May 4, 2015

DataLocker: Endpoint encryption product developer's time has come

FEATURED STORY THIRDCERTAINTY STAFF

By Rodika Tollefson, ThirdCertainty

As encryption of data at rest becomes a standard practice to protect against data breaches, the security of endpoints, such as external media storage, can prove quite complicated.

One vendor that's been trying to solve that problem is DataLocker—a Kansas City-based, growing tech company that got started with a chance elevator meeting.

"Our core guiding principle is what we call 'simply secure.' We wanted to develop a product that was easy to use," says DataLocker co-founder and CEO Jay Kim.

Security* & *Privacy News Roundup: *Stay informed of key patterns and trends*

DataLocker's line of products includes encrypted external hard drives and flash drives and self-encrypting, recordable CDs and DVDs. All are "plug and play" media that don't require installation of special software.

"We take the biggest root cause of data breaches out of the equation, which is human error," Kim says.

The hard drives, which can hold as much as 2 terabytes of data, come with a touch-screen control panel, are platform-independent, and can connect to any type of computer system.

"The secret sauce behind our hard drive is the fact that you authenticate and administer the device at the device level itself," Kim says.

In 2013, DataLocker added a cloud-encryption gateway, called SkyCrypt, for encrypting data in cloud apps such as Dropbox. And soon, it will launch its newest offering, an encryption-management platform (DataLocker EMP), which will allow users to remotely manage all their encrypted USB-based endpoints.

"We are trying to grow. At the heart of it, we're a product-development company—that's in our DNA," Kim says.

A startup Cinderella story

Jay Kim was running a family pharmaceuticals business and also was involved in steel fabrication when he took a business trip to South Korea in the fall of 2007. He was meeting a friend, who introduced him to another friend in an elevator.

"My buddy here is an inventor," the friend said. "He has a great invention, would you like to look at it?"

Kim says he didn't know anything about data security or encryption, but became convinced that the inventor, David Kim (no relation), was on to something. So he divested of his real estate portfolio and invested in what would become DataLocker.

Two months later, thanks to a serendipitous cancellation, DataLocker managed to get a booth at the 2008 Consumer Electronics Show in Las Vegas. Kim hired a handful of interns, creating sales collateral and making hasty copies on the way to the airport.

CEO Jay Kim demos a product prototype at CES 2008.

Back in 2008, encryption was not a commonly used word.

"Very few people truly understood what it meant," Kim says.

Yet the crowd's response was highly enthusiastic. MSNBC even named DataLocker one of the top business products at CES, and shortly after the phone began ringing.

There was just one small problem. Two months after shipping the first orders, the company got a call from a United Kingdom customer. The company's forensics person hacked the device in five minutes. The device wasn't truly encrypted, protected instead by a password.

"We basically had a diary lock on a hard drive, a very simple diary lock," he says.

Faced with the decision of either investing much more money into making a truly encrypted product, or calling it quits, Kim chose the former. DataLocker went into full research and development mode for more than two years, coming out of R&D in 2010.

DataLocker has been growing 70 percent every year since.

It had several other "elevator moments" along the way.

Through one of Kansas state's entrepreneur programs, Kim met mentor Gary Fish, founder of FishNet Security. During a breakfast meeting, Kim told him about his company and was asked by Fish how much funding he needed.

Two weeks later, Fish called back to offer $1.2 million in investment from him and two others.

"This is in 2010, when not many investors were writing checks," Kim says.

Entering growth mode

The company has been profitable since 2013, and Kim no longer considers it a startup. Its products are used for storing and transporting anything from forensic evidence collected in the field and tactical satellite imagery, to medical images.

The military was among DataLocker's first customers, and still one of the largest.

As DataLocker was entering the market, the U.S. government banned the use of flash drives after a major hacking incident. Someone had used an unauthorized USB drive on a secured network.

"But they approved the use of USB hard drives. So that really opened the door for us," Kim says. "We had the right product at the right time."

In 2011, DataLocker became the first vendor to receive FIPS 140–2 certification from the National Institutes of Standards and Technology—and according to Kim, it's still the only one to have the certification for the entire device. (FIPS 140–2 is a U.S. government security standard for cryptographic modules).

The company does business in 20 countries, and currently has 22 employees.

With the upcoming launch of the DataLocker EMP—which Kim expects out in a few weeks—the company is tapping into new ways to deliver encryption security.

Next up? Most likely mobile devices.

"The roadmap for us is, what's the next place where people store their data?" Kim says. "At the end of the day, we're protecting the data that's stored from unauthorized use, whether it's on the phone, flash drive, Dropbox (etc.)."

With additional reporting by Byron Acohido

More on emerging best practices

Encryption rules ease retailers' burden
Tracking privileged accounts can thwart hackers
Impenetrable encryption locks down Internet of Things

Posted in Cybersecurity, Data Security, Featured Story