2 Steps to Close the Gap in Ransomware Defense

Ransomware is a global epidemic that is spreading like wildfire. According to the 2019 CyRiM (Cyber Risk Management) Report, ransomware could cause $193B in economic damage.

The FBI estimates that ransomware infects more than 100,000 computers a day around the world. According to the 2018 Internet Organized Crime Threat Assessment by EUROPOL (European Union Agency for Law Enforcement Cooperation), "Ransomware remains the key malware threat in both law enforcement and industry reporting." Remember, in 2017, how the WannaCry worm wreaked havoc around the world causing an estimated damage of over $5B[1]? Well, it continues to be a threat—"WannaCry infections are still spreading in Asia Pacific"[2]

Organizations can easily neutralize the threat with a 2-step approach where we first strengthen protection against intrusions, if the virus manages to get through, we quickly resolve the issue with an up-to-the minute copy of the data ready for restoring our systems back to operational status.

Dynamic Ransomware Landscape

Ever since ransomware appeared, there has been an ongoing evolution of attacks, which target different IT system vulnerabilities with increasingly creative and/or sophisticated techniques. Why? It is because ransomware is a very profitable business. According to a ZDNet report, "The cyber gang behind the SamSam ransomware have netted almost $6m since they started distributing the file-locking malware in late 2015—and their profits are still on the rise, netting around an additional $300,000 each month."

In fact, RaaS (Ransomware as a Service), which allows cyber criminals without much software development experience to launch attacks, is available on the Dark Web. This will further drive the proliferation of ransomware. In a world of escalating attacks that are diverse in nature, organizations are constantly fighting an uphill battle to keep up.

In the case of WannaCry, which exploits vulnerabilities in Windows and was launched in May 2017, Microsoft actually released a security patch (MS17-010) addressing such flaws in March 2017. Systems behind on the security update became victims. As for SynAck, it bypasses malware detection with a technique called Process Doppelgänging, which masks the attack by making it look like a legitimate process to gain entry.

These are just two examples among many that highlight the need for a comprehensive approach to ransomware defense.

Ever since ransomware appeared, there has been an ongoing evolution of attacks, which target different IT system vulnerabilities with increasingly creative and/or sophisticated techniques. Why? It is because ransomware is a very profitable business.

2 Steps to Neutralize Evolving Ransomware

1. Continuous Data Protection

When faced with a ransom demand, there is a dilemma that you may not get your data back even if you pay. According to an FBI internet crime report[3], "The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom."

So, what should an organization do? IDC states in a white paper titled *Ransomware Defenses Require Backup and a Comprehensive Security Strategy*—"Investigators are consistently finding a lack of comprehensive defenses that include continuous data protection products that track and save data to disk so that information can be recovered from any point in time, even seconds or minutes ago. "

It is easy to say 'no' to a ransom demand when you have an up-to-the-minute copy of the data tucked away safely somewhere that the ransomware cannot touch. Equally important is how easy it is to restore the data to minimize productivity impact and operational disruptions. An effective solution should be:

- Policy based to ensure that business critical data is backed up with the right RPOs and RTOs.
- Deep integration with primary storage, is critical to meet the recovery performance expectations
- Manage the snapshot schedule performing snapshots on an hourly

1 *CISCO Annual Cybersecurity Report*
2 *Article—270% increase in malware detection among Asia Pacific businesses in 2018—Enterprise*
3 *2017 Internet Crime Report*

basis, thus minimizing the amount of data loss if ransomware strikes.

- Efficient in consuming network bandwidth and storage through advanced deduplication capabilities.
- Secure in both data transmission and storage.
- Bare metal recovery capabilities to be able to recover to dissimilar hardware and that it can recover both system information and data as well.

For a risk-free evaluation of a proven Data Protection solution with more than 30 years of experience, please sign up for free trial of Micro Focus Data Protector here.

2. Real Backup Solution

Protecting corporate assets is a tremendous responsibility placed on IT teams, and the only real solution to ransomware and other cyber-attacks is to prevent them from infecting users in the first place. But, it's a task that is too vast and complex to be handled without the right tools and automation.

Effective solutions should include functionalities specifically designed to help IT teams cope with not only current ransomware attacks, but a vast number of future cyber-attacks on IT businesses. From intrusion to infection and propagation, your solution should provide a holistic capability for protecting critical enterprise assets. These solutions should include:

3-2-1 BACKUP RULE

A well-known backup strategy is to follow the 3, 2, 1 rule. This first involves keeping three copies of your data (the original and at least two backups). The backup data should then be stored on two different storage types which could be disk or tape or cloud. Finally, at least one copy of the backup should be offsite for maximum protection, disaster recovery and often for long term backup. For compliance reasons it is sometimes necessary to store data on different technologies which fits well and is supported with this methodology.

Data Protector is an enterprise class, highly scalable backup and recovery software solution that allows data to be backed up to multiple targets including disk, tape, or cloud either on site or off site. Data Protector allows additional copies of any existing file system or image backup without the need to create a separate special backup. The target for these additional copies can be whatever best fits the needs of the company and can often be on different media in different locations for different data sets.

Centrally managed it provides reports and status dashboards for instant visibility of your data backup status.

RPO AND RTO POLICIES FOR EACH DATA

Micro Focus Data Protector provides one of the most comprehensive mission critical applications protection for applications such as Oracle, SQL, Microsoft Exchange, SharePoint, SAP, and SAP HANA. This provides backup support across the enterprise and ensures business continuity with a rapid recovery after any data loss or system interruptions.

For each mission-critical application it could be necessary to be able to define different Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to reduce any downtime. Less critical applications with lesser service level expectations can then be tiered to enable a strategic approach for disaster recovery.

The application integration offers granular recovery to enable individual files, directories or file systems to be recovered quickly to minimize any disruption. Data corruption and restore inconsistencies are avoided by utilizing the application-consistent recovery of Data Protector rather than having to rely on crash-consistent recovery.

Finally, the solution is application aware thus, it automates snapshot management including on Windows, Linux and HPE-UX.

As stated by George Crump in his article *how to ensure your backup protects you from ransomware*: Since backup is the primary means for recovery from a ransomware attack, IT needs to take extra precautions to protect the backup system. The vulnerability of the backup software to ransomware attack may be the only motivation required to switch to a new backup vendor. It is critical that the backup software protects itself to make sure it is not infected.

The shifting sands of ransomware attacks and the dire consequences necessitate a holistic approach that protects against malware. Continuous data protection and advanced recovery options are essential weapons in this winnable fight.

For a risk-free evaluation of a proven Data Protection solution, please sign up for free trial of Micro Focus Data Protector here.

Contact us at:
www.microfocus.com

Like what you read? Share it.

Learn More

If you are interested in trying out Data Protector for free, please visit here.