ESG SHOWCASE

Bolstering Your Cyber Resilience with Veritas

Date: September 2021 **Authors:** Christophe Bertrand, Senior Analyst; and Monya Keane, Senior Research Analyst

ABSTRACT: IT organizations are constantly challenged by the risk of cyber-attacks and the resulting severe impact on business operations when an attack occurs. Establishing a strong foundation to protect, detect, and recover from these events is crucial. That's where Veritas can help with a set of proven and differentiated technologies that all IT professionals should have in their toolset for combatting cyber-criminals.

Market Landscape

ESG research confirms what we already know from watching the news: ransomware attack frequency is high. This year, 18% of organizations reported experiencing daily attacks, and 24% are being attacked on a weekly basis.[1] These attacks have a direct negative consequence in the form of downtime. Downtime is expensive, and it affects a whole organization, not just IT. Consider that on average, one in three business applications is deemed to be mission-critical, according to ESG research. Fifteen percent of those apps are so important that they can tolerate no downtime at all, and the estimated mean for tolerable downtime for mission-critical applications is just two hours.[2]

But it's not just production environments at risk—43% of the IT professionals surveyed by ESG report being very concerned that their organizations' backups also could become infected or corrupted by a ransomware attack (see Figure 1).[3] This concern is leading to action: 47% of ESG survey respondents view fortifying cybersecurity as a business issue driving their organization's tech spending, with 25% also focusing on investing in strengthening their business continuity/disaster recovery programs.[4]

The situation is exacerbated by the severe skill shortages that plague the IT industry. Cybersecurity expertise tops the list—with shortages reported by 48% of respondents—and data protection skill shortages were mentioned by 24%.[5]

Figure 1. Today's Cyber-threat Landscape

Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.
[2] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, August 2020.
[3] Source: ESG Master Survey Results, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.
[4] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[5] ibid.

Leveraging the NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has published the NIST Cybersecurity Framework (see Figure 2) to help organizations assess the cyber-threat risks they face. The framework provides guidance on how both internal and external stakeholders can manage and reduce those risks.

Within this framework, core guidance is organized into five functions, then further subdivided into 23 categories. And in each category, the framework defines a number of subcategories (108 in all) pertaining to cybersecurity outcomes and security controls.

Figure 2. The NIST Framework

Source: NIST.gov

Focus on Protect, Detect, and Recover Using the Veritas Approach

In recent months, Veritas has been using the NIST Framework to identify where its solutions fit in the context of an organization's cyber-resilience strategy. Based on that work, Veritas defined three pillars: protect, detect, and recover. It is in those areas that Veritas is confident it can help businesses quite significantly.

Protect

Organizations need protection software that is all-encompassing. If any one part of an environment is accidentally left exposed to a possible ransomware attack, then essentially you haven't done a good enough job protecting the environment as a whole. Recovery will become more difficult or even impossible. It's notable that many of today's attackers tend to focus not just on capturing data, but also on attacking the infrastructure itself—for example, blowing up businesses' virtual machine environments or targeting specific components of the network.

Immutability

That trend makes immutability absolutely vital. Data that has been made immutable cannot be changed or corrupted by ransomware after the data has been stored. This provides a significant layer of protection. Veritas provides native immutability on its Flex appliances but doesn't stop there. The Flex appliances also feature an independent, tamperproof clock that prevents attackers from artificially accelerating the expiration of images (which is a well-known and particularly unsavory tactic employed by ransomware thieves).

Veritas works with third-party hardware providers including Dell Data Domain and NEC HYDRAstor, interfacing through OST plugin technology. Through the API, the Veritas solution is able to tell the hardware that is receiving the data how long to keep it immutable. Veritas has created two deployment modes. They are:

- Compliance Mode: This is a lockdown mode. No matter what credentials you have, during the predefined duration that you're keeping data immutable, it will remain both immutable and indelible. In other words, no one can delete it, and no one can encrypt it.
- Enterprise Mode: This mode allows IT admins to expire images if concerns arise regarding storage capacity management (which can become a challenge with immutable data). Similar to the "two-man rule" of protection given to nuclear-silo keys, Enterprise Mode requires two sets of administrator credentials for added security.

Please note that the two deployment modes are for the Veritas Flex Appliance immutable storage, not for the OST capabilities.

Air Gapping

Broadly defined, air gapping is the creation of a system, data, or network that has no other interfaces, either wired or wireless, connected to outside networks. For many years, Veritas supported tape air gapping through vaulting and ejectable cartridge media-based solutions. It has long been a proven-reliable methodology. But many organizations today want similar resiliency in a digital form ("e-air gapping," so to speak). Veritas has come up with a way to configure its Auto-Image Replication functionality to mimic a lot of the benefits of traditional tape air gapping.

Specifically, a primary NetBackup backup server writes unidirectionally to NetBackup server #2. Within that second backup server, the deduplicated, encrypted data is held. And the network for outbound services is completely separate from the unidirectional server, thus replicating the functionality of air gapping.

Importantly, that server's credentials can be different, too. Therefore, even if an entire primary production environment is compromised, it doesn't necessarily mean the secondary environment will be affected as well.

And the data is written in an image data format for NetBackup. That means the data is actually *inert*. If any ransomware-encrypted files made their way into your backup images, they're not going to infect the rest of the system. They just rest there as inert images, frozen in time, unable to infect the rest of the environment. And all of the images are isolated from each other, which serves to bolster the strength of this approach even further.

Cloud and S3

NetBackup can be deployed in a cloud environment. NetBackup v9.1 is able to use S3 as a storage target—not just "dumping" data there, but actually being aware of it and communicating with the target to define how long to retain a particular image. No data rehydration is needed, and no third party needs to be involved. The data goes directly to the S3 object bucket and remains deduplicated there. This is a remarkably efficient way to leverage cloud immutable storage targets for ransomware protection.

Detect

Veritas makes sure that organizations can have complete visibility into their entire environment. As mentioned, anything (e.g., workloads or hardware) that IT doesn't know about is at risk. It is dangerous not to have a full, all-seeing view.

Veritas APTARE IT Analytics

Veritas APTARE IT Analytics reports on all the compute elements, storage, physical servers, VMs, and cloud servers across an environment. It also reports on portions of the environment that may be protected by other backup vendors' products—not just Veritas, but also Dell EMC, Rubrik, Cohesity, Veeam, Commvault, etc.

Veritas APTARE IT Analytics also performs anomaly detection that extends just as broadly. It comes with pre-built templates for ransomware anomaly detection, providing automation and ease of use for admins who don't have PhDs in cybersecurity. When you are dealing with hundreds or thousands of VMs, you need a solution such as this one.

Within the backups, Veritas NetBackup performs anomaly detection to determine if an operation took too long, the backup itself is suspiciously large, or the dedupe ratio is different than expected. Those anomalies can be infection markers, and they trigger a report to an admin who can assess and remediate the issue as needed. Over time, it even learns through AI to become better at detecting anomalies and differentiating false positives from real threats.

Other NetBackup capabilities related to phishing mitigation include role-based access control, segmentation of the environment, and multi-factor authentication to prevent a phishing attack from becoming a significant threat. Veritas supports Security Assertion Markup Language (SAML) for multi-factor authentication, thereby extending multi-factor authentication to the NetBackup environment.

Veritas also makes sure that communications can't be spoofed. A certificate-authorization step must take place between clients and backup servers. And on the end-user front, NetBackup offers very granular, role-based access control.

In terms of ransomware that targets backup data, any exfiltration of that data is mitigated with data encryption in transit and at rest. NetBackup is capable of supporting various encryption services.

Veritas Data Insight

For file systems, the Veritas Data Insight solution provides reporting out of the box—with built-in templates designed to find known ransomware file extensions. It also takes a highly granular look at user activity: One of the most common ways ransomware is inserted into an organization is through a phishing attack. Veritas Data Insight tracks usage of files by users and by groups. It recognizes:

- Unusual read operations, indicating exfiltration attacks that would appear first as unusual read activity.
- Unusual write operations, which could be an encryption attack.
- Any unusual activity in which files are being accessed by a user.

When it does, it flags that activity as a potential preliminary attack. You can then nip that attack in the bud by taking advantage of this granular view of user activity.

Recover

You need *options* for recovery. Sometimes what is encrypted is a particular server that has a database running. Maybe it's a particular file system or set of files. But maybe servers elsewhere in your environment are on a different VM farm or on AWS or Azure that could, in theory, run the workload.

Granular Recovery

Veritas is able to offer very rapid, granular recovery—bare-metal restoration of physical servers, plus restoration of onsite VMs, cloud VMs, and Kubernetes containers.

This recovery extends to individually targeted systems. If the server itself is encrypted, NetBackup can do a full bare-metal restore of that entire server. It also does bulk rapid recovery. With Instant Rollback, instead of doing a complete restore, Veritas came up with a way to couple the new continuous data protection included in the latest version of its flagship software with rollback functionality. It sends relatively little data, yet still gets a full VM running again quickly.

Cloud

As mentioned, Veritas possesses strong capabilities related to writing and storing data efficiently in a deduplicated state to S3 immutable storage. Leveraging that efficiently stored data, Veritas is capable of standing up a data center on demand in the cloud: What had been a secondary or tertiary copy of data can now be the core of a data center that didn't exist the day before.

This capability saves money during normal operations: You don't have to have it up and running until it is needed. But it also provides the ultimate option of complete data center replacement if required. IT can stand up this environment as an EC2 environment in the cloud created from the deduplicated data. The result is a fully functioning separate data center now available, without incurring always-on compute charges.

Orchestration and Testing

Everything is done in an orchestrated manner via one-click execution. Dozens of servers and different parts of the stack can all be recovered in a specific order. With a single click, you can execute your resiliency plan.

You can also test the plan in a non-impactful way. A plan is only as good as the last time it's been tested. But you're not going to test at all if it's going to take down your production environment. Veritas wants to make sure that you're testing your ransomware-recovery capabilities often and easily.

The Bigger Truth

Ransomware and cyber-risks are not only here to stay, but they are also getting worse. Building a resilient infrastructure that fosters a proactive posture is going to be key to winning this fight. Leveraging the NIST framework, as Veritas has done, is a great way of approaching the problem.

Veritas also offers a differentiated solution. Its robust e-air gapping with Auto Image Replication, the ability to send data deduplicated natively directly to S3 objects, the NetBackup AI/ML engine, the broad reporting, the analytics and alerting capabilities, the granular recovery options, and the advanced orchestration all reflect the amount of thought that Veritas has put into helping its customers and prospects keep their businesses safe from the bad guys.

Veritas delivers significant value by offering solutions that cover the protect, detect, and recover components of the methodology. Collectively speaking, it's all proven technology that will work across a variety of environments at scale.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188