



# IT Security

## Cybersecurity and The Art of Possible

Lynsy Marshall



**Lynsy Marshall**  
Senior Field & Channel  
Marketing Manager for  
the Americas  
Infinidat

### Biography

Lynsy Marshall is the Senior Field & Channel Marketing Manager for the Americas at Infinidat (<https://www.infinidat.com>). Additionally, Marshall is the Marketing Lead for Infinidat Federal (<https://infinidatfederal.com>), a wholly owned subsidiary of Infinidat focused on the U.S. Government.

Prior to joining Infinidat, Marshall led events for both Netcracker and Connectwise, formally Continuum Managed Services.

She has a Bachelor's of Science degree from the University of New Hampshire.

Lynsy blogs at <https://www.infinidat.com/en/blog>

**Keywords** RSA Conference 2024, Cyberattacks, Immutable snapshots, Data recovery, Threat actors, Infinidat  
**Paper type** Opinion

### Abstract

At the upcoming RSA Conference 2024 at the Moscone Centre in San Francisco (May 6-9), the Infinidat team will be engaging with attendees at Booth #263 in the South Hall, and exchanging insights, experiences, and knowledge about how to secure an enterprise storage infrastructure, safeguard against cyberattacks, and, when attacked by threat actors, rapidly recover mission critical data from immutable snapshots in primary storage and secondary storage. With the theme of the RSA 2024 being "The Art of Possible" is it possible to go on vacation to Hawaii with the peace of mind that your enterprise will not get waylaid by a massive cyberattack? The answer is yes, says the author of this article.

### Introduction

Imagine your company is on the verge of being hit by a cyberattack, like the Scattered Spider ransomware attack that has disrupted businesses, corrupted data, and brought enterprises to their knees in takedowns that have cost hundreds of millions of dollars in lost revenue and IT system reconstruction. Malicious actors with highly sophisticated hacking tools take data hostage and demand enormous ransoms. Since any enterprise – including yours – can be hit unexpectedly at any time amid an ever-increasing threat window, are you awake all night long pondering if your organization's data could be taken hostage and exploited, or do you go on vacation to Hawaii?



IT Security

Hint: Pack your bags ... if you're using Infinidat's cyber resilience, cyber detection, and cyber recovery capabilities in your enterprise storage environment.

The key to success is having the right level of enterprise cyber storage resilience and recovery. We are so confident in Infinidat's cyber secure storage solutions that – and here's where it gets really fun – we'll be running a sweepstakes in our booth at RSA for a chance to win \$2,500 that you can spend on vacation in Hawaii.

You might be wondering how we can be so confident and so at ease. While cybercriminals may never take a break, you can take a break as an Infinidat customer or one of our partners. It doesn't matter if the onslaught of ransomware, malware and other cyberattacks persists. Infinidat has your back.



**“Queen of the Hackers”**

With cybercrime projected by Cybersecurity Ventures to cost \$9.5 trillion<sup>1</sup> by the end of 2024, Rachel Wilson, the Head of Cybersecurity at Morgan Stanley Wealth Management, was a keynote for one of our webinars at Infinidat, asserting that everyone is living in “a brave new world” in which enterprises need to be more cyber resilient against the increase in cyberattacks.

“The rise in cybercriminal syndicates has been dramatic over the last few years,” Rachel said in a sobering statement. “Now, 70% of malicious cyber activity we see on the Internet is criminal in nature and financially motivated. It’s opportunistic and it’s egalitarian.” In other words, cyber criminals will hit any enterprise at any time for any reason that profits them. They are equal opportunist hackers.



Nicknamed the “queen of the hackers” when she led a team of elite cybersecurity experts protecting the United States, Rachel spent 15 years working for the National Security Agency (NSA). She says that any entity with data is a potential target. AI has dramatically lowered the barrier to entry for cyber actors. “Lowering that barrier to entry has increased the scope, scale and velocity of cyber action we’ve seen across the board,” she added.

The reasons for her sleepless nights over cybersecurity issues today are becoming more diverse. Among them are ransomware and knowing the right level of cyber resilience to have in your data infrastructure.



“Ransomware is the most lucrative cyberattack in history,” Rachel stated on Infinidat’s eye-opening webinar. “Hacker calls, ‘Hi, Happy Monday, you’ll see that I am in your environment. I’ve encrypted all your systems. If you want your data back, if you want your systems restored, I’m going to need \$500,000 in this cryptocurrency equivalent, in this South African bitcoin wallet by 2 o’clock this afternoon. And if you don’t pay by 2 o’clock, make it \$600,000. We’ll keep ratcheting up that ransom until you are willing to pay.”

Rachel has unequivocal advice in our webinar<sup>2</sup> that is available for on-demand viewing: “Now, I can tell you as someone in the cybersecurity business for 25 years, we never recommend paying the ransom. What happens when you pay the ransom is that you have told the world that you are someone willing to pay a ransom, and the hackers will just keep coming back.”





### What are you to do?

Hackers are looking for vulnerabilities in your enterprise data infrastructure. To combat it, enterprises need the appropriate level of cyber storage resilience and recovery to match the level of threat and make sure primary storage and secondary storage systems are battle-hardened and hacker-proof. Too many enterprises lack cyber resilience, or they think what they have is better than it actually is. Advancements in enterprise cyber storage resilience and recovery capabilities have been catapulted forward in the last 18 months.

Our channel partners who assist enterprises understand that a cybercriminal's ability to cripple an organization by encrypting, corrupting, and exposing sensitive data must be taken out of their hands. It's highly advisable to loop in partners who can help implement a solution that will keep you a step ahead of the threat.

The answer is a combination of cyber detection, cyber resilience, and cyber recovery. When you can retrieve a known good copy of data that is clean and trustworthy, you can rapidly recover your enterprise data. This eliminates the leverage and the power that cybercriminals have over enterprises that have been compromised. It turns "just rolling the dice" with the cyber resilience capabilities in your data infrastructure into a sure bet.

To make sure that the data is uncompromised, you need strong cyber detection capabilities on a storage platform. This is where artificial intelligence (AI) and machine learning (ML) comes into play. The self-learning automation is a vital part of allowing you to take that much-needed vacation, even when it seems like cyberattacks are coming 24/7. Infinidat has devised new strategies to unlock the power of cybersecurity within the storage infrastructure. The Infinidat team will be talking about this exact scenario at our Hawaiian-themed "oasis" at RSA 2024.



**INFINIDAT** RSAConference2024

**Join us at RSA!**

Cyber criminals never take a break, but you can! Visit us and learn how we are always protecting, defending and recovering your data.

Booth #263, South Hall | May 6-9 | Moscone Center, San Francisco

We encourage you to come by our Infinidat Booth #263 in the South Hall at the Moscone Centre and enter our sweepstakes for a chance to win \$2,500 for your vacation. We'd love to see you at one of the biggest cybersecurity conferences of the year. Just look for the booth with the palm trees and cyber resilient storage experts in Hawaiian shirts.

Aloha! We'll keep the storage on for you.

#### Reference

- <sup>1</sup> Morgan, S. (25 October 2023), Cybercrime To Cost The World \$9.5 Trillion USD Annually In 2024. Cybercrime Magazine. Available at <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/>
- <sup>2</sup> [https://www.youtube.com/watch?v=-bltQU4IEwk&list=PLyQfubVs1\\_nVfdiynQW-Y3zpGWH3Duo7&index=4](https://www.youtube.com/watch?v=-bltQU4IEwk&list=PLyQfubVs1_nVfdiynQW-Y3zpGWH3Duo7&index=4)