TAG

QUESTIONS AND ANSWERS FOR CISOs ON THE NASUNI SOLUTION OFFERING

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

NASUNI

QUESTIONS AND ANSWERS FOR CISOS ON THE NASUNI SOLUTION OFFERING

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This report offers brief answers to common questions modern chief information security officers (CISOs) ask regarding the Nasuni file data protection solution. The objective is to offer practical guidance on how Nasuni supports both security and compliance requirements..

INTRODUCTION

This report provides guidance for chief information security officers (CISOs) in the form of answers to a series of questions commonly posed with respect to the commercial Nasuni offering. This is important because Nasuni offers file data services that are increasingly being utilized in the context of cybersecurity – and the mitigation of ransomware in particular.

The TAG team of analysts was engaged to support this process to ensure that the explanations are consistent with the practical day-to-day concerns of the modern CISO. All vendors, including Nasuni, will offer their own unique perspective, so the discussions below were generated based on live interactions with working CISOs, rather than based on marketing conjecture.

BRIEF OVERVIEW OF NASUNI

Nasuni employs an approach known as UniFS (Universal File System), which serves as the basis for its services. UniFS combines cloud storage with traditional file systems, delivering a scalable solution that utilizes cloud resources to expand storage capacity, enabling businesses to cost-efficiently manage their data growth.

One of Nasuni's features is its data security framework, which includes data encryption support, both in transit and at rest, thus ensuring that sensitive data avoids unauthorized access. Nasuni's continuous versioning and snapshot capabilities facilitate data protection and recovery, which are key elements in any ransomware prevention or response scheme.

Nasuni's customers come from many different industries and are all sizes and shape. Its services help organizations seeking simplified data management, streamlined collaboration, and obviously, support for security requirements driven by ransomware and related data attacks. Nasuni's value proposition can be summarized as follows:

- **Scalable and Agile Data Management** – Nasuni frees enterprises from the constraints of traditional storage solutions, offering a cloud-native architecture that can accommodate data growth while maintaining optimal performance.
- **Rigorous Data Security** – With encryption, versioning, and snapshot capabilities, Nasuni empowers businesses to protect their data from breaches and mishaps – including ransomware, thus improving security posture.
- **Holistic Approach to File Services** – Nasuni's comprehensive platform covers a wide spectrum of data-related needs, including backup, disaster recovery, global file sharing, and remote work enablement.
- **Fast Edge Performance** – Nasuni enables customers to access data everywhere with no changes to apps or user workflows, zero-latency edge performance, smart data synchronization, and elimination of file data duplication and replication costs.

QUESTIONS AND ANSWERS FOR CISOS ON NASUNI

The questions and answers posed below are offered for CISOs and their team members in the context of general enterprise usage. Any highly specialized usage or tailoring of the platform in a local context might result in slightly different answers. For the most part, however, we would expect that the material shared below will be generally useful and applicable.

As suggested earlier, these questions are commonly posed by CISOs to the Nasuni team, and the issues raised are consistent with what TAG sees from CISOs on a daily basis. It should come as no surprise that CISOs gravitate to Nasuni based on ransomware concerns. What occurs after, however, is that they come to appreciate the more general benefits of the platform.

QUESTION: DOES NASUNI PREVENT RANSOMWARE ATTACKS?

ANSWER:

It should come as no surprise that no storage, backup, and recovery solution can prevent ransomware attacks. To properly avoid such incidents, security teams must engage a comprehensive plan that combines protections across all aspects of the infrastructure with dramatic emphasis on simplification of systems and avoidance of complexity. Engaging in the prevention of ransomware is beyond the scope of this report and certainly beyond the scope of what Nasuni brings to the table. What can be said, however, is that Nasuni is an attractive, perhaps even essential, aspect of any security solution that minimizes the consequences of a ransomware attack on the enterprise. Professional and experienced CISOs fully understand the distinction here, but it is worth reinforcing, especially for any less-informed readers, that prevention of an attack and minimization of the consequences are different, but complementary aspects of a working enterprise security program.

Nasuni offers ransomware detection for file activity, attack mitigation, and recovery support. The company's ransomware solution is focused on detecting attacks in real time at the edge. Its detection looks for both known signatures and anomalous behavior that signify ransomware activity at certain thresholds. These activities are then immediately mitigated by isolating them from the rest of the network. The recovery process can handle millions of files in minutes using a patented rapid recovery process based on dialing back an unlimited number of immutable snapshots. This recovery and detection at the edge is an important line of defense for any security stack that has an advantage over traditional storage methods which rely on analyzing and recovering from completed backups.

QUESTION: HOW DOES NASUNI HANDLE DATA ENCRYPTION AND ESCROW?

ANSWER:

CISOs are wise to recognize first that storage, backup, and recovery vendors such as Nasuni will properly leave the data encryption decisions to the data owners. This is no deficiency but is rather an important and desirable design goal. Accordingly, Nasuni offers two options for customers regarding the encryption of their data. First, the encryption scheme can be employed without escrow support from Nasuni, which would leave all obligations for key management and encryption to the customer. Law enforcement requests, for example, to Nasuni for access to data would not be possible for fulfillment, based solely on the non-escrow of keys with Nasuni, which implies non-access. Nasuni does, however, offer a second option for customers who choose to partner with the company on escrow-related operations. In this operational case, Nasuni would provide escrow support, which would oblige Nasuni to provide on-demand support for law enforcement seeking access, should such occasion arise. Obviously, the robustness benefits of outsourced escrow would apply as well, especially during times of great stress, where external assistance truly helps.

QUESTION: HOW DOES NASUNI DEAL WITH INSIDER THREATS FOR ITS OWN ADMINISTRATORS?

ANSWER:

Like all modern companies, including vendors, Nasuni understand the challenges of having insiders who might be disgruntled or compromised. This is a fact of modern business, and it exists in every company, regardless of size or scope. To that end, Nasuni has taken steps to adhere to proper security compliance requirements including the salient aspects of ISO 27001 and SOC 2 assessment. Nasuni also employs a suite of modern security functionality and tools designed to protect against inappropriate data leaks or improper administrative activity. All administrative activity is logged and managed, and the company employs commercial identity and access management solutions using Okta in its infrastructure. CISOs should thus view Nasuni as providing reasonable, state-of-the-art security across its operation, with the observation that security schemes can always be improved.

QUESTION: WHAT SECURITY RISKS EMERGE WITH A SINGLE CONSOLE ACCESS TO STORED DATA IN THE NASUNI CLOUD SERVICE?

ANSWER:

This is a common question from CISOs who might be dependent on the decentralized nature of their unstructured data to provide security-through-obscurity protection of this important base of information. (By the way, this is an ill-advised approach to protecting data scattered across an enterprise.) While Nasuni does offer a means for gaining more centralized reporting and management of this data, the platform addresses this single-point-of-risk by providing support for multiple volumes with access controls that can be deployed to reduce the risk of a single console for all stored unstructured data. This approach can help security teams avoid the reliance on security through obscurity toward a more controlled deployment that supports review, monitoring, and compliance.

QUESTION: IF A DATA LEAK IS EXPERIENCED FOR MY COMPANY, HOW CAN I BE CERTAIN THAT NASUNI WAS NOT INVOLVED IN THE DISCLOSURE?

ANSWER:

Such assurance of non-involvement could never be provided with 100% certainty, so every situation would have to be reviewed to determine root cause. TAG has confirmed, however, that Nasuni offers direct support for customers who are experiencing a security incident and would provide best effort assistance in situations where Nasuni might be helpful. This support would be initiated via the normal ticketing process. Nasuni does have its own incident response plan in case of local situations requiring attention. CISOs are reminded, however, that most breaches targeting their data will tend to occur at the application layer and through interfaces that operate above and beyond the underlying infrastructure. Assuming that the underlying infrastructure could be involved is a reasonable aspect of any analysis during or after a breach, but experience dictates that most attacks operate at the application and data layers.

QUESTION: WHAT SUPPORT DOES NASUNI OFFER CISOs WHO HAVE COMPLIANCE AND QUESTIONNAIRE REQUIREMENTS AROUND DATA STORAGE SECURITY?

ANSWER:

Nasuni offers pre-completed compliance answers to typical questionnaires made available through trustcenter.nasuni.com. This includes support through OneTrust and CyberGRX, and information can be obtained from Nasuni on demand. This is an increasingly common question, by the way, despite the straightforward nature of the inquiry. Sadly, many CISOs are spending a greater portion of their time dealing with compliance inquiries and offering detailed answers to long questionnaires on commercial governance, risk, and compliance (GRC) platforms. Nasuni cannot help customer avoid this trend, but they do have useful resources to help with the answering and response process.

QUESTION: WHAT ARE THE GEOGRAPHIC FOOTPRINTS FOR PHYSICAL STORAGE OF DATA IN THE NASUNI CLOUD?

ANSWER:

Nasuni is back ended by Amazon Web Services, Microsoft Azure, and Google Cloud Platform. The customer works their own hosting deal with the major service provider to ensure compliance with any physical facility requirements, and Nasuni offers its solution consistent with design and deployment decisions made by the customer. Nasuni should not introduce any geographic problems for customers who are required by law to host in a particular country. Nasuni services work independently of this arrangement.

QUESTION: HAS NASUNI EVER HAD ANY PUBLICLY REPORTED CYBERSECURITY INCIDENTS OR BREACHES?

ANSWER:

To date, the TAG analysts have been unable to identify any publicly reported breaches for Nasuni. As any expert knows, this provides a level of confidence that extends only to known and reported breaches, but it is nevertheless a good result. Discussions with Nasuni confirm that no major breaches have had to be reported publicly. This is not to say, however, that no cyber vulnerabilities, minor incidents, and other security situation have every occurred, for this would be inconsistent with any company operating non-trivial infrastructure. From what TAG can see, however, the track record to date has been good.

QUESTION: WHAT IS THE NASUNI CYBERSECURITY ARCHITECTURE FOR ITS INFRASTRUCTURE PROTECTION?

ANSWER:

This is question best answered by customer through perusal of two excellent reports provided by Nasuni on its data security solutions. The first white paper covers the Nasuni Access Anywhere Security Model and offers an overview of the Nasuni Access Anywhere solution. The second white paper covers the Nasuni File Data Platform which is designed to leverage cloud object storage. Both documents are updated frequently by Nasuni and provide technical and operational insights into the security design decisions embedded in the platform.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc.." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: Nasuni commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.