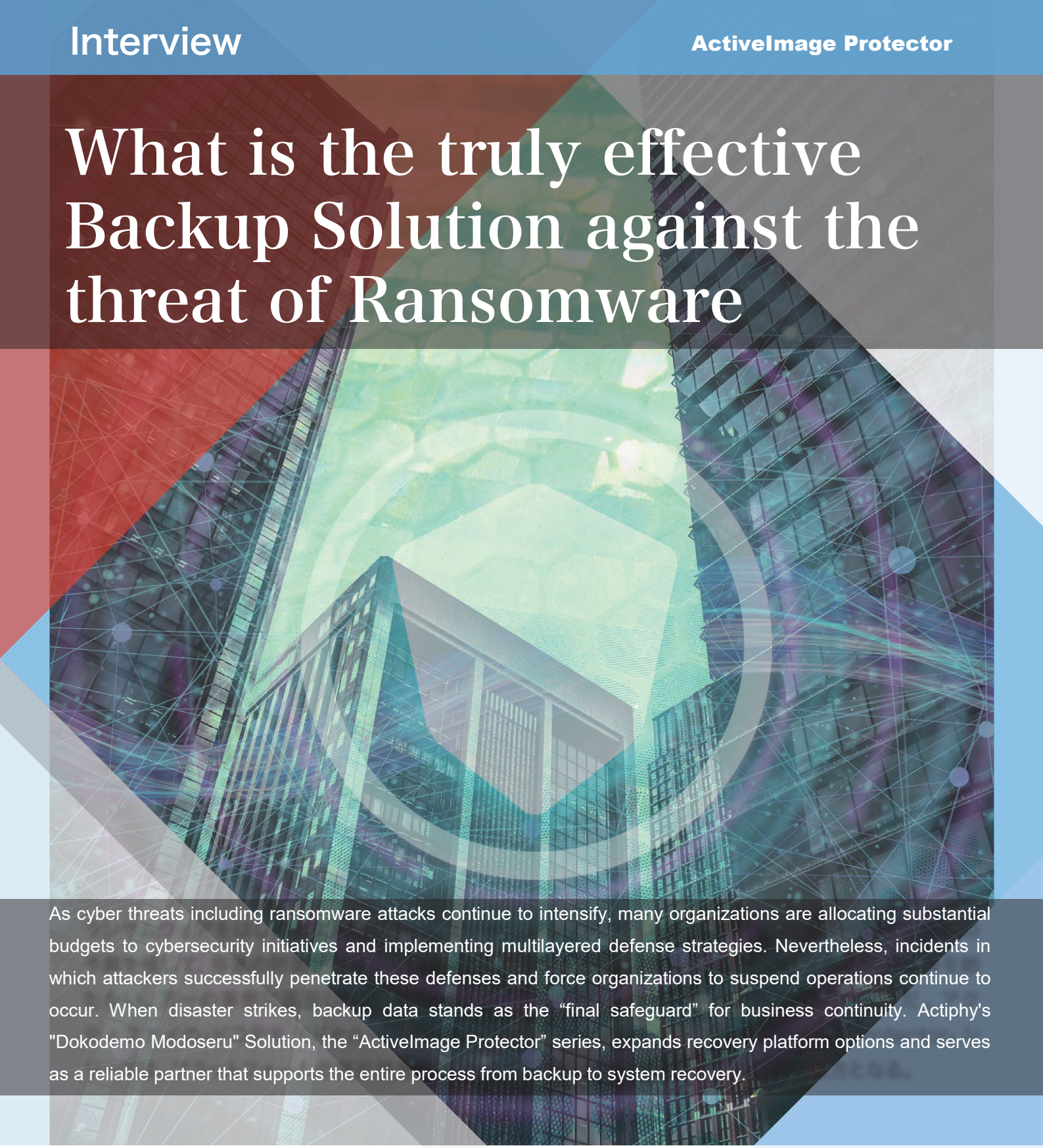
What is the truly effective Backup Solution against the threat of Ransomware



As cyber threats including ransomware attacks continue to intensify, many organizations are allocating substantial budgets to cybersecurity initiatives and implementing multilayered defense strategies. Nevertheless, incidents in which attackers successfully penetrate these defenses and force organizations to suspend operations continue to occur. When disaster strikes, backup data stands as the “final safeguard” for business continuity. Actiphy's "Dokodemo Modoseru" Solution, the “ActiveImage Protector” series, expands recovery platform options and serves as a reliable partner that supports the entire process from backup to system recovery.

“No Backup, No Security.“ The Growing Threat of Ransomware and the Limits of Prevention

According to the National Police Agency's report, "The Threat Landscape in Cyberspace," the number of reported cyberattack incidents affecting businesses and organizations in 2025 exceeded several hundred cases. The cumulative number of reported incidents since 2020 has surpassed 1,000 cases. More than 60% of these incidents involved small and medium-sized enterprises (SMEs), indicating that cybercriminals are targeting not only large corporations but also SMEs with increasing certainty.

Here, it is important to note that these figures represent only reported incidents while the actual number of incidents is likely to be significantly higher. A wide range of products are available to protect corporate IT systems and networks from cyberattacks. While these solutions are highly effective, they cannot guarantee complete prevention. Shogo Sato, Senior Vice President and CSO, Actiphy, Inc., warns against the industry's overreliance on preventive security measures, stating that "Once an attacker

obtains or creates an account with administrative privileges, even security solutions may be rendered ineffective. Furthermore, many organizations face the risk that backup data stored on network-attached storage (NAS) devices could also be compromised or altered.“

If organizations assume that a ransomware infection will eventually occur despite their defenses, backup data becomes the final safeguard for ensuring business continuity. This is the reason Actiphy emphasizes its philosophy: "No Backup, No Security."

Backup serves as the only dependable method for recovering from various types of system failures, including ransomware attacks, natural disasters, human error, and hardware failures. However, when designing a backup strategy for ransomware protection, saving backup data in immutable storage is a fundamental requirement.

When a company faces an unexpected crisis, the most critical factor in ensuring business continuity is “how quickly it can recover.” However, in many organizations, “taking backups” has become the goal by itself, while there are still many cases where concrete measures for restore operations from those backups have not been properly tested or verified.

Mr. Sato says “Although many companies back up their data to NAS devices, if the company’s systems become infected with ransomware, there is a risk that the backup files on the NAS will also be compromised by ransomware.

Although ActiveImage Protector provides protection for its backup files, relying on this protection alone may not be sufficient against sophisticated ransomware attacks.” Therefore, it is essential to combine the backup solution with an “immutable” storage destination that prevents data from being altered or deleted. In other words, this highlights the need to ensure the security of the backup data itself against attacks.

Furthermore, “dedicated immutable storage solutions are often very costly, making it difficult for many companies, especially small and medium-sized businesses, to adopt. Therefore, it is worth considering the use of Linux-based NAS solutions with built-in immutable capabilities, or S3-compatible object storage that can provide additional benefits for disaster recovery.”

Actiphy, Inc.
Senior Vice President and CSO
Shogo Sato

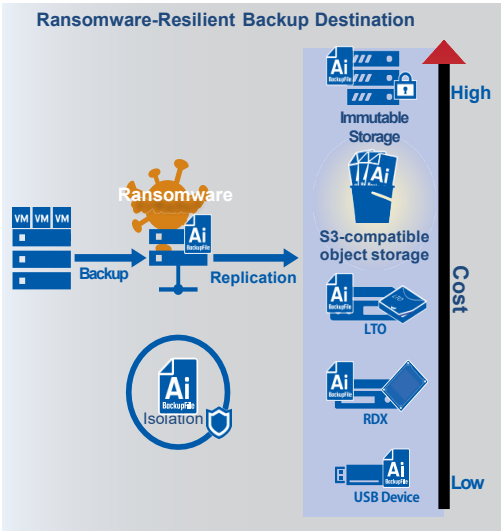
It is important to establish a recovery path by leveraging versioning and object lock capabilities

Actiphy supports a wide range of currently available S3-compatible object storage solutions, allowing versioning and object lock-enabled environments to be utilized as either primary or secondary destinations. With the ActiveImage Protector series, object storage services offered by major public cloud providers can be easily configured as storage destinations, enhancing usability and operational efficiency.

Object Lock is a feature that protects specific versions of data saved in object storage by preventing them from being altered or deleted. When a retention period is configured, the data remains undeletable even by administrators with root privileges until the period expires. This makes Object Lock an effective defense against ransomware attackers attempting to destroy backup data in addition to compromising production systems.

Some object storage services offer relatively low storage costs per unit of storage capacity. In addition, users are relieved of the burden of managing additional hardware. This makes object storage a practical and realistic option for small and medium-sized businesses, which may face significant barriers to adopting costly immutable storage solutions due to their high cost.

Mr. Sato stated, “Object storage provides a good balance of cost-effectiveness and functionality, while it also serves as a disaster recovery solution. Another advantage is the ease with which backup files can be easily transferred over the Internet to locations such as major public cloud and remote data centers. As a countermeasure against ransomware, there has been a growing number of cases in which ActiveImage Protector is proposed in combination with object storage.”



“Secondary Infrastructure” & “Backup Data Adaptability”: Key Considerations in Recovery Planning

To achieve rapid recovery from cyberattacks and maintain business operations, organizations must focus not only on preserving backup data, but also on the concrete steps required to restore their systems.

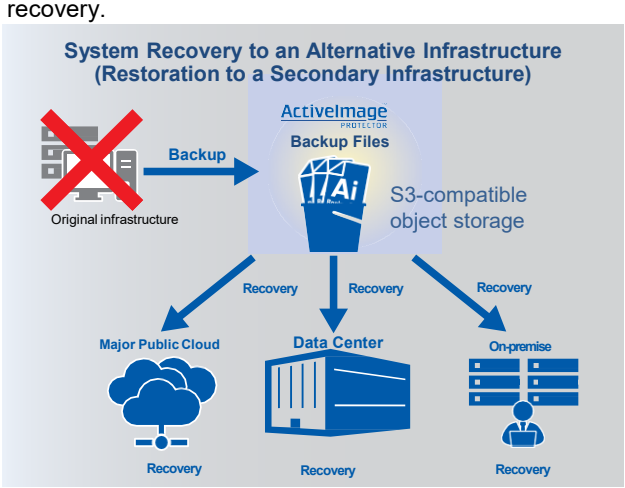
“When an organization falls victim to a ransomware attack, servers and other systems that were part of the affected environment are often isolated for an extended period to investigate the intrusion path, determine whether data have been compromised, and preserve evidence. As a result, they are generally unavailable for use.

In such situations, organizations may need to restore their systems to an alternative infrastructure using backup data in order to maintain business operations. However, most backup software vendors generally do not provide support for this aspect of the recovery process.” according to Mr. Sato.

ActiveImage Protector, Dokodemo Modoseru Solution, offers the features and technical support required to facilitate this stage of recovery.

When migrating on-premises physical or virtual machines to an alternative infrastructure provided by a major cloud service provider or a data center, ActiveImage Protector is implemented with functionality that performs the post-migration processing required for the target environment. Actiphy also provides technical support, including guidance on the specific procedures involved.

To ensure smooth business continuity following a ransomware attack, organizations must make the necessary preparations well in advance. A unique aspect of Actiphy’s approach is its commitment to providing tailored training sessions nationwide, covering not only these topics but also broader best practices for business continuity and disaster recovery.



ActiveImage Protector and Actiphy partner companies will protect the businesses in Japan.

ActiveImage Protector is provided to companies nationwide through sales partners, primarily system integrators (SIers).

Most mid-sized and small businesses in Japan do not employ a large number of in-house IT engineers; as a result, they often rely on external SIers not only for the development and operation of business systems but also for setting up backup systems and implementing security measures.

However, SIers are also facing pressing challenges, including the need to adapt to emerging technologies such as AI. In addition, labor shortages are becoming increasingly severe due to the retirement of experienced engineers, making it difficult to assign dedicated personnel solely to the management of backup solutions.

Mr. Sato said, “We are working to help busy SIers quickly gain the expertise they need regarding our products by offering seminars, enhancing our technical documentation to include detailed procedural guides as well as detailed implementation and operation guides, and strengthening our partner support programs.” At the same time, while continuing to enhance support for SIers who work directly with end users, Mr Sato emphasized the company’s commitment to “further evolving ActiveImage Protector into a solution that truly embodies the concept of the Dokodemo Modoseru (Restore Anywhere) Solution.”

Mr. Sato concluded with confidence “Through the unique feature development and support capabilities that only Actiphy can provide, we will continue to bring to market practical and realistic solutions that help organizations minimize the impact of any type of disruption and achieve effective business continuity planning (BCP).”

This document is a revised and reorganized version of an article in “Weekly BCN+” published on April 6, 2026.

CONTACT

Actiphy Actiphy, Inc.

NCO Kanda-kon’yacho Building, 8 Kanda-kon’yacho, Chiyoda-ku, Tokyo 101-0035, Japan
https://www.actiphy.com global-sales@actiphy.com