BEYOND BACKUPS

Immunizing Data From the Effects of Ransomware

sāf.ai
Data.
Evolved.

2022

Contents

Introduction

Ransomware is hitting hard. Everywhere. Victims include SMBs that fall prey to "spray and pray" campaigns to large organizations that are specifically targeted, and the size of the ransoms demanded is rapidly increasing.

- **The bad guys will find a way in (and likely already have)**
  Intrusion detection and prevention systems are critical components to combat a wide variety of threats. However, when faced with the sheer number and variety of attacks that are out there and the risk of a targeted attack (e.g. social engineering), it's safe to assume that you're eventually going to get breached and likely have been already - whether you know it or not.

- **Ransomware victims had invested in backup systems**
  Victims, particularly larger enterprises, have invested in backups, including state-of-the-art solutions (e.g. differential backups, isolated copies, multiple backup locations, etc.) and were still successfully attacked.

- **Ransoms are being paid**
  When an attack occurs, we often find that backups - no matter how frequently they are occurring, where they are maintained, etc. - do not provide the resiliency to rapidly recover from an attack that the victim had anticipated.

Backups Aren't Enough

Today, businesses preparing a defense against ransomware, too often, are only investing in a better backup system. The logic follows: “If my data gets corrupted, I’d better have a recent backup to which I can restore.” Unfortunately, it isn’t this simple; if it were, we wouldn’t see ransoms being paid and the number of attacks on the rise. For most data loss scenarios, a solid backup solution should be best practice for any organization, but to protect against the current crop of ransomware, you need more.

While backups have a place in the network architecture, they DO NOT and CAN NOT prevent ransomware (or any other type of malware) attacks.

Where Backups Fall Short

Let’s look at some of the areas where backups are coming up short as a defense against the current ransomware threat:

01 **Restoring from a "clean" backup takes more time and creates more disruption to operations than expected.**

This has always been the case in the event of a ransomware attack, but these days the issue is compounded with malware often remaining in a latent state for weeks or even months — infecting backups and complicating efforts to find a recent, clean restore point.

02 **When restoring from a backup, servers and other storage devices need to be remediated to ensure the removal of any latent malware.**

Remediation is a time- and labor-intensive process that is often very expensive — both in the cost paid to 3rd party consultants and in operational costs to the business (e.g. downtime, lost revenue, depressed productivity, etc.).

03 **Too much critical, current data may be lost when restoring from a backup.**

Backups are fairly blunt instruments, where data is restored en masse rather than distinguishing between "good" current data that should be maintained and "bad" data that needs to be restored from a prior point. In a restore, large amounts of good data are lost, and this problem is exacerbated the further back in time the organization must go to find a clean backup.

04 — In an attack, backups may be encrypted or deleted.

Current ransomware strains (e.g. Ryuk, SamSam) are targeting backups. Ransomware will opportunistically attack backups that it encounters (e.g. automatic copies created by Windows, shadow volumes, etc.).

05 — Data exfiltration and the threat of private data being made public.

Prior to launching the payload of a ransomware attack, bad actors often attempt to gain additional leverage on their victims by exfiltrating confidential data. In a recent attack on the security staffing firm, Allied Universal, data was exfiltrated and partially made public; the remaining data that hadn't been published was then used as leverage to further pressure the victim to pay the ransom.

After a ransomware incident, the process to restore from a backup, rebuild systems, and return to normal operations can take weeks or even months. Faced with that kind of disruption, it's no wonder that many businesses (and their insurers) opt to pay the ransom.

After the ransom is paid (assuming the decryption key works), a costly remediation process is still to come, but in the meantime, an organization is at least able to recover to a semblance of business as usual.

However, paying a ransom is a short-term fix and only encourages future attacks. We can't accept this as the status quo so....

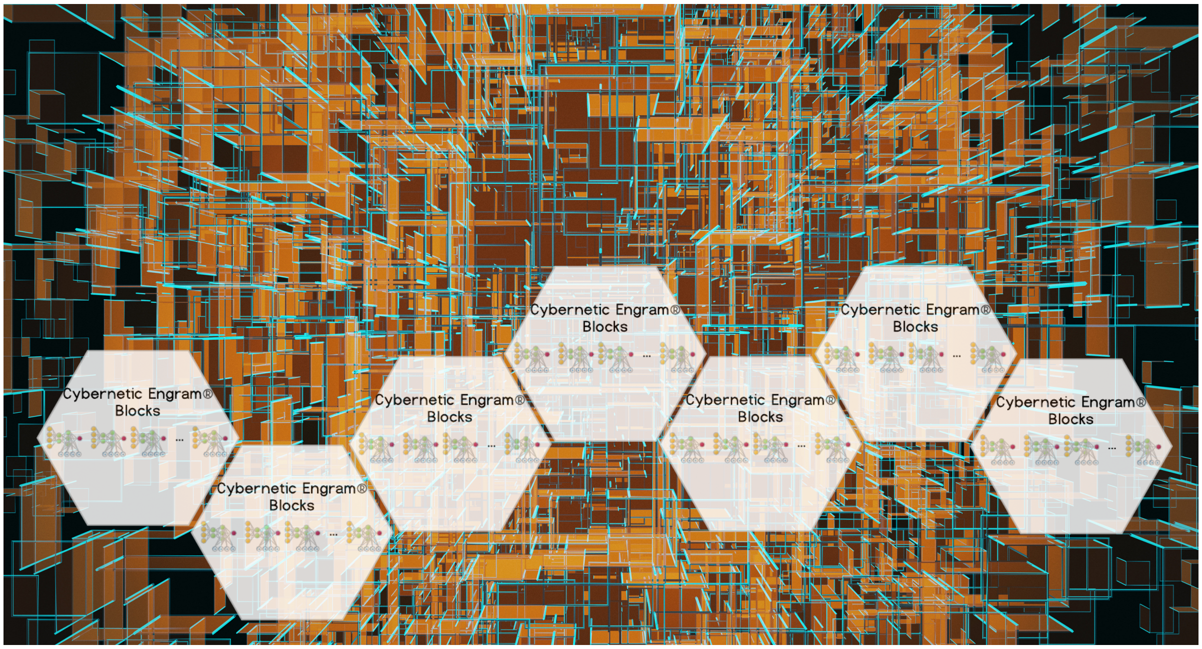
- Where does the search for a solution begin?
- As with so much of our data security architecture, is the answer to layer solutions to fill each of these gaps?
- Do these issues derive from a common root cause that we can address?
- What qualities would data need to have to be made immune to these types of attacks?

The Proven Defense

Resiliate™

sāf.ai's Resiliate enables data to be truly resilient—ensuring that an organization is able to maintain continuous access to its mission-critical data:

- Resiliate confers each block of data with its own memory and ability to learn.
- Data is fused with its own security protocols — thus transforming it from a passive entity to one that can participate in its own defense. These security protocols are enforceable against sysadmin / root privileges, which means that data cannot be destroyed or corrupted by bad actors even in the most extreme cases of privilege escalation.
- Data has a fundamental understanding of its nature. It is able to detect anomalous changes that are made to it (e.g. the entropy that's introduced by a ransomware attack).


Cybernetic Engram® Blocks
Cybernetic Engram® Blocks
Cybernetic Engram® Blocks
Cybernetic Engram® Blocks
Cybernetic Engram® Blocks
Cybernetic Engram® Blocks
Cybernetic Engram® Blocks

Resiliate vs. Ransomware

01 Each block of data evaluates all I/O versus its history to ensure “clean” recover points.

Self-aware files identify aberrant behavior (e.g. corruption in the case of ransomware) and automatically revert to the last clean version of the data. This automated detection and recovery from any corruption immunizes data from the effects of ransomware and allows for business operations to either continue unabated or with minimal downtime even as the ransomware is attempting to deploy its payload.

02 Immutable record of data’s complete history.

As noted above, destroying backup files is often a priority directive for ransomware prior to beginning to encrypt files. An immutable storage architecture is critical -- protecting data both from an attack and human error. Resiliate storage virtualization engine provides Hyperledger Sawtooth blockchain to ensure decentralized and immutable data and metadata.

03 Instantaneous restores.

In most instances of a ransomware attack, Resiliate will deny the rogue action or revert data to its last clean state immediately. However, in a worst case scenario where a file is corrupted, Resiliate dynamic-response subsystem conducts deep analysis on all data, will trigger the files and data to go back to their last known good state, update their internal resilience, and trigger relevant security protocols (recoveries can be configured to occur automatically or through admin-directed processes). Resiliate can recover petabytes of data in a matter of minutes.

04 — Integrated data forensics.

As noted above, self-aware data creates an immutable record of the history of all data and metadata. In the event of an attack, this provides immediate intelligence to system administrators and security officers to trace the source of any breach.

05 — Cooperation with existing security infrastructure.

Resiliate works in cooperation with existing security hardware and software architecture to enhance their capabilities. If an attack occurs that existing security does not have signatures for, Resiliate will stop the attack, alert other systems that an attack was attempted and provide signatures for the attack. In the event of an attempt to exfiltrate data, Resiliate can coordinate with a firewall to prevent malicious transmission of data.

Ransomware is an ever-evolving threat, and recently released strains have upped the ante considerably with actively-targeted attacks and seven-figure ransom demands. If we're going to break out of the cycle of patching security gaps and fighting the last war, we need to take a data-centric approach to security. By enabling data with its own memory and unique whitelisting protocols, sāf.ai enables data to defend itself at a fundamental level against all ransomware, including zero-day, as well as other threats.

Breaches Happen
Resiliate makes them irrelevant

Contact

sāf.ai, Inc.
888-997-2324
https://saf.ai
info@saf.ai
@_saf_ai_