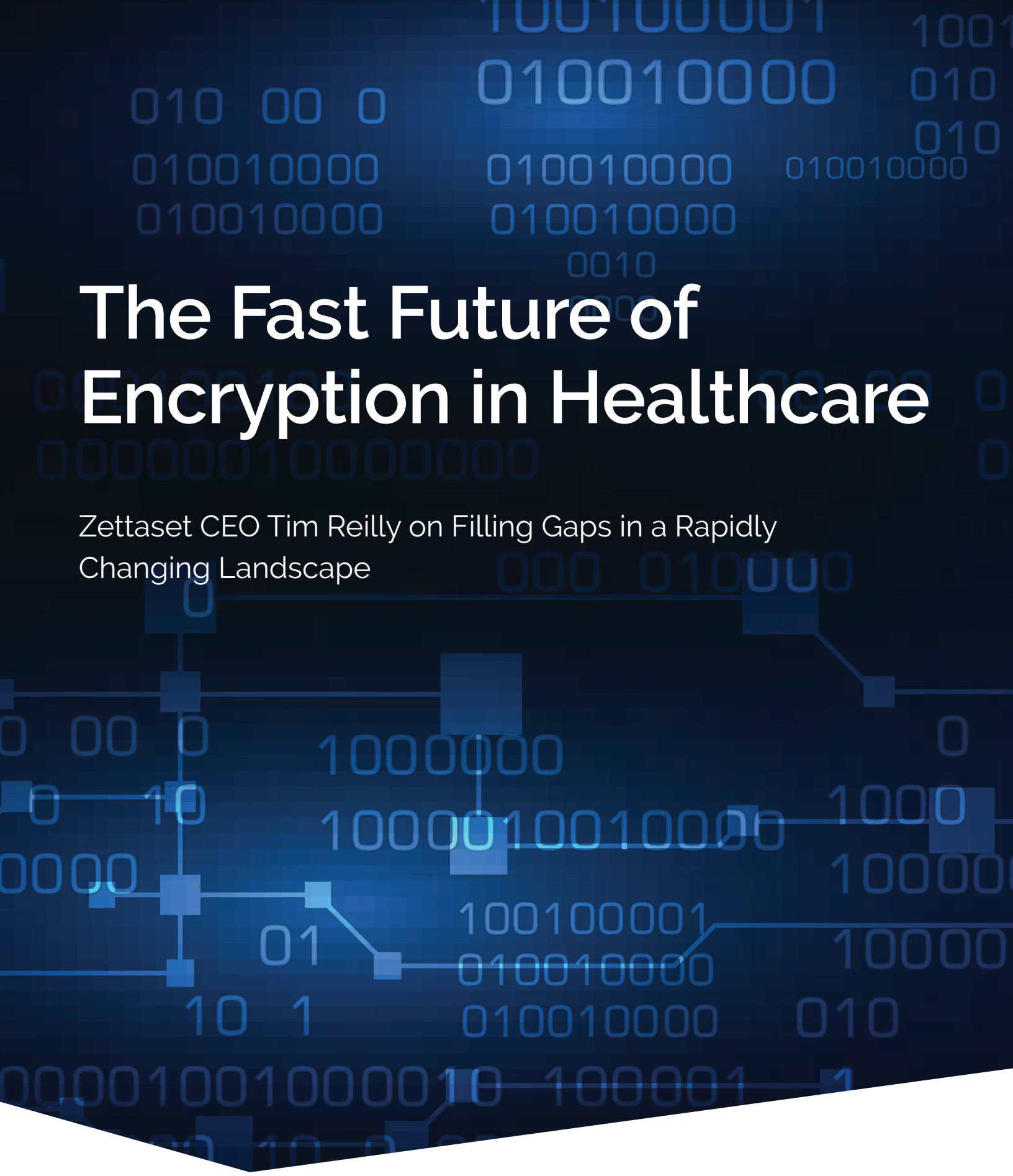
The Fast Future of Encryption in Healthcare

Zettaset CEO Tim Reilly on Filling Gaps in a Rapidly Changing Landscape



Zettaset

ISMG INFORMATION SECURITY MEDIA GROUP

Zettaset


Tim Reilly

Reilly has more than 25 years of successful experience in the high-tech industry filling key operational roles within product line business units and venture capital-funded companies through all stages of growth. During his time at Zettaset, the company has grown its software-defined encryption portfolio to provide a comprehensive data protection solution across all physical, virtual and cloud environments. Prior to joining Zettaset, he was vice president of finance and operations at Trapeze Networks.

In mere weeks, as a result of the pandemic, the healthcare industry was able to leapfrog ahead years in its digital transformation. But this came at a price to data security, which now faces new kinds of exposure. Zettaset CEO **Tim Reilly** discusses these vulnerabilities and the future of encryption in the healthcare sector.

Encryption was a healthcare challenge prior to the pandemic, Reilly points out. And the advent of a remote workforce and new telehealth initiatives have only exacerbated the issue. In an interview with Tom Field of Information Security Media Group, Reilly discusses:

- The data security impact of rapid digital transformation;
- The future of encryption in healthcare;
- Why 2020 is a “breakout year” for Zettaset.

A Rapid Transformation

TOM FIELD: The healthcare sector has undergone an unprecedented digital transformation over the past quarter year. In fact, many of them did it over a weekend in March. What would you say are the ramifications for data security of this rapid transformation?

TIM REILLY: Healthcare needs to be at the forefront, especially during a pandemic like this. The question becomes, with more data being generated, what do we do with it, especially since there’s telehealth now, and all of these connected devices? A university hospital we’ve talked to recently said they’ve seen a huge increase in online appointments. Now imagine how much data that is. So here you are stuck in the middle of a legacy system with all of the data that still needs to be encrypted, and now comes this new world … and it’s not going to stop.

In March, the HHS Office for Civil Rights waived certain HIPAA requirements to help enable telehealth. They knew that there was no way they could respond to this pandemic and still keep all the security checks in place. And that’s where the concern comes in.

The top three verticals that need encryption are: federal, financial and healthcare. Federal agencies protect our way of life and our infrastructure. Financial institutions protect our money. The healthcare industry protects pretty much everything about our wellbeing – who we are, all of our personal secrets. And out of all three, which one is the least encrypted? It’s healthcare.

Healthcare data is being generated at a rapid rate beyond anything we comprehended. And the need to provide urgent services during the pandemic has caused security to be cast to the wind to a certain extent.

Encryption was never seen as that first or second security item. Instead, the priority was always identity access control and monitoring. Data security is essential, and encryption needs to be there, but it wasn’t seen as a priority before – and it definitely isn’t right now.

The Threat Landscape

FIELD: How do you see data being exposed in new ways in today’s new healthcare threat landscape?

REILLY: The digital transformation has created new initiatives that say, “Hey look, I’ve got all this data. There has to be a way to slice and dice it that gives me analytics and gets value for me and gets value for the end user and the patients.”

DevOps is one of the main methodologies for how to get there. Two of the main technologies are containers and Kubernetes. Essentially, you’re taking everything and putting it in a container, so you don’t have to have an entire server virtualized. You just have a container that deals with exactly what you need. What happens when you have 700 instances of people at the edge, their devices might go through Epic or Cerner health information systems, and it goes back to their database. Now all of a sudden you have those little instances all over these boxed out servers, and if you get into one, you get into all of them. So containers have a hole there. Kubernetes does its best to manage those containers and orchestrate them over thousands of servers. But if an attacker gets in and gets to the access management key and decrypts it, they can get free reign to all of that.

That is a huge exposure. And you’ll never completely stop it. But you need to make sure you have things encrypted, and you need to make sure you limit what people can get to. While we have to align ourselves with access management and monitoring and audit and logging vendors, we also need encryption. It’s the third leg of the stool. We were able to re-architect from the ground up to use encryption to protect in these new environments.

Often, encryption is an afterthought. If you’re now in this triage mode where you’ve got devices everywhere and you’re still trying to leverage this new technology, you’re exposed beyond all belief.

Gaps in Legacy Systems

FIELD: What are the biggest gaps that you see in legacy systems?

REILLY: DBAs have to make sure the servers work, they provide the reports and the data in the right form and they have basic protection.

Of course, to comply with HIPAA and avoid having a breach posted on the HHS “wall of shame” tally, be sure you’re using encryption.

Our company is able to do encryption for data in place, which means an organization can just install it wherever the data is, and it’s instantly encrypted. This is where we can provide a lot of value.

You don’t see people at the top of organizations taking the need for encryption seriously until it’s too late. Our hope is that if we make it simple enough, and if our software doesn’t impact performance and it’s easy to install and maintain at a favorable cost, more organizations will adopt it.

If suddenly encryption is as easy as passwords, why wouldn’t you do it?

The Future of Encryption

FIELD: What is the future of encryption in the healthcare sector?

REILLY: Multifactor authentication means your identity and access management will be effective. The audit and monitoring piece of it will always be a cat-and-mouse game. If an attacker gets through those two lines of defense, then you have the castle and you have the moat, drawbridge, the walls, the guards and the search towers. But if you can get inside, you have free reign. So you've got to protect the data itself.

My concern is everyone's so focused on the infrastructure right now, they're forgetting about protecting the data with encryption.

You see the larger companies, like Red Hat, VMware, HPE, as well as the three cloud providers, all really embrace these new technologies. They're right to embrace it. It is the future. If you don't learn from history, you're doomed to repeat it.

With legacy systems, it wasn't completely adopted. Hopefully this time around, people like me and everyone else in the industry are raising a flag, going, "Guys, let's do it right from the beginning."

Securing the data needs to be put in the front for once, and we have that ability finally. Think about it. If you're just about to implement Kubernetes and DevOps, and deploy containers, we can say, "Hey, look. Haven't you been scared enough already? We can help encrypt you and get your organization ahead of the game." I see the digital transformation pushing the limits of optimization of DevOps and any other technology. I'm sure there'll be something else beyond Kubernetes and containers. But I would say the race for the golden goose is, "How do I take all this data, optimize, save myself money, provide value and yet still protect my data?"

The future is this tech and I hope this time around there is more of an emphasis on security.

Zettaset's Role

FIELD: Talk to me about Zettaset for a moment. How are you helping healthcare entities to protect their data?

REILLY: We have customers that collect data from all the major health providers, and all of them are required to have business associate agreements, which is what you're responsible for under HIPAA if you touch PHI data. Some providers are telling their vendors: "No, you're not getting any more of our data until it's encrypted."

Some of these vendors have been around for 10 years. Why haven't they encrypted data to this day? So suddenly there is an emphasis on encryption because of HIPAA-related fines and because of the threats that are out there and the damage that can be done to the reputation of the business. Plus, customers are requiring their data to be encrypted.

On top of that, let's not forget the key management piece of it. We have a key manager; it's virtual software. We have a comprehensive solution. We want you to use our crypto. You can use somebody else's key manager, but if you don't want to, you can use ours. It installs easily and it's easy to maintain. And now you can control the keys. You don't have to be an expert. It's transparent to the end user, and it does it without impacting performance.

> "Zettaset will be providing de facto encryption across all of DevOps."

On the other side of it, we saw the future coming with DevOps, and we got ahead of the game, and we had talked with the likes of a Docker about encryption. And we asked them, "How are you doing the protection of the data?" And they said, "Really, no one's doing it for us yet." So we went right in and took advantage of that.

And then the container folks said, "Well, Kubernetes is the next hot thing. What are you doing over there?" Well, that's exposed even further than a container, so we created a product for that.

Hopefully, security this time around is baked in a little bit more. And that's what we call DevSecOps. We want people to go from DevOps to DevSecOps. We're playing a role in that by encrypting the data.

The Future of Zettaset

FIELD: So in 2021, where is Zettaset headed?

REILLY: Zettaset will be providing de facto encryption across all of DevOps. We're going to be able to protect data wherever it is. Like a container, we can spin up encryption and bring it back down. So it's effectively on demand. We will be offering the ability to have it multi-cloud, where you can see everything. It doesn't matter if the container is on premises or in a private or public cloud. We have the ability to move with the container and keep it encrypted. Wherever the data goes, we're going to follow it and protect it.

We have had an interest in a couple of the civilian agencies, and one said: "All right, we are now embracing Kubernetes and DevOps, but we know we can't go any further with the data without having it encrypted." The financial sector sees the need as well.

In healthcare, organizations have all this data and they're starting to adopt the DevOps technologies. They're starting to adopt Kubernetes and containers - and we know that needs to be protected as well.

We're saying, "We can protect your data with encryption, wherever it is, in whatever form, and whatever technology, and however long you need it. Throughout the data lifecycle, we'll be there with you." ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY® Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io