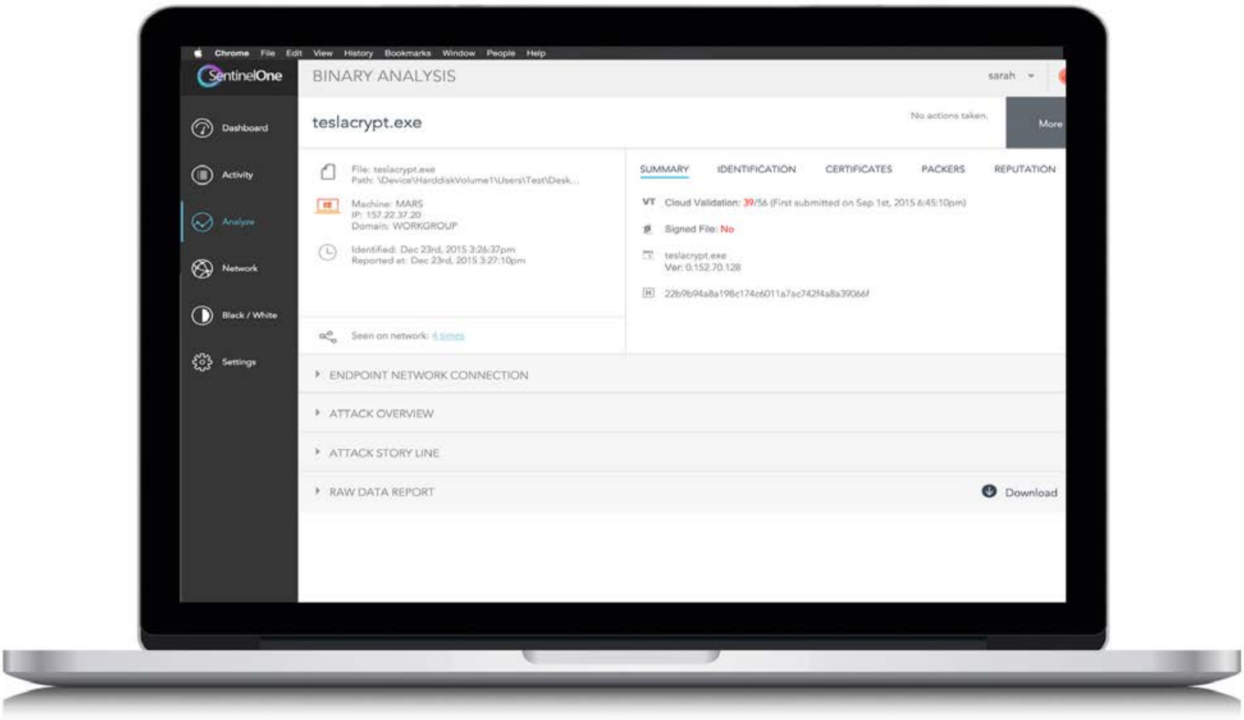
To decrypt the files and allow the victim to recover from an attack, these tools require payment using either cash cards or BitCoin. The threat actors mostly operate out of TOR websites in an effort to obfuscate their identities. Payments typically range from $200 to $500, although it is not uncommon for the extortion scheme to run into tens of thousands of dollars per victim. Once paid, a decryption key may be sent which is used to recover the locked system or files – although, as can be expected in a criminal enterprise, this is not guaranteed.

HOW DOES RANSOMWARE WORK?

Ransomware follows an attack pattern that consists of 5 steps. In most cases, these steps take less than a few seconds to execute. Even the most benign activities can result in the endpoint becoming a victim of ransomware, and your personal and/or business critical files becoming hostage to extortion.

Step 1: Targeting

Ransomware has primarily targeted endpoints running the Microsoft Windows operating system, although attacks targeting Mac OS X and mobile platforms are on the rise given their increasing popularity. Users in specific geographic regions like Russia, Brazil and of course the US have seen the bulk of ransomware attacks.



BINARY ANALYSIS

teslacrypt.exe

No actions taken.

File: teslacrypt.exe
Path: \Device\HarddiskVolume1\Users\Test\Desk...

Machine: MARS
IP: 157.22.37.20
Domain: WORKGROUP

Identified: Dec 23rd, 2015 3:26:37pm
Reported at: Dec 23rd, 2015 3:27:10pm

Seen on network: 4 times

VT Cloud Validation: 39/56 (First submitted on Sep 1st, 2015 6:45:10pm)

Signed File: No

teslacrypt.exe
Ver: 0.152.70.128

22b9b94a8a198c174c6011a7ac742f4a8a39066f

Because websites are a mechanism for the hackers to initiate the attack through hidden redirects and drive-by-downloads, hackers will also focus their attention on public websites running vulnerable web- or application-servers that they can leverage. This avenue is particularly dangerous if the hacker is able to find vulnerabilities in banking, online commerce or other payment websites.

Step 2: Propagation

Ransomware is usually propagated through the use of spear-phishing emails that have malicious attachments. These attachments are often Trojans in the form of MS Office or Adobe PDF documents, but have the ransomware embedded within them. Also common are websites hosting the malicious ransomware. Users are directed to these websites using fake pretenses and are victimized through "drive-by-download" attacks causing the ransomware to install itself on their device. Very often, ransomware seems to come from legitimate sources, including financial institutions, government entities or for corporate users, from someone within their organization. This could be in the form of email or websites. Some examples that hackers have used include pretending to be the FBI, the IRS and multinational banks.

Step 3: Exploit

Many hackers today use malware packaged into exploit kits that they covertly place on legitimate websites, or host on fake websites designed to look like a legitimate site. When a potential victim's browser lands on a website hosting such an exploit kit, the kit probes the visitor's system and extracts information like OS, browser type, version information and applications installed to find and exploit vulnerabilities. Once the exploit kit has found a security vulnerability that it can exploit, the attack proceeds to the next step.

Step 4: Infection

In the infection stage, the previous steps are used to download and install a "payload" to the victim's endpoint or mobile device. This payload could be the actual ransomware itself, or it could also be a hidden malicious downloader like Upatre which then creates a backdoor through which multiple types of malware can be downloaded and many different attacks can be executed.

Step 5: Execution

Once the ransomware has been installed on the victim's endpoint, the actual execution of the malicious program starts doing what it is designed to do – which is disable the system's critical operation or find and encrypt the data files on the endpoint. At this point the disruption directs the victim to the hacker's monetization mechanisms with instructions on where to send the ransom, in what form to make the payment (usually BitCoin) and other details to ensure the victim complies with the hacker's instructions.

WHAT CAN YOU DO IF YOU'RE INFECTED?

Ransomware follows an attack pattern that consists of 5 steps. In most cases, these steps take less than a few seconds to execute. Even the most benign activities can result in the endpoint becoming a victim of ransomware, and your personal and/or business critical files becoming hostage to extortion.

1. **Alert law officials.** They probably won't be able to help, but like any ransom activity, they should be informed.
2. **Isolate the infected machine**. It's important that the system is taken offline, as they essentially own your machine now and can use it to gain access to other systems on the network.
3. **Don't pay the ransom.** As with any form of ransom, you are not guaranteed to get your data back, and you're just encouraging attackers to keep up their lucrative game. In addition, if you pay and actually get your keys once, you may be the target of a repeat (and potentially more costly) ransom attack in the future.
4. **Remediate.** Run endpoint security software to discover and remove the ransomware software. If it cannot detect the threat, wipe your machine.
5. **Restore.** Restore your files with the most recent back-up.

SentinelOne: the ultimate ransomware defense

It is obviously best to prevent the ransomware attack from occurring, as recovery is difficult. SentinelOne is the only endpoint and server security software that protects against unknown forms of ransomware. SentinelOne's uses a groundbreaking Predictive Execution Inspection Engine that goes beyond file based analysis – even mathematical algorithmic analysis – that observes the actual execution of every system process or thread, in real-time. By understanding the execution behavior of all applications, programs and processes in real-time, SentinelOne provides the ultimate defense against ransomware.

SentinelOne provides the following features for protection against ransomware:

- **Real-Time Behavioral Detection:** SentinelOne is focused on real-time code execution rather than static markers for threat detection. This execution engine is able to monitor all endpoint processes, add full context for every process and then predict advanced and hidden ransomware attacks based on the execution behavior of the suspicious software. The focus on process execution can find and prevent ransomware that evades static detection techniques, and remains hidden to most other security products.

- **Predictive Execution Inspection:** Unlike static filters that analyze files and persistent elements of the ransomware, SentinelOne's Execution Inspection engine allows and monitors limited execution of all suspicious software, including memory-based and script-based ransomware to understand its behavior. We are able to detect and respond to what is happening on the endpoint as it happens. This allows SentinelOne to find extremely advanced ransomware that does not have any disk or file activity, that does not leave any indicators of compromise and that uses sophisticated embedding techniques to mask its activity.

- **Cloud Intelligence:** Cloud intelligence extends the protection of SentinelOne to block known threats using a unique approach called "passive scanning". The SentinelOne agent constantly monitors every file and process on the endpoint or server and sends file information to the cloud intelligence reputation service where it is scanned in real time by dozens of scan engines and leading reputation services. When a known threat is detected, it is immediately blocked before the user is exposed to any risk.

- **Kernel-Space Operation:** The SentinelOne agent operates in the kernel-space. This allows SentinelOne to perform the protection, detection and response with an extremely small footprint compared to other products. In addition to the performance advantages, the SentinelOne agent provides protection from all vectors while being highly tamper resistant to ransomware attempts that try to evade or disable the agent.

- **Roll-back:** Ransomware among other forms of malware specifically relies on encrypting or obfuscating system and data files as an attack vector. Many of the sophisticated ransomware variants being used today go one step further and eliminate the victim's ability to recover encrypted data by destroying the "shadow copies" created by the operating system. These shadow copies are used in data recovery operations by IT professionals as well as the OS itself e.g. when it recovers from critical system failure. SentinelOne is the only solution that saves and protects the shadow copies of data files, making it uniquely capable of helping victims recover from a ransomware infection.

- **Automatic Response and Mitigation:** SentinelOne is the only solution that provides full Endpoint and Server Protection as well as Endpoint Detection and Response (EDR) in a unified platform. Our ability to provide a single product that covers detection, prevention and response is unique. We have been certified against AV-TEST and are a true replacement for all endpoint and server security products – including traditional antivirus as well as newer security products.

- **Broad Platform Support:** While ransomware largely targets Windows based endpoints today, other platforms particularly Mac OS X and mobile OSs are becoming more common targets. In addition to Windows, SentinelOne supports Mac OS X, as well Android and iOS mobile devices, providing device coverage across the endpoint attack surface area. SentinelOne also supports Windows and Linux servers.

CONCLUSION

Individuals and corporations alike are struggling with the problem of ransomware. Users continue to bridge the gap between "personal" and "company" devices, and BYOD policies make accessing all kinds of data from any device a reality. At the same time threat actors are pouring their energies into developing increasingly advanced techniques to evade legacy defenses that rely on static signatures as well as new, seemingly innovative solutions to endpoint protection. The only way to ensure ransomware does not hold your device or data hostage for extortion is by using SentinelOne's Endpoint Protection Platform and Critical Server Protection Platform.

SentinelOne

With intelligent automation becoming an obvious replacement for signature-based detection, SentinelOne offers a comprehensive solution for servers and endpoints. SentinelOne offers a lightweight solution secures endpoints and servers without compromising performance. Behavioral threat analysis that leverages machine learning to capture and neutralize both known and unknown threats, while providing a forensics package that allows administrators to visualize attack paths and remediate vulnerabilities.

In terms of compliance, behavioral threat analysis also removes some of the necessity of patching systems to their latest version. While this is best practice, oftentimes updating one system will break the dependencies of its connected subsystems—meaning that administrators must trade a functioning network infrastructure for security and compliance on the other. Organizations can rely on SentinelOne to monitor unpatched systems, meaning that even an out-of-date program retains its security.

In terms of mitigation, SentinelOne can block and identify malware, even if it hasn't been seen before in the wild. In Alert Mode, it can identify malware, such as ransomware, and detect malicious behavior, such as creating an executable file without permission. SentinelOne will display the entire attack path of malware—and then enable administrators to seamlessly rollback an infected machine.

With SentinelOne, IT teams finally have a viable path forward that allows them to stay ahead in the arms race against bad actors. Instead of spending limited time, money, and manpower remediating breaches that are already in progress, security practitioners can now usefully devote their time to reinforcing the solid foundation which SentinelOne provides.

For more information about SentinelOne, please visit www.sentinelone.com.