WHITE PAPER

Ransomware: A Threat to National Security

A guide for U.S. Federal agencies to mitigate ransomware attacks.

Contents

Public Sector: Ransomware's Next Target

Until recently, ransomware was viewed as an attempt for unknown entities to attack corporate networks and seize control of critical systems and data in return for payment. In the last year alone, oil pipelines, meat producers, transit systems, governments, and media organizations around the globe have all become targets. U.S. federal, state, and local agencies are not immune to these attacks. As cybersecurity initiatives have jumped to the forefront, the White House issued guidance on how to deal with ransomware. And the Institute of Security and Technology recently commissioned a Ransomware Task Force to form a best-practices framework for the public and private sector.

Protecting Data: A Core Mission for All Agencies

Agencies across the nation are tasked with fulfilling diverse missions, serving citizens in an evolving world, and protecting citizen and agency data. Fulfilling these tasks was already a tremendous undertaking before Covid-19. But the pandemic has caused Federal leaders to rethink how they run their agencies and fulfill their missions. Covid-19 thrust federal workers into a work-from-home environment, IT teams had to manage devices and data spread across the country, and the need for digital transformation initiatives for citizen services increased rapidly. These issues have made the mission of securing our federal data and systems even more daunting. Network and security architecture can no longer simply focus on securing the perimeter; users and data are dispersed across the nation. Data and applications are spread across on-premises and cloud systems, and the amount of data being created has never been greater.

In 2020, almost 2,400 U.S.–based government agencies, healthcare facilities, and schools experienced ransomware attacks, according to a report from the Ransomware Task Force. Ransomware attacks have been on the rise across public sector organizations. And the level of sophistication is increasing. As a result, government agencies, educational institutions, and healthcare systems have been hit hard with attacks at an average cost of $760,000—and that cost is rising according to Sophos in The State of Ransomware 2020.

There's no end in sight. With virtually no industry spared, the question isn't if you'll be compromised—it's when. Proper education and preparation can help you combat the threat. It's not easy, but fighting ransomware is a battle you can win. The White House has stated that organizations should not pay foreign actors and cybercriminals. FBI Director Christopher Wray recently said, "We must meet ransomware with the same kind of response that authorities took to terrorism after the 9/11 attack." In a recent publication by CISA and a White House press release, both agencies note that regularly backing up systems is a crucial step in ensuring resilience against ransomware.

Limitations of Current Data Protection Systems

Backups safeguard critical data against common scenarios such as natural or human-created disasters, data corruption, or accidental deletions. Ransomware attacks can stress existing data-protection infrastructure built on legacy architectures, such as disk and tape, more than expected. If you're already struggling to meet recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. An attack can also compromise your backup systems and data, requiring you to reinstall and reconfigure your backup solution before even contemplating data recovery.

Defending against Ransomware

The ever-increasing rate of ransomware attacks demands that agencies have a comprehensive approach to defend against such threats. This defense needs:

- Inclusion of cybersecurity awareness and education for employees since many attacks launch through human interaction
- Collaboration between cybersecurity, systems, and data protection teams to harden infrastructures
- A response plan that is easy to execute from backups that can be kept secure and validated if recovery is required

> "We must meet ransomware with the same kind of response that authorities took to terrorism after the 9/11 attack."
>
> **CHRISTOPHER WRAY, FBI DIRECTOR**

Enter Pure Storage FlashBlade®

Pure Storage FlashBlade is the modern-data platform built for backups and rapid restoration of critical data. FlashBlade is an advanced unified fast file and object (UFFO) storage platform designed to consolidate data silos like backup appliances and data lakes. Its high performance and broad feature set are the foundation for a data hub that can deliver significant value for workloads beyond data protection, including analytics, AI, TestDev, and more. FlashBlade is deployed across civilian, defense, and intelligence agencies and supports diverse missions across the world.

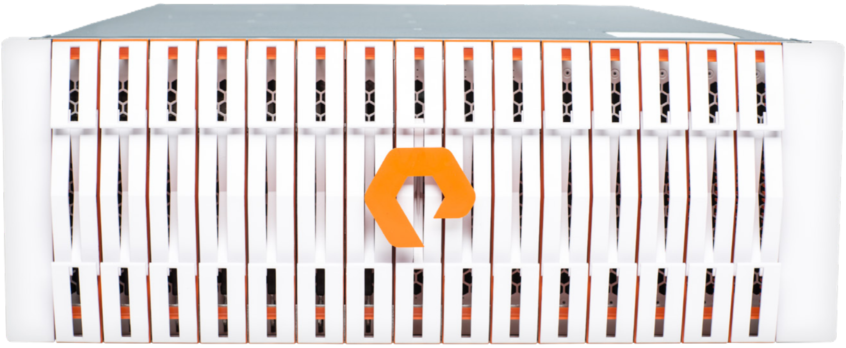

Figure 1: Pure Storage FlashBlade

Pure Storage SafeMode™ Snapshots

Backups safeguard critical data against common scenarios like disasters, data corruption, or accidental deletions. But ransomware can stress existing data-protection infrastructure even more. Pure SafeMode™ snapshots, available with FlashBlade and FlashArray™ storage systems, provide immutability to help recover data backups from ransomware attacks quickly and effectively.

Pure SafeMode snapshots protect backup data and backup metadata by creating a secure copy. Ransomware can't eradicate, modify, or encrypt SafeMode snapshots, even with admin credentials.

In an unpredictable world, you're covered 24x7x365. Snapshot scheduling and retention are fully customizable and easy to deploy. SafeMode snapshots are a built-in feature of FlashArray and FlashBlade systems that enable you to create read-only snapshots of backup data and associated metadata catalogs after you've performed backups.

SafeMode snapshots are created and managed automatically, independent of administrator control. You can recover primary or backup data directly from these snapshots, helping guard against attacks by ransomware, activities of rogue administrators or employees, and even accidental deletion where original copies are corrupted or no longer available to facilitate a restore. Expand and upgrade without disruption. And there's no need to change your backup software. Simply set it and forget it.

Key features of SafeMode snapshots include:

- **Enhanced Protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots. Only an authorized designee from your organization working directly with Pure Storage technical support can configure, modify policies, or manually eradicate snapshots.
- **Simplicity:** SafeMode setup is very simple and requires no daily operational overhead to maintain.
- **Backup Integration:** Agencies can utilize the same snapshot process regardless of the backup product or native utility used to manage data protection processes. Pure Storage supports Cohesity, Veeam, Commvault, Veritas, Rubrik, and many other backup products.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable.
- **Rapid Restore:** Ransomware uniquely challenges backup systems to recover potentially massive amounts of data. FlashBlade helps organizations leverage a parallel architecture with elastic performance that scales with data to speed backup and recovery.
- **Investment Protection:** All Pure FlashBlade and FlashArray systems include SafeMode snapshots at no extra charge. A current Pure subscription or maintenance support contract covers enhancements.

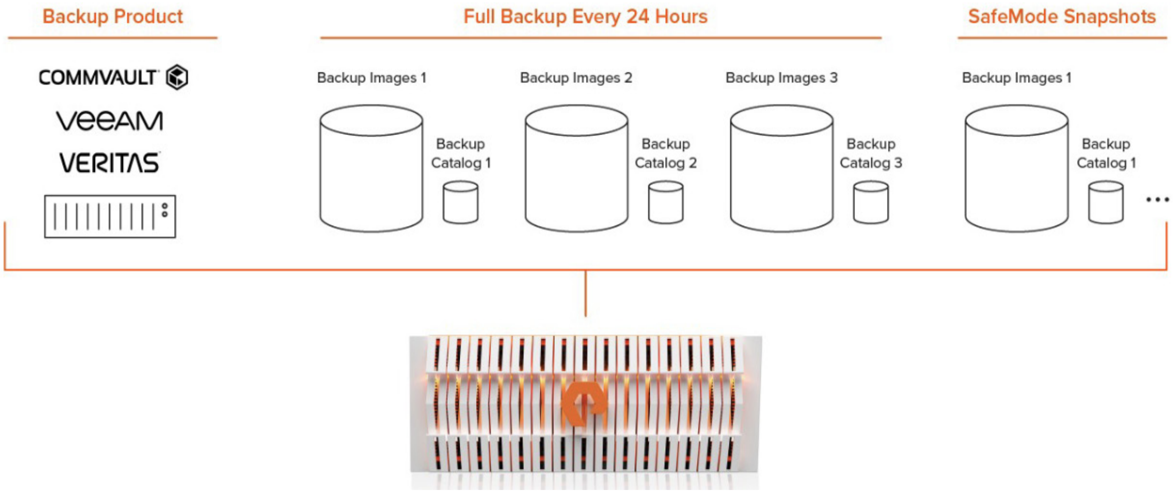

Figure 2: Day-to-day operations create read-only snapshots of backup images and metadata catalog.

Case Study: City of New Orleans Ransomware Attack

Agency Issue: After shutting down hundreds of servers to mitigate damage from a cyberattack, the City of New Orleans needed a new IT infrastructure to test, cleanse, and store data. Within days, Pure Storage helped the IT team migrate data to Pure Storage FlashArray NVME and FlashBlade object storage. The new storage lowers risk with fast backup, restore, and data snapshots.

Pure Storage Solution: Pure Storage FlashArray replicates data to a second data center for fast backup and restore. Pure Storage FlashBlade, with the SafeMode snapshots feature, protects the city's data backups from further ransomware attacks. Kimberly Lagrue, CIO for the City of New Orleans, states, "Our investment in Pure has more than proven its short-term worth, but we're in it for the long-term value it provides to our citizens."

How Pure accelerated time to value for the agency's mission initiatives:

- Accelerates time to value with storage that is easy to deploy and manage
- Provides an additional layer of protection from ransomware attacks
- Minimizes disruption of delivering critical services and data to citizens

How Pure enabled IT Transformation:

- New storage required minimal learning curve, accelerating time to value
- Migrated data to Pure storage platforms quickly and efficiently
- Lowered risk with space-saving snapshots, plus faster backup and restore

Read more about how the City of New Orleans protects its data from cyberattacks.

Conclusion

Ransomware has put leaders across all Federal agencies on the clock: They are expected to have plans and systems in place to ensure critical data is immune to threats from bad actors (both foreign and domestic). Are you prepared to protect one of your agency's most valuable assets: Data? Contact Pure to learn more about mitigating ransomware attacks before they occur.

Additional Resources

- Learn more about how Pure can help protect your agency from ransomware.
- View additional resources on combating ransomware in the public sector.
- Learn why FlashBlade is the unified fast file and object platform that delivers a Modern Data Experience™.

About the Author

Zach Duncan has been helping Federal agencies align technology to strategic missions across civilian, DOD, and intelligence agencies for years. He believes that ensuring efficient use of taxpayer dollars while driving the Federal government to utilize best-of-breed technologies is tantamount. Currently, Zach is a specialist for unstructured data and supports the Pure teams that support the entirety of the Federal Government.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. PURE STORAGE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Pure Storage, Inc.
650 Castro Street, #400
Mountain View, CA 94041