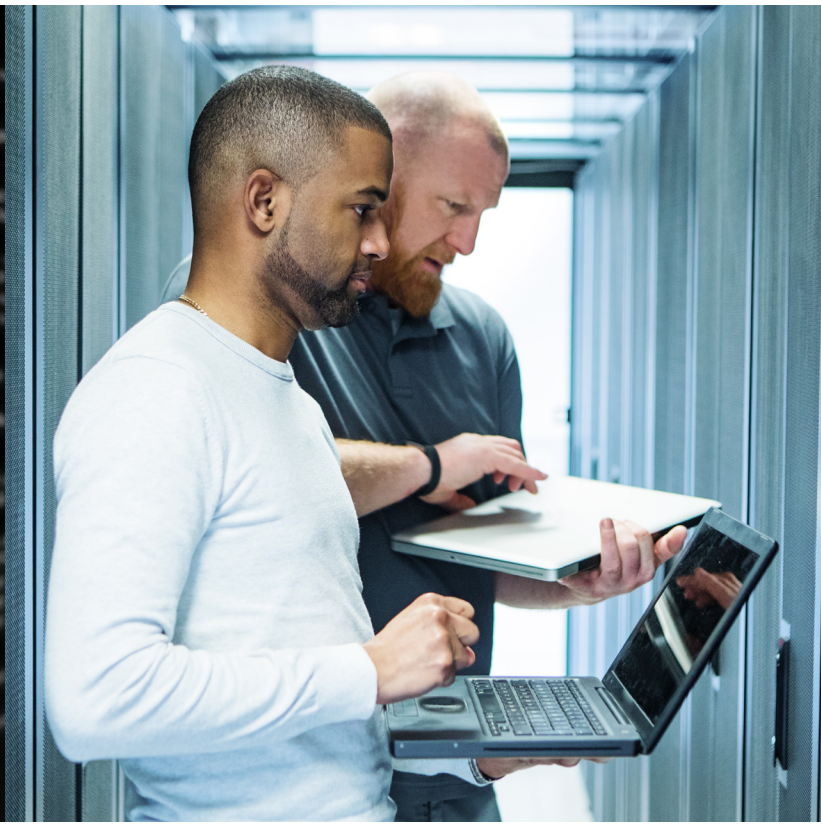
Immutable and Air-Gapped Backups are Dead

How Ransomware 2.0 Penetrates Your Last Line of Defense



asigra

> "Captain, they've adapted!"
>
> *Worf – Star Trek First Contact*

In Star Trek, humanity's most lethal enemy, the Borg, are notorious for having the ability to analyze and adapt. Unfortunately, cybercrime organizations have adapted and can now evade the security strategies that most organizations utilize to protect their backups (their last line of defense), air-gapping, and immutability.

In previous decades, backups were utilized to protect against building sprinkler systems, fires, floods, or hardware failure. However, with the advent of the cloud, the true value of backups has morphed into a last line of defense against ransomware and other cyber-attacks.

Ransomware attacks have become the most lethal threat to your business. Cybercrime syndicates are highly organized, well-resourced, and are either profit-motivated or directed by state actors for political and military means. The dramatic year-over-year rise of ransomware attacks illustrates how well cybercriminals have adapted. Unfortunately, most backup solutions depend on security strategies with vulnerabilities that have been known for years and have simply not kept pace with the attackers who are extracting billions in ransom from companies worldwide.

What is Air-gapping?

Air-gapping, while popular, is not a new tactic. Air-gapping means physically disconnecting a computer device or medium from the network or the internet, so it's not accessible digitally and is only accessible through physical intervention. The concept is that if a storage medium is not available or accessible via the network, it is functionally impossible for hackers to access the data.

In some cases, backup software companies create "logical" or "virtual" air-gaps by making it impossible to access backup data after it's been backed up, even though the data is located on a storage medium connected to a network. An example is storing backup copies in the cloud which is accessible by a separate storage account requiring another set of logins for access or stored in a separate region.

What is Immutability?

Immutable means not capable or susceptible to change. Immutable backups are stored in a WORM (write once, read many) state, meaning they cannot be modified, overwritten, or deleted.

Both immutability and air-gapping have the same goal. To prevent backup data from being deleted, encrypted, or corrupted. In the event of a ransomware attack, this has been considered a best practice and an effective means of protecting your business's data from attack.

How Ransomware 2.0 Evades Immutability and Air-Gapped Strategies

Intelligence from ransomware response teams and attack postmortems show air-gapping and immutable backups have not protected the data, often with tragic outcomes for the businesses that must pay the ransom. While these "best practice" tactics give the impression that the backup data is impenetrable, the reality is that the backup data is still at risk. Unfortunately, immutability and air-gapped strategies breed a false sense of security.

Ransomware 2.0 Utilizes Sleeper Attacks

Today's ransomware attackers utilize zero-day attacks to gain entry, but they are not immediately encrypting data on the network. Instead, the new breed of attacks infect as many systems as possible over days, weeks, or even months by installing backdoors, mapping networks, and hunting for highly privileged credentials to access sensitive systems, including the backup software.

Additionally, they embed dormant ransomware code in otherwise legitimate files. Because the ransomware is dormant, it can be challenging for antimalware, and other security solutions to detect it. When the systems are backed up, the file infected with dormant ransomware is backed up along with the rest of the days' data. Unfortunately, the infected file has now been carried into both immutable and air-gapped storage.

Immutability Subversion Attacks

One of the most common attack strategies involve credential hunting. Once attackers have gained access to part of an organization's infrastructure via zero-day malware infiltration, social engineering, or a phishing attack, they can start to hunt for the credentials of privileged users. Common tactics include key loggers, phishing, and credential stuffing attacks.

With stolen credentials, attackers can use the backup system against itself. Once they have access to the backup software, they can delete backup sets or change data retention policies from 3 years to 3 days. Even though the data is immutable, the backup system will follow orders and delete the data as instructed by the "pseudo-authorized" administrator.

Limitations of Immutability

The immutable data is usually connected to an online network connection and can be kept up to date with a high RPO.

Unfortunately, immutable backups are vulnerable to the new breed of ransomware that utilizes sleeper (trojan horse) attacks. An immutable backup that contains malware has zero value. With attackers targeting organizations weeks or months before encrypting the network, companies are finding themselves with no clean backups when they need them most.

Additionally, credential hunting attacks pose a massive risk for immutable data. The ability for the attacker to use the backup software against itself to change retention periods or delete data are a common attack strategy that exploit the application instead of the data within the backup application.

Hardware Issues Can Harm Immutable Backups

Though Immutable backups are designed to protect against intentional data destruction, they are still susceptible to natural data corruption. The typical backup medium for today's immutable backups – hard drives – can still cause degradation and corruption of data. In addition, testing and updating immutable backup can be cumbersome as the administrator is required to be onsite with the immutable storage. And, unless those backups are tested frequently, a corrupted backup could cause a restoration failure when needed most.

3-2-1 Air-Gapped Backups Are Only a Piece of the Puzzle

Air-gapping is a crucial strategy and part of the last line of defense in the event of a ransomware attack, but other security strategies must complement it. As mentioned above, sleeper attacks can easily embed dormant ransomware into otherwise normal files. Unfortunately, because the dormant ransomware is very difficult to detect, the malware will be backed-up into all repositories, including those that are air-gapped.

It's Time to Evolve and Bring the Fight to Ransomware 2.0

To stay ahead of the advanced ransomware that has been weaponized and deployed at scale, companies can not rely on air-gapping and immutable storage as their last line of defense. Instead, to avoid falling victim to the proliferation of advanced attacks, a security-first mindset is needed where IT operations and cybersecurity teams work together, recognizing that backup is now a critical piece of cybersecurity defense. Therefore, a security-first backup solution is required. One that continually evolves and is purpose-built to stop the ever-evolving ransomware.

Agentless Backup Allows for Advanced Security

Asigra Tigris Ultra Secure Backup is unique in that it is genuinely agentless and does not use endpoint agents to collect data but instead utilizes a proprietary "Data Security Module" software module that runs on a physical or virtual machine on the LAN. The Asigra Tigris Secure Data Collector acts as a funnel gathering data from all endpoints on the LAN to prepare the data for backup. Here, it can execute advanced malware scanning, FIPS 140-2 certified encryption, and industry-leading compression and deduplication.

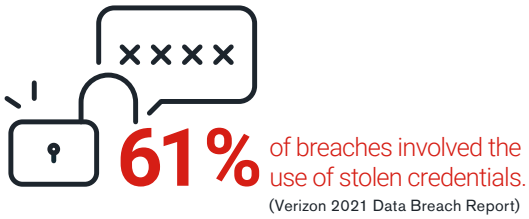
Bidirectional Scanning

Asigra Tigris uses an industry-leading AI-driven malware detection engine that hunts both known and unknown ransomware and malware. Asigra Tigris' ransomware detection engines are constantly updated with new signatures and improved AI detection based on evolving attack vectors amassed via a global network of intelligent receptors. All data is scanned for malware during the pre-backup process, and suspicious files are quarantined in a

password-protected zip file. Asigra Tigris uses advanced heuristics to hunt and identify even zero-day attacks. And more importantly, Asigra Tigris also scans all files before restoration. In the unlikely event that malware went undetected during the backup phase, it is improbable that it will go undetected during the second scan, prior to restoring the files into the live environment. The chances of detecting the malware rise dramatically during the second scan. This is because the previously dormant malware is no longer a zero-day attack (the most challenging attack to identify). The bidirectional, in-line ransomware scanning is critical to preventing an attack-loop scenario.

Deep MFA

Because credential hunting attacks are so prevalent and devastating, it's critical that key functions in the backup system are protected from stolen credential attacks.



To protect against credential hunting, Asigra Tigris has integrated advanced Deep MFA technology. This password-less authentication feature relies on biometrics embedded in mobile phones (facial recognition or fingerprint authentication). Like many MFA solutions, a user can't sign into the Asigra Tigris Management Console without authentication. However, Deep MFA ensures specific tasks, like changing backup retention policies (e.g., from 2 years to 2 days) or permanently deleting backup data, require a second authentication. This Deep authentication request can also be routed to multiple people, either inside or outside the organization. This multi-person authentication for key actions is critical protection against advanced attacks as well as protection from insider threats.

Autonomic Healing and Restore Validation

With any storage media, backups will degrade over time. If a backup is stored on a disk drive, like many backups are today, there's always a chance that a drive can have a block sector failure and that part of a file may be corrupted, even with "immutable" backups.

Asigra Tigris ensures the ability to restore these files using a feature called Autonomic Healing. Asigra Tigris continually analyzes all backup data looking for degradation, monitoring the logical and physical integrity of the backup data. If a file is corrupted or damaged, Asigra Tigris will automatically reach back to the source file, obtaining the specific piece of data required to repair the backup.

In addition to self-healing, Asigra Tigris makes it very easy to perform restore validations, ensuring your ability to restore data prior to a backup. An MD5 check can be scheduled or run on demand to ensure the backup data is in recoverable state. It is essentially a restore that runs in the repository software memory and flushed after the MD5 check is complete. No data is restored back to the source location.

Final Thoughts

With the recent invasion of Ukraine, Log4J vulnerabilities, and the continued "professionalization" of cyber-criminals, the frequency and severity of ransomware attacks is predicted to explode. Any IT professional on the receiving end of a successful ransomware attack is likely to have a career-altering experience. As the cybercrime syndicates have adapted to immutability and air-gapping strategies, every IT professional needs to adapt and evolve in kind. Asigra Tigris can help you adapt.

What's next?

Are you looking to strengthen your data security?
Learn more about Asigra Tigris Ultra Secure Backup.

Contact Us