**CloudBerry** Lab

#1 Cross-Platform Cloud Backup

# The **Value of Backup** in your **Ransomware Protection Strategy**

# The Value of Backup in your Ransomware Protection Strategy

The fear of every IT organization is being hit by a strain of malware so intrusive and effective in its design, it is not just disruptive, but downright damaging to IT, to the productivity of the organization, to the revenue generated, and to the organizations reputation. It used to be that only external attacks had the power to devastate companies, but in recent months and years, ransomware has shown itself to be a powerful adversary.  Sure, there's the ransom – that can range (depending on which article or analyst briefing you read) from a few hundred to tens of thousands of dollars. But, that's not where ransomware really hurts.

FedEx recently acknowledged the ransomware hit on their Dutch subsidiary TNT Express that occurred in June 2017 has cost the worldwide shipper nearly $300 Million in damages. The massive number is made up of the loss in shipping volume, and the resultant revenue and profit. While your organization may not be FedEx-sized, the impact of a single ransomware attack can bring productivity to a halt, cause service outages, reduce revenue, and cause reputation damage that will far outlive the news of the attack.

## Ransomware: Everyone's at Risk

If you're new to the game, ransomware is a form of malware that encrypts anything from specific files up to, and including, entire systems – holding them for ransom (usually paid in bitcoin). It started with attacks impacting single endpoints, but with the advent of ransomware using a set of exploits developed by the NSA that allowed malware to leverage SMB connections to spread between systems, ransomware has become a full-fledged threat.

Today, ransomware is truly a criminal business. Organizations authoring ransomware are keenly aware of the value of the machines and data they are encrypting. Nearly every industry vertical is a target and has been impacted (see below).

| | Industry sector | % attacked with ransomware |
|---|---|---|
| 1. | Education | 23 |
| 2. | IT/Telecoms | 22 |
| 3. | Entertainment/Media | 21 |
| 4. | Financial Services | 21 |
| 5. | Construction | 19 |
| 6. | Government/public sector/defence | 18 |
| 7. | Manufacturing | 18 |
| 8. | Transport | 17 |
| 9. | Healthcare | 16 |
| 10. | Retail/wholesale/leisure | 16 |

As demonstrated by the FedEx story, the real cost isn't the ransom itself (which organizations may or may not pay); it's the impact the infection can have on operations and, therefore, the business.

*So, how can you protect your organization from Ransomware?*

In this whitepaper, we'll outline what your ransomware protection strategy should look like, highlighting the value of having a solid backup and recovery plan to ensure you can get the organization back into a state of operation as quickly as possible.

# Building a Ransomware Protection Strategy

If you were to outline what you want to accomplish with a ransomware protection strategy, the obvious focus is to keep it from ever infecting the organization. But, in reality – as this whitepaper will show – the greater focus needs to be on eliminating the impact of ransomware within the organization. In some cases, you will be able to keep ransomware from ever entering in. But your protection strategy needs to be humble enough to entertain the possibility that ransomware will get through any defenses you stand up, requiring reactive steps to minimize the impact of any encrypted data and systems.

Think of your protection strategy as providing a layered defense in three parts: Prevention, Detection, and Response. Each part of the strategy may utilize a number of methods, as shown below.

| Prevention Methods | Detection Methods | Response Methods |
|---|---|---|
| Whitelisting | Antivirus | Ransom Payment |
| URL Blocking | Next Gen AV | Malware Removal |
| Email Filtering | | Backup and Recovery |
| Sandboxing | | |

The three parts exist because, as you'll see, the assumption should be that somewhere, sometime, ransomware is going to get through. Let's look at each part of the strategy.

## Prevention

This part of your strategy focuses on attempting to stop ransomware from ever running. URL blocking keeps users away from compromised websites hosting malware-laden code, email filtering scans attachments and links within emails for potential threats, and whitelisting limits what processes can run on an endpoint to only those that are approved. Sandboxing is a method where email links and attachments are tested to look for any malicious behavior, such as attempting to run or install software.

Some challenges exist with all four of these prevention methods. Tactics like URL blocking and email filtering rely on historical data to identify new ransomware variants. And ransomware authors know this, using polymorphic malware (where the ransomware evades detection by constantly changing its identifiable features) or evasive malware (where the ransomware looks for virtual environments) to keep from being detected by email filtering. Similarly, leveraged malicious URLs are constantly changing so that the latest IP address or compromised website lists may not be part of a security solution's current threat database. Even application whitelisting can be defeated using direct memory injection techniques that bore out existing known processes in RAM to host malware.

None of this means you shouldn't have prevention as part of your strategy. Quite the contrary – having a layered set of preventative solutions helps to keep the majority of ransomware out.

## Detection

Should preventative measures not stop ransomware from reaching an endpoint, it's important to have a means in place to detect when ransomware attempts infection. Antivirus solutions provide signature, heuristics, behavioral, and machine-learning detection to identify ransomware. "Next Generation" AV (NGAV) solutions dive deeper, watching process spawning and changes within the OS, looking for abnormal behaviors.

The challenge with both of these types of solutions is that, at their core, they are historical-based. Even the most advanced techniques have a basis of some infection that occurred in the past. So, when a new zero-day attack hits that does not behave like any ransomware variant before it, or when evasive malware senses the presence of AV and simply does not run to avoid detection, these solutions can be eluded.

Like preventative measures, detection is critical, as the endpoint is ground zero for a ransomware infection. While it's possible to avoid detection, at some point, ransomware has to fit a behavioral profile (that is, it will encrypt lots of files or an entire file system), making these solutions still viable.

## Response

Despite the best of prevention and detection strategies, mature IT organizations have a response plan in place. With the average ransomware attack infecting 6 workstations and 2 servers* , it's necessary to have a plan that covers whether to pay the ransom or not, removal of malware from the infected endpoints and, if needed, recovery of endpoints and data.

*KnowBe4, Endpoint Protection Ransomware Effectiveness Report (2017)

## Paying the Ransom

This is largely an issue determined per-organization. Some companies have a strict policy not to pay ransoms, while others determine the cost to repair the damage done versus paying the ransom. Do keep in mind that, with ransomware-as-a-service existing today allowing anyone to infect your endpoints, the idea that your decryption key will be valid, or that the decryption will work flawlessly isn't always sound. The possibility exists that there is no key available, and that the decryption may not work. Keep this in mind as you prepare your response plan.

## Malware Removal

Just because the ransom gets paid and the decryption runs perfectly, the problem isn't solved! That endpoint still has ransomware on it! You need a plan of how you will remove any remnant of the ransomware. This includes files, registry entries, browser plug-ins, etc. In reality, it may be a better plan to simply reimage the machine entirely.

## Backup and Recovery

The entire exercise of having a ransomware protection strategy revolves around the idea that each layer of protection proceeding it fails and ransomware is successful. If you are to follow that logic through to completion, you must conclude it is possible that, in a successful ransomware attack scenario, the ransom is too high to pay, the decryption fails, or the ransomware can't be properly removed from the infected endpoint. In each of these three outcomes, it will be necessary to recover the infected endpoint completely.

*So, how do you create a backup and recovery strategy that ensures you can recover from ransomware?*

# Creating a Ransomware-Ready Recovery Plan

IBeing able to recover from a ransomware attack is a bit tougher than one would think – you have no idea which endpoints will be impacted, how critical those endpoints are to the business, and whether specific files, an entire partition, or the entire machine will be encrypted. So, it's necessary to have a plan in place.

## Planning is the Key

The most effective planning results when you play a ransomware attack backwards. Consider which workstations, servers, and data sets are critical to the operation of the business. If not sure, involve the executive team, line of business owners, and application owners, asking what data can the business not afford to do without. Then establish backup types (e.g. file- or image-level) and backup frequency (which determines the recovery point in the event of an infection) for each system and data set.

It's likely you already have some of the server-side systems and data sets backed up, making this largely a double-checking exercise on the server side, and more a focus on which workstations and laptops need to be protected.

Consider whether these systems need to be backed up locally or to the cloud. In cases of laptops, consider using the cloud, so as to facilitate the possibility of recovery, regardless of where the user is physically.

## Test Recovery

TLike any good recovery plan, it requires testing to ensure success. Periodic testing of backups is relatively easy if done at an image-level; simply recovering to a virtual environment, booting up, and logging on will give you a solid indicator of whether a backup – and, therefore, recovery – is successful.

### Knowing How Far Back to Recover

One of the greatest challenges today – and a question often asked when discussing recovery after ransomware – is determining exactly how far back to go in your backup sets to recover. Most ransomware authors aren't interested in lying dormant, as it generates no revenue for them. They are interested in exploiting the successful infection as quickly as possible.

Even so, does that mean you can simply recover yesterday's backup? It's tough to tell. You obviously don't want to go back too far, as it can potentially outdate a workstation, its connection to a Windows domain, the most recent sets of local file data used by a user, etc. And since the ransomware got past all your security measures, checking with them seems rather useless.

What's needed is a way to identify when data has significantly changed. Some backup solutions offer an ability to detect, in essence, when ransomware has encrypted (read: modified) large numbers of files – a clear indicator of the presence of ransomware, and a marker denoting the previous backup should be used.

# Protecting from Ransomware: From Blocking to Backup

Ransomware is a threat that is only growing, becoming more intelligent, intrusive, and negatively impactful. It represents perhaps the single greatest threat to organizations in the near future, already growing well into the billions of dollars in damages annually.

Every organization needs a proactive protection plan in place, ready to thwart off ransomware attacks from ever entering in, stopping those that do make it past your external security layers of defense, and a backup and recovery plan – as part of an overall incident response plan – ready to bring the environment back into a state of operational readiness at a moment's notice.