Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Dr. Georgianna Shea

Executive Summary

Ransomware attacks are a lucrative practice for hackers. In just one attack in June against meat processing company JBS, hackers extorted an $11 million payment.[1] In the wake of the May 2021 Colonial Pipeline ransomware attack, Secretary of Homeland Security Alejandro Mayorkas said, "More than $350 million in losses are attributable to ransomware attacks this year. That's a more-than-300 percent increase over last year's victimization of companies. And there's no company too small to suffer a ransomware attack."[2]

Ransomware is a type of malware that encrypts the target's files and data or even its entire system, preventing users from accessing the data until they pay the ransom. After receiving payment, the hacker provides the decryption key in the form of a password. The hacker may also engage in double extortion, threatening to leak the stolen data if the victim does not pay.

Prevalent strategies for dealing with ransomware emphasize defensive measures, even though experience shows that one cannot thwart a well-resourced adversary determined to penetrate a target's system.[3] To the extent that current strategies seek to build resilience, they call for maintaining system backups, which may not prevent substantial data loss. For example, the ransomware best practices guide from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) begins with an admonition "to maintain offline, encrypted backups of data and to regularly test your backups."[4] The CISA guide then turns to cyber hygiene measures for preventing infections.[5]

To deal more effectively with the threat from ransomware, the most pressing need is to configure networks in a manner that promotes post-attack resilience. Specifically, there is a need to shift from defending devices — such as servers and workstations — to ensuring that the data on those devices is immediately recoverable. Decentralized file storage systems provide a potential solution. Instead of storing files and data on a central server that may become a single point of failure for the entire network during a ransomware attack, a decentralized storage system "shards" (breaks up), "hashes" (labels), and encrypts files, then stores the fragments in multiple locations.

If the system works as intended, users can discard compromised devices following a ransomware attack, then use new machines to reassemble their files and resume business as usual without costly disruptions. Even if attackers exfiltrate files or data, encryption prevents them from exploiting it for extortion or other purposes.

In this pilot project, the Transformative Cyber Innovation Lab (TCIL) at the Foundation for Defense of Democracies (FDD) partnered with CyLogic, a cybersecurity products company, to demonstrate how decentralized file storage systems can mitigate the effects of ransomware. TCIL tested this new approach to file storage using CyLogic's CyDrive, a secure, decentralized file storage system that enables users to manage and share files securely. The TCIL pilot tested a user's ability to create a file, store it, have it infected by ransomware, and immediately recover the file. The TCIL pilot

1. Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," *The Wall Street Journal*, June 9, 2021. (https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781)

2. Secretary of Homeland Security Alejandro Mayorkas, The White House, *Remarks to the Press*, May 11, 2021. (https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/11/press-briefing-by-press-secretary-jen-psaki-secretary-of-energy-jennifer-granholm-and-secretary-of-homeland-security-alejandro-mayorkas-may-11-2021)

3. U.S. Cybersecurity and Infrastructure Security Agency, "Ransomware Guide," September 2020. (https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf)

4. U.S. Cybersecurity and Infrastructure Security Agency, "How Can I Protect Against Ransomware," accessed September 9, 2021. (https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware); U.S. Cybersecurity and Infrastructure Security Agency, "Ransomware Guide," September 2020. (https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf)

5. For more information on practical steps that small- and medium-sized businesses can take to improve their cybersecurity posture, see: RADM (Ret.) Mark Montgomery and Theo Lebryk, "Cyber Hygiene 101 for Small and Medium-Sized Businesses," *Foundation for Defense of Democracies*, July 28, 2021. (https://www.fdd.org/analysis/2021/07/28/cyber-hygiene-101-for-small-and-medium-sized-businesses)

also compared CyDrive's recovery capabilities against 11 commercially available tools that the National Institute of Standards and Technology (NIST) identifies in its reference architecture for post-attack recovery.

The TCIL pilot demonstrated in practice that decentralized storage systems can deliver the following expected benefits:

1. If ransomware locks a machine, the user can still recover all the data with minimal (if any) delay. The organization can resume business as usual within minutes.
2. If a hacker gets into the system, the hacker cannot read files (or engage in double extortion), since the data are encrypted.
3. The document creator determines the document permissions, preventing access by a system administrator or users who could act as an insider threat.

How Ransomware Works Against Traditional File Storage Systems

Instead of incentivizing the design of resilient networks, cybersecurity requirements often result in the addition of security controls on top of the existing system architecture. Security controls are necessary, but they do not address the root cause of vulnerability, which is the imperfection of the human beings who use the network. Attackers understand the human root of vulnerability, so many of their initial access techniques involve deceiving a user into visiting a compromised website, clicking a malicious link, downloading malware, or inserting a compromised USB drive.[6] Cybersecurity strategies often focus on training users to recognize and avoid the attackers' attempts at deception. Training is necessary, but human users will eventually fall prey to deception. Alternatively, attackers may obtain access by paying off employees — potentially even system administrators — of the targeted firm.

When security measures are simply layered on top of the system architecture, the consequences of a potential attack may be catastrophic. For example, when organizations provide their employees with a computer operating Microsoft Windows, users usually create and store files within a folder on their C: drive or in a central repository. All the file protections are located outside of the document, in the form of system and network controls. When a breach occurs, there is nothing to prevent the attacker from achieving wholesale access to and encryption of the data.

Current best practices emphasize the maintenance of system backups as the primary means of limiting damage and creating post-attack resilience. System backups do provide some resilience, but there may be significant data loss in reverting to the last known good state of the data. For example, if the data backup happens daily or weekly, victims can count on losing hours' or days' worth of data. If backups occur monthly, companies should count on losing weeks' worth of data. If it is unclear when the attacker breached the system or if the hacker surveilled the system for weeks or months before launching the attack, the last known good state may have been many months prior. System backups may be better than nothing, but they are far from sufficient.

The NIST Privacy Framework observes that mission success and business functions depend on the "confidentiality, integrity, and availability of information processed, stored, and transmitted,"[7] meaning protecting data is more important than protecting devices or training users to protect devices. Ransomware has proven so effective against networks that employ traditional file storage systems, because those systems are so limited in their ability to preserve the confidentiality, integrity, and availability of data after an attack.

Confidentiality: Centralized storage risks wholesale exfiltration of data following a breach, creating a situation in which firms are in violation of regulatory confidentiality requirements. Similarly, exfiltration could expose or compromise

6. "Initial Access," *MITRE ATT&CK*, July 19, 2019. (https://attack.mitre.org/tactics/TA0001)

7. U.S. Department of Commerce, National Institute of Standards and Technology, "NIST SP 800-37, Revision 2," December 2018. (https://www.nist.gov/privacy-framework/nist-sp-800-37)

proprietary information, intellectual property, personally identifiable information, and other sensitive data. Users in centralized systems also tend to have much more access than they need to do their jobs, which increases the risk that an insider threat will exfiltrate data. Hackers often seek access to system administrator credentials because those administrators have access to all files, even though such access is rarely necessary to perform administrative duties.

Integrity: Traditional file storage systems do not use hashing to ensure data integrity. Hashing involves converting data into a unique numeric value. Each change to the data (or file) changes the hash value. Without hashing, organizations cannot determine if an unauthorized modification to a given file has occurred. A malicious actor may be able to change critical data undetected, and without an integrity check, it can be difficult to identify the last known good state of the data.

Availability: Storing files on a local machine or central server creates a single-point-of-failure vulnerability. If malware infects the location, it will infect (or otherwise affect) all stored data. Availability may suddenly become zero, creating the risk of a protracted disruption of business.

Prior to the proliferation of ransomware, organizations often believed they would not suffer attacks, because they had no removable capital (unlike banks) and nothing valuable to steal and sell on the black market. Hackers, however, recognized that a company's data, or at least the confidentiality of that data, is often priceless to the company itself. Suddenly, the number of profitable targets for ransomware attacks grew exponentially.

Ransomware-as-a-Service

Recognizing the potential of ransomware attacks at scale, certain hackers created ransomware-as-a-service (RaaS) providers that give others the tools to carry out attacks.[8] For example, one RaaS group, DarkSide, reportedly responsible for the Colonial Pipeline attack, generated $90 million in Bitcoin payments over nine months as a malware provider.[9] RaaS functions as a partnership between a malware provider and an affiliate with access to a victim. Together, the partners plan and execute the attack and split the ransom. The affiliates may even be disgruntled system administrators or other employees acting as insider threats.[10]

After the provider and affiliate form an agreement, the affiliate exfiltrates data from the victim to determine if the attack is likely to achieve a return on investment to justify the time and effort spent. If the partners agree, they launch the ransomware attack and demand payment from the victim. To increase pressure on the victim, hackers will sometimes engage in double extortion by threatening to publicize the stolen data. The hackers may also publicly shame the victim for its poor security or for other real or perceived indiscretions revealed by the confidential data. Figure 1 illustrates the RaaS business model. With the number of ransomware attacks growing rapidly, thanks in no small part to RaaS providers, there is an urgent need to rethink conventional approaches to defense and mitigation.

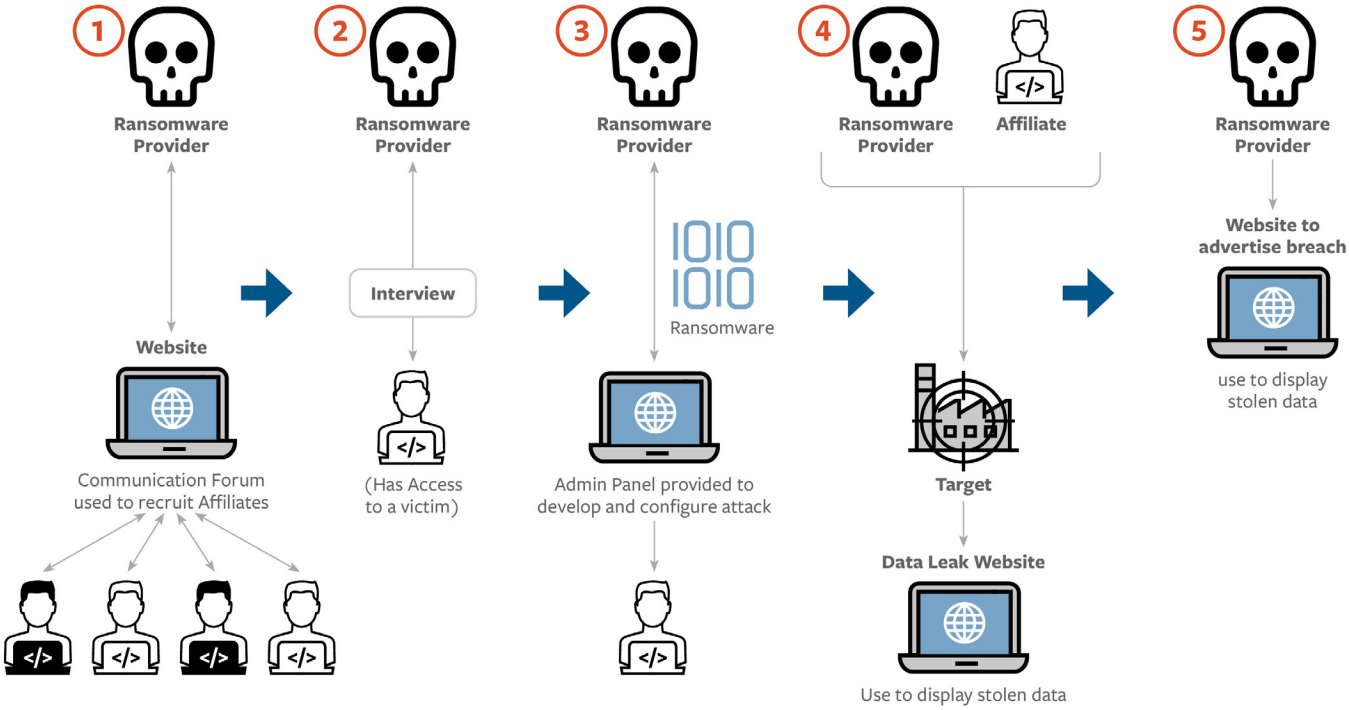
8. Jeff Stone, "The anatomy of a modern-day ransomware conglomerate," *CyberScoop*, January 4, 2021. (https://www.cyberscoop.com/ransomware-attack-schools-hospitals-egregor-sophos); Tim Starks, "How REvil evolved into a ransomware collective capable of extorting Kaseya, JBS," *CyberScoop*, July 8, 2021. (https://www.cyberscoop.com/revil-ransomware-gang-russia-us-attacks)

9. Ryan Browne, "Hackers behind Colonial Pipeline attack reportedly received $90 million in Bitcoin before shutting down," *CNBC*, May 18, 2021. (https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html)

10. Kelly Jackson Higgins, "Ransomware Attacker Offers Employees a Cut if They Install DemonWare on Their Organization's Systems," *Dark Reading*, August 19, 2021. (https://www.darkreading.com/threat-intelligence/ransomware-attacker-offers-employees-a-cut-if-they-install-demonware-on-their-organization-s-systems)

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

RANSOMWARE AS A SERVICE EXPLAINED



1) *The ransomware provider recruits an affiliate from an online chat forum.*
2) *The ransomware provider interviews the affiliate.*
3) *The ransomware provider and the affiliate develop the attack plan.*
4) *The team compromises the target and begins to exfiltrate data, reviews that data, and then executes ransomware.*
5) *The ransomware provider informs the victim of the compromise. Once the ransom is paid, the ransomware provider splits the ransom with the affiliate.*

Piloting the Solution: Inherently Secure Decentralized File Storage

A more effective approach to resilience against ransomware attacks focuses on securing what is most important, the data, not the devices. In a decentralized file storage system, the machine is replaceable and irrelevant to the security of the data. Randy Bias, an expert on cloud computing, explained the difference with an analogy, "Pets vs. Cattle." In the traditional system, "we treat our servers like pets," which we consider unique and indispensable. We spare no expense and try everything to heal a sick pet. "In the new way, servers are numbered, like cattle in a herd," Bias writes. "When one server goes down, it's taken out back, shot, and replaced on the line."[11] A decentralized system turns servers and other devices from pets into cattle. If a machine becomes infected, the user simply discards the device and signs into another machine to resume business as usual.

TCIL wanted to show that this approach works in practice, so that firms at risk of ransomware attacks understand there is a viable alternative to the status quo. To that end, TCIL partnered with CyLogic, the developer of the CyDrive decentralized file storage system. The system works as follows: When a user saves a file, instead of simply saving the file locally or on a central server, the data are hashed, broken up into pieces (or sharded), hashed again, and encrypted. The fragments (called shards)

11. Randy Bias, "The History of Pets vs Cattle and How to Use the Analogy Properly," *Cloudscaling*, September 29, 2016. (http://cloudscaling.com/blog/cloud-computing/the-history-of-pets-vs-cattle)

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

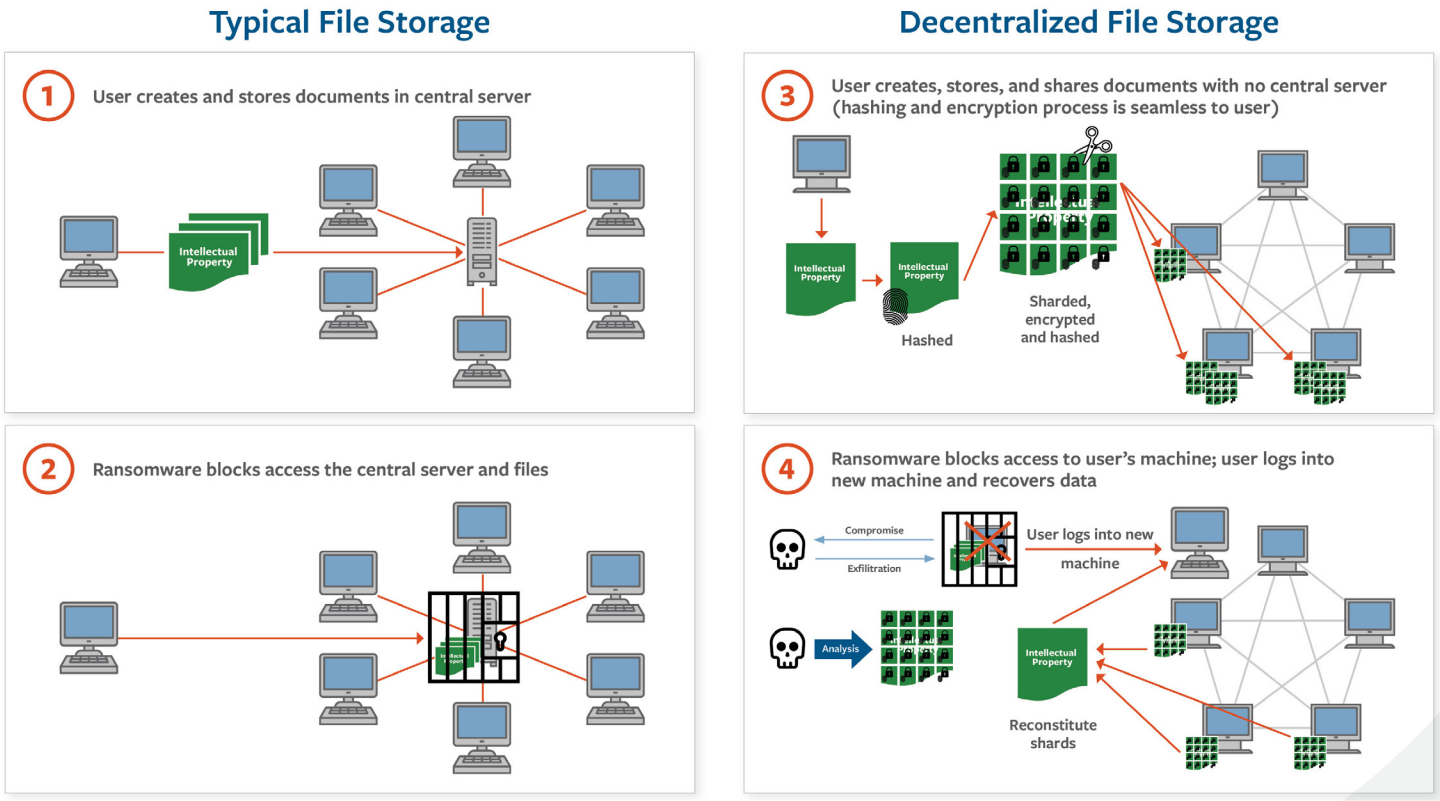
are then distributed to multiple other machines. The distribution may occur through an encrypted tunnel, but that is not a precondition for adequate security. The fragments are symmetrically encrypted, and the keys are always in an encrypted state when traveling.

The TCIL pilot mirrored test cases found in NIST SP 1800-11, "Data Integrity Recovery from Ransomware and Other Destructive Events," as a baseline by which to judge pilot performance. NIST establishes national standards for cybersecurity, and NIST SP 1800-11 identifies a reference architecture for ransomware recovery. (See Appendix A for test cases and results.)

NIST SP 1800-11 highlights 11 commercially available tools with distinct yet complementary functions that can be used together to provide ransomware recovery capability. TCIL sought to gauge whether CyDrive would outperform the established alternatives in a realistic scenario. (See Appendix B.)

The pilot showed that the "cattle, not pets" approach, implemented via the CyDrive decentralized file management capability, removes the need for a central server, since authorized users share and restore all files. Removing the central server eliminates the primary target of a ransomware attack. When an individual machine is infected by an attack, the user simply logs in from a different device and rebuilds the files from the encrypted, distributed fragments. Figure 2 illustrates the typical file storage process compared to the decentralized file storage process. The top row shows the network topography and where data get stored. The second row illustrates a ransomware infection that blocks access to the data storage location.

Figure 2: Comparison of File Storage Processes



Box 1 *represents a typical file storage topography. A user creates files and stores them in a central repository.*

Box 2 *represents the central server being infected with ransomware, which denies all users access to the files.*

Box 3 *represents a decentralized, secure file storage topography. The user stores a file; it gets hashed, sharded, encrypted, hashed again, and then distributed.*

Box 4 *represents a user's systems becoming infected with ransomware and denying access to the files stored on the infected system. The user logs into a new device to reconstitute the files from the distributed shards.*

Real-World Benefits of Decentralized, Encrypted File Management

While the pilot's purpose was to demonstrate how a secure, decentralized file management system mitigates the effects of ransomware, cyber resiliency involves recovering from different kinds of attacks, not just the popular threat of the day. Decentralized file management provides other real-world benefits beyond protections against ransomware and may facilitate significant cost savings.

- System administrators and other personnel are not granted access to files by default, because the file creator controls access and permissions. By limiting file access to only those who require access, and by removing it from system administrators and super-users, organizations can avoid large-scale exfiltration campaigns conducted by super-users or system administrators. Removing file access from administrators would have prevented Edward Snowden, for example, from exfiltrating huge volumes of classified information. Limiting file access also creates potential cost savings, since administrative duties can be outsourced without the risk of the administrator accessing data.
- From the user's perspective, the encryption and security process is seamless and requires no additional tasks. This results in greater fidelity to security best practices because users simply create, store, and share the file as per their normal workflow instead of serving as a primary line of defense. A decentralized system greatly reduces the damage associated with unavoidable instances in which users are lazy, forgetful, or gullible.
- Once the user creates a file and saves it within the encrypted drive, the encrypted file is archived, creating an auditable log of all file versions to ensure data integrity.
- When files are updated, only the changes in the file require additional storage. This reduces redundancy in required storage space and operational bandwidth. The cost savings may expand beyond this to include eliminating other redundant services and technologies for creating system backups and maintaining file servers.
- Along with these benefits, there are two challenges to the effective implementation of a decentralized file management system. The first is balancing the use of encryption with the organization's need for access to the user-developed files. Since the data creator sets the permissions for access, he or she could essentially hold files hostage from the organization. To mitigate this risk, the organization could grant access to all files to a single data fiduciary, such as the chief information security officer. The second challenge is overcoming the traditional perception that peer-to-peer topologies are not secure due to their lack of centralized file storage and backup systems; as demonstrated by this pilot, that is not the case.

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Recommendations

CISA should update its Ransomware Guidance to discuss resilient, decentralized data storage solutions as a best practice. The CISA Ransomware Guidance consists of two parts, Ransomware Prevention Best Practices and a Ransomware Response Checklist.[12] Neither part includes recommendations for building a resilient system that plans for a ransomware infection and mitigates its effects by engineering a decentralized, distributed, secure data solution. The first step in Ransomware Prevention Best Practices is to be prepared. Being prepared requires planning for a ransomware attack and quickly recovering from it with little to no effect. Specific recommendations for chief information security officers and system security professionals are:

1. **Focus on data security, not just device security.** Consider adopting the "cattle, not pets" model, emphasizing a resilient infrastructure that anticipates ransomware attacks and other potential file system attacks and can withstand the effects of those attacks.
2. **Practice secure systems engineering.** New system acquisitions or upgrades should include security-focused requirements that drive engineering solutions to address design vulnerabilities specific to data security.
3. **Identify single points of failure.** Organizations should identify the single-location assets that result in mission failure when blocked by ransomware, then develop and execute a plan that removes that vulnerability. In addition, organizations should conduct an Attack Surface Analysis that identifies how an adversary could get into a network or system.
4. **Use encryption.** Encrypt data-at-rest and data-in-transit to prevent hackers from exfiltrating sensitive data.
5. **Remove document access from system administrators.** The principle of least privilege is an important security principle, yet most organizations give file access to system administrators. In most cases, system administrators do not need read access to company files to perform administrative duties.
6. **Conduct ransomware cyber tabletop exercises.** Develop, execute, and maintain a response plan, and use cyber tabletop exercises to fine-tune that plan and to train response staff.

Conclusion

Ransomware attacks will stop only when hackers stop seeing a return on investment. Organizations should anticipate that a hacker may breach their systems, but they do not have to accept that their data will be compromised by being leaked or locked. By applying secure engineering practices that focus on securing their data through a decentralized and distributed file storage architecture, organizations can absorb and withstand the impacts of ransomware attacks.

12. U.S. Cybersecurity and Infrastructure Security Agency, "CISA MS-ISAC Ransomware Guide," September 2020. (https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf)

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Appendix A: Pilot Test Cases

TCIL partnered with CyLogic to demonstrate ransomware recovery with a decentralized file storage capability by replicating the functional evaluations found in NIST SP 1800-11, Data Integrity Recovery from Ransomware and Other Destructive Events.[13] The National Cybersecurity Center of Excellence created NIST SP 1800-11 to document a reference architecture supporting data integrity that provides a recovery capability when a hacker infects an organization with ransomware.

Tables 1 through 5 are modified versions of the test requirements and scenarios from NIST SP 1800-11. The darker green header represents a TCIL-added column. The lighter green columns and cells represent the comparative TCIL data.

The TCIL pilot mirrored the functionality testing described in NIST SP 1800-11 on a new product, CyDrive, to illustrate a like-for-like comparison of how one product engineered with data security and integrity protections compares to a suite of add-on tools. In addition to the limitations identified within NIST SP 1800-11, the TCIL pilot focused only on the user's machine and files; database testing was not included. Table identifies NIST SP 1800-11's functional requirements. The TCIL pilot replicated Capability Requirements 1 through 4. Capability Requirements 5 and 6 were outside the scope of the pilot.

Table 1: Data Integrity Use Case Requirements From NIST SP 1800-11

Capability Requirement (CR) ID	Parent Requirement	Sub-Requirement	Test Case
CR 1	The data integrity example implementation shall respond/recover from malware that encrypts files and displays notice demanding payment.	CR 1.a (Logging) Produce notification of security event	Data Integrity-1
		CR 1.b (Corruption Testing) Provide file integrity monitor	
		CR 1.c (Backup Capability) Revert to last known good	
CR 2	The data integrity example implementation shall recover when malware destroys data on user's machine.	CR 2.a (Corruption Testing) Provide file integrity monitor	Data Integrity -2
		CR 2.b (Backup Capability) Revert to last known good	
CR 3	The data integrity example implementation shall recover when a user modifies a configuration file in violation of established baselines.	CR 3.a (Corruption Testing) Provide file integrity monitor	Data Integrity -3
		CR 3.b (Backup Capability) Revert to last known good	
CR 4	The data integrity example implementation shall recover when an administrator modifies a user's file.	CR 4.a (Corruption Testing) Provide file integrity monitor	Data Integrity -4
		CR 4.b (Logging Provide) user activity auditing	
		CR 4.c (Backup Capability) Revert to last known good	

13. Timothy McBride, Michael Ekstrom, Lauren Lusty, Julian Sexton, and Anne Townsend, U.S. Department of Commerce, *National Institute of Standards and Technology, Computer Security Resource Center*, "Data Integrity: Recovering from Ransomware and Other Destructive Events," September 22, 2020. (https://csrc.nist.gov/publications/detail/sp/1800-11/final)

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Table 2: Test Case: Data Integrity – 1

Test Case Fields	NIST SP 1800-11 Results	TCIL Pilot Results Using CyDrive
Parent requirement	(CR 1) The data integrity example implementation shall respond/recover from malware that encrypts files, and displays notice demanding payment.	
Testable requirement	(CR 1.a) Logging, (CR 1.b) Corruption Testing, (CR 1.c) Backup Capability	
Description	Show that the Data Integrity solution can recover from a data integrity attack that was initiated via ransomware.	
Preconditions	User downloaded and ran an executable from the internet that is ransomware. The ransomware then encrypts the user's files.	
Procedure	1. Open the Tripwire Enterprise interface. 2. Click on the Tasks Section, enable the associated rule box, and click Run. 3. Open HPE ArcSight ESM. 4. Under Events, select Active Channels, then select Audit Events. 5. Find the Tripwire Enterprise event logs associated with the event. Select Fields in the Customize dropdown and enable the following fields: a. End Time b. Attacker Address c. File Name d. Device Action e. Source User Name f. Device Custom String 6. Open IBM Spectrum Protect. 7. Click on Restore a. Select missing files and click restore to the original location.	1. User requests and receives a new device. 2. The user's organizational CyDrive administrator initiates the addition of a new device to the user's account. (Note: Doing so locks all other devices currently on the user's account.) 3. The CyDrive system sends a welcome/activation email to the user. 4. The user receives CyDrive installation instructions via email. 5. User downloads/installs CyDrive software onto a new device. 6. User reboots. 7. User logs in. 8. User accepts license agreement and enters key and password. 9. User logs into CyDrive with multifactor authentication. 10. Selects option for restore. 11. All user's data (previously shared with and stored on CyDrive Data Repo) is restored to the user. Approximate total time: ~3 minutes
Expected Results (pass)	Event identified (CR 1.a), details of the event are understood and moment of last known good is identified. Provide file Integrity monitor (CR 1.b). Modified files are correctly identified. Recovery complete (CR 1.c)	
Actual Results	Details of the event were understood and the moment of last known good was identified for the file in question. All the files affected within that timeframe were correctly identified, and a complete and successful restore was executed.	
Overall Result	Pass. All metrics of success were met to satisfaction.	Complete and successful restoration was executed. The files recovered include all contents of the CyDrive from the last save, not the last backup.

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Table 3: Test Case: Data Integrity – 2

Test Case Fields	NIST SP 1800-11 Results	TCIL Pilot Results Using CyDrive
Parent requirement	(CR 2) The data integrity example implementation shall recover when malware destroys data on user's machine.	
Testable requirement	(CR 2.a) Corruption Testing, (CR 2.b) Backup Capability	
Description	Show that the data integrity solution can recover from a data integrity attack that destroys data via a malware attack.	
Preconditions	User downloads a malicious executable that modifies critical data.	
Procedure	1. Open the Tripwire Enterprise interface. 2. Click on the Tasks Section, enable the associated rule box, and click Run. 3. Open HPE ArcSight ESM. 4. Under Events, select Active Channels, then select Audit Events. 5. Find the Tripwire event logs associated with the event. Select Fields in the Customize dropdown and enable the following fields: a. End Time b. Attacker Address c. File Name d. Device Action e. Source User Name f. Device Custom String 6. Open IBM Spectrum Protect. 7. Click on Restore. 8. Select missing files and click restore to original location.	The user opens CyDrive and opens the previous version of the corrupted file before corruption.
Expected Results (pass)	Provide file integrity monitor (CR 2.a). Modified files are correctly identified. Recovery complete (CR 2.b). System was restored to pre-Data Integrity event version.	
Actual Results	Details of the event were understood and the moment of last known good was identified for the file in question. All the files affected within that timeframe were correctly identified, and a full and successful restore was executed.	All versions of the files are stored in CyDrive encrypted and hashed. Any change, including a corruption, would create a new version of the files with an updated hash. The last known good version is always available as the previous version. CyDrive provides continuous, not periodic, backup.
Overall Result	Pass. All metrics of success were met to satisfaction.	

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Table 4: Test Case: Data Integrity – 3

Test Case Fields	NIST SP 1800-11 Results	TCIL Pilot Results Using CyDrive
Parent requirement	(CR 3) The data integrity example implementation shall recover when a user modifies a configuration file in violation of established baselines.	
Testable Requirement	(CR 3.a) Corruption Testing, (CR 3.b) Backup Capability	
Description	Show the data integrity solution can recover from a data integrity event modifying configurations.	
Preconditions	Run a script that would simulate the effects of a configuration modification event (for example, adding unauthorized fake accounts.)	
Procedure	1. Open HP ArcSight ESM. 2. Under Events, select Event Search. 3. Use the search bar to search for the keyword "created" to find associated event logs for account creation. 4. After determining the point in time of a malicious event, restart the Active Directory server, holding down the F2 and F8 keys while restarting to enter the Advanced Boot Options menu. 5. Select Directory Services Repair Mode. 6. Log in as the machine administrator. 7. Open a command prompt. 8. View visible backup versions with the following command: wbadmin get versions 9. Restore to a selected backup target with the following command. Note that the selected date should reflect the last known good backup: - wbadmin start systemstaterecovery version:<Version Number> -backupTarget:<Backup Location> - Replace <Version Number> with the desired version's version identifier, and <Backup Location> with the version's corresponding backup location. 10. Provide a username (with domain if applicable) and password for a privileged user to the backup location. 11. Acknowledge the remaining prompts and wait for the backup to complete. The system will automatically restart.	Note: The configuration files must be stored in CyDrive. The user opens CyDrive and opens the previous version of the configuration file before corruption.

Test Case Fields	NIST SP 1800-11 Results	TCIL Pilot Results Using CyDrive
Expected Results (pass)	Provide file integrity monitor (CR 3.a). Modified files are correctly identified. Recovery complete (CR 3.b). Modified files are restored to their original state.	
Actual Results	The fake accounts were successfully identified and deleted. The remaining accounts were restored to their original states at the time of the backup.	All versions of the files are stored in CyDrive encrypted and hashed. Any change, including a corruption, would create a new version of the files with an updated hash. The last known good version is always available as the previous version. CyDrive provides continuous, not periodic, backup.
Overall Result	Pass. All metrics of success were met to satisfaction.	

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Table 5: Test Case: Data Integrity – 4

Test Case Fields	NIST SP 1800-11 Results	TCIL Pilot Results Using CyDrive
Parent requirement	(CR 4) The data integrity example implementation shall recover when an administrator modifies a user's file.	
Testable req.	(CR 4.a) Corruption Testing, (CR 4.b) Logging, (CR 4.c) Backup Capability	
Description	Show that the data integrity solution can recover when an administrator modifies a user's file.	
Preconditions	Two VMs on Microsoft Hyper-V have been backed up. The administrator accidentally runs a command that deletes a critical VM. **Remove-VM -Name "<VMName>" -Force**	
Procedure	1. Open HP ArcSight ESM. 2. Under Events, select Event Search. 3. Use the search bar to search for the deleted VM's name and then find the associated event log. 4. Locate previous logins from that machine by searching for the VM host machine's domain and name in the search bar. 5. Open the VEEAM console. 6. Navigate to the Backups menu. 7. Right-click on deleted VM and click restore, and then Entire VM. 8. When prompted, search for the deleted VM's name and select it for restoration. 9. When prompted, enter reason for VM restoration.	Note: This requires the VM snapshot to be stored within CyDrive (like any other file). The administrator would have to be explicitly granted access to the file or have a CyDrive user account from which he or she could restore. The user opens CyDrive and opens the previous version of the corrupted file before corruption.
Expected Results (pass)	Provide file integrity monitor (CR 4.a). Missing files are correctly identified. Provide user activity auditing (CR 4.b). User who initiated deletion is correctly identified. Revert to last known good (CR 4.c). VM is fully restored to original functionality.	
Actual Results	The VEEAM system functioned as expected. Deleted VM is restored to its original functionality. Any user logged in during the deletion event was identified.	All versions of the files are stored in CyDrive encrypted and hashed. Any change, including a corruption, would create a new version of the files with an updated hash. The last known good version is always available as the previous version. CyDrive provides continuous, not periodic, backup.
Overall Result	Pass (partial). The file integrity monitoring and reversion to last known good requirements were met. User activity was audited, but it is not possible to determine which user caused the deletion event if multiple users were logged in to the machine at the time of the event.	Pass. All metrics of success were met to satisfaction. Files are not deleted in CyDrive.

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Appendix B: CyDrive Comparison in Ransomware Recovery

NIST SP 1800-11 proposes a ransomware recovery architecture solution that relies on a collection of 11 different tools with various functions that enable components of recovery, as seen in the table below. The first three columns of the table come from NIST SP 1800-11, Table 3-2 Products and Technologies. The table's fourth column compares the CyDrive capability to the functions performed by the collection of tools.

Since CyDrive was engineered to focus on data security, all the components required for ransomware recovery are enabled through a single tool. Some of the specific functions, such as analysis and correlation of cyber events, can be enhanced with CyDrive but are not primary capabilities of the tool.

Table 6: Requirements Evaluation

NIST SP 1800-11 Table 3-2 Products and Technologies			CyDrive Capability
Component	**Specific Product**	**Function**	
Corruption Testing	ArcSight Enterprise Security Manager (ESM) v6.9.1	Provides monitoring for changes to data on a system.	Provides a log of all file changes and all user and administrator activities
		Provides logs, detection, and reporting, in the event of changes to data on a system.	Provides a log of all file changes and all user and administrator activities
		Provides audit capabilities for database metadata and content modifications.	Files cannot be deleted (unless configured to allow) from CyDrive, which enables the auditable history of all file versions and all user and administrative activities
		Provides notifications for changes to configuration.	Provides a log of all file changes and all user and administrator activities
		Provides analytic capabilities to determine the impact of integrity events.	N/A
	Tripwire Enterprise v8.5	Provides file hashing and integrity testing independent of file type (can include software executable files).	Stores files in a fragmented, encrypted, hashed decentralized state, allowing them to be recovered from any device. Provides continuous, not periodic, backup.
		Provides notifications for changes to configuration	Provides a log of all file changes and all user and administrator activities.
		Provides file monitoring for cyber-security events	N/A
		Provides audit capabilities for database metadata	Files cannot be deleted (unless configured to allow) from CyDrive, which enables the auditable history of all file versions and all user and administrative activities.
	Tripwire Log Center Manager v7.2.4.80	Provides logs in the event of changes to data on a system	Provides a log of all file changes and all user and administrator activities.
Secure Storage	Spectrum Protect v8.1.0	Creates encrypted backups	Stores files in a fragmented, encrypted, hashed decentralized state, allowing them to be recovered from any device. Provides continuous, not periodic, backup.
	WORMdisk v151228	Provides write-once read-many file disk storage for secure backups of integrity information.	Stores files in a fragmented, encrypted, hashed decentralized state, allowing them to be recovered from any device. Provides continuous, not periodic, backup.
		Provides immutability of backups	All files are store encrypted and hashed, and each version is therefore immutable.

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

NIST SP 1800-11 Table 3-2 Products and Technologies			CyDrive Capability
Component	**Specific Product**	**Function**	
Logging	ArcSight Enterprise Security Manager (ESM) v6.9.1	Provides auditing and logging capabilities configurable to corporate policy	Files cannot be deleted (unless configured to allow) from CyDrive, which enables the auditable history of all file versions and all user and administrative activities.
		Provides logging of some user activity of monitored systems	Files cannot be deleted (unless configured to allow) from CyDrive, which enables the auditable history of all file versions and all user and administrative activities.
		Provides network information about certain cybersecurity events	N/A
		Correlates logs of cybersecurity events with user information	N/A
		Provides logs of database activity and database backup operations	N/A
		Provides analysis capabilities for log data	N/A
		Provides analysis capabilities for finding anomalies in user activity	N/A
		Provides automation for logging	N/A
		Provides logs of database activity	N/A
	Tripwire Enterprise v8.5	Detects changes to database metadata and database backup operations	N/A
		Provides auditing capabilities configurable to corporate policy	Files cannot be deleted (unless configured to allow) from CyDrive, which enables the auditable history of all file versions and all user and administrative activities.
	Tripwire Log Center Manager v7.2.4.80	Provides logs of database metadata changes	N/A
Backup Capability	Spectrum Protect v8.1.0	Provides backup and restoration capabilities for systems	Restoration not needed, because files are continuously backed up and always available on-demand versus using static scheduled backups.
		Provides backup and restore capabilities for configuration files.	Stores files in a fragmented, encrypted, hashed decentralized state, which enables them to be recovered from any device. Provides continuous, not periodic, backup.
		Performs periodic backups of information.	Stores files in a fragmented, encrypted, hashed decentralized state, which enables them to be recovered from any device. Provides continuous, not periodic, backup.
	WORMdisk v151228	Provides immutable storage.	All files are store encrypted and hashed, and each version is therefore immutable.

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

NIST SP 1800-11 Table 3-2 Products and Technologies			CyDrive Capability
Component	**Specific Product**	**Function**	
Virtual Infrastructure	Veeam Availability Suite	Provides backup and restoration capabilities for virtual systems and virtualized data.	Stores files in a fragmented, encrypted, hashed decentralized state, allowing them to be recovered from any device. Provides continuous, not periodic, backup.
		Provides ability to encrypt backups.	Stores files in a fragmented, encrypted, hashed decentralized state, allowing them to be recovered from any device. Provides continuous, not periodic, backup.
		Provides logs for backup and restoration operations.	Provides a log of all file changes and all user and administrator activities

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Appendix C: TCIL Pilot Mapped to the Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a flexible tool that addresses and manages cybersecurity risk through a repeatable and performance-based approach.[14] Executive Order 13800 of 2017 required all federal agencies to use the framework. The table below maps the technologies used in the TCIL CyDrive pilot to the CSF.

Table 7 is a modified version of the CSF. The darker green header represents a TCIL-added column. The lighter green columns and cells represent the comparative TCIL data.

Table 7: NIST CSF With Enabling Technology

Function	Category	Subcategory	Enabling Technology Used With CyDrive
PROTECT	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Creator determined access control and separation of data access from administration
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Two-Factor Authentication
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	Secure storage through encryption and hashing
		PR.DS-2: Data-in-transit is protected	Secure storage through encryption and hashing
		PR.DS-4: Adequate capacity to ensure availability is maintained	Decentralized continuous backup and decentralized data storage
		PR.DS-5: Protections against data leaks are implemented	Secure storage through encryption and hashing
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Corruption testing through hashing
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-3:** Configuration change control processes are in place	Backup capability with hashing and continuous, automated version control and management
		PR.IP-4: Backups of information are conducted, maintained, and tested	Decentralized continuous backup
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Decentralized continuous backup
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Logging of continuous backup and all user and administrative activities
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Creator determined access control and separation of data access from administration
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot-swap) are implemented to achieve resilience requirements in normal and adverse situations	Decentralized continuous backup and decentralized data storage

14. U.S. Department of Commerce, National Institute of Standards and Technology, "Cybersecurity Framework," accessed September 9, 2021. (https://www.nist.gov/cyberframework)

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

Acknowledgments

FDD's Transformative Cyber Innovation Lab is a nonprofit organization that relies on volunteers with a passion for advancing cybersecurity practices. Thank you, Adam, for your contributions and expertise as well as your appreciation for Warren Zevon, Monty Python, and the Marx brothers. I thoroughly enjoyed working with you. You offered this pilot truly unparalleled experience that will help government agencies and private-sector companies on the front lines of the cyber battlespace to adopt the mindset of operational resilience. Cyberattacks are inevitable; this paper helps demonstrate how companies can truly be prepared to work through them.

Adam Firestone
Chief Engineering Officer
CyLogic

Secure the Data, Not the Device: How Decentralized File Storage Creates Resilience Against the Risk of Ransomware Attacks

About the Author

Dr. Georgianna "George" Shea serves as chief technologist for FDD's Center on Cyber and Technology Innovation and TCIL. In that role, she identifies cyber vulnerabilities in the U.S. government and private sector, devising pilot projects to demonstrate feasible technology and non-tech solutions that if scaled, could move the needle in defending U.S. prosperity, security, and innovation.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects that begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab