Cyber Security Solutions with Hitachi

Darren W Pulsipher, Colin McLean, & David Rowley – Jan 30, 2022

A complete cyber-security solution includes physical protection, prevention, detection, and identity management.

Darren Pulsipher, Chief Solution Architect, Intel, talks to Hitachi's Colin McLean, Intel Global Team Lead, and David Rowley, Senior Solutions Consultant, about Hitachi's full circle cyber security offerings.

HITACHI
Inspire the Next

Video: Youtube Channel
Podcast: SoundCloud

On this episode, Darren talks with Hitachi's Colin McLean, Intel Global Team Lead, and David Rowley, Senior Solutions Consultant, about their full circle cyber security offerings.

Colin has been with Hitachi for almost 24 years after working for IBM right out of college. He is primarily focused on accounts in the Pacific Northwest and SLED accounts. He had the unusual opportunity of taking his father's post when his father retired from Hitachi.

David has been in IT for over twenty years, starting just before the .com craze. He's been a hands-on guy for most of his career, dealing with servers, storage, and security.

Many people think of Hitachi as anything from a large equipment or power tool company to one that produces bread makers. Hitachi is, in fact, a one-hundred-year- old engineering and manufacturing company that started making electric motors in 1910 and has morphed into hundreds of operating organizations and wholly-owned subsidiaries, including Hitachi Vantara. Hitachi Vantara is the largest wholly-owned subsidiary, focused primarily on managing data. They build and deliver not just traditional block enterprise storage systems, but they have grown into a digital solutions company embracing the extreme expansion into IoT and data-driven insights.

Robert Mueller said, "There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again." This quote sets the stage for how Hitachi can help companies. It's not a matter of if, but when, you will be hacked, and when you will be hacked again. This applies not just to companies, but organizations in the public space as well.

Hitachi has a whole federal division that works out of Washington D.C., primarily focused on the Department of Defense and federal accounts. Hitachi Vantara does a lot of work with SLED accounts and works together with the federal division to provide solutions for federal, state, and local requirements.

The best way to visualize a security solution from Hitachi is to imagine your organization as your home, and in that home are four elements of protection that we must deploy.

First is physical security. Hitachi has a smart system, a visual intelligence solution, that can provide video surveillance with intelligence. It can do everything from gunshot detection to license tracking to facial recognition. Hitachi deploys these all across the world. Hitachi cameras picked up on a lot of the events at the Washington Mall last year, and they are used by police organizations all over the country. This has all grown from Hitachi's transportation division, which is highly dependent on video tsechnology for security.

Physical security is not often a topic of discussion, but it is a key aspect. If you can't control your own building and your own data center, then you do not have security. If someone can get through the door, they can get into your data center.

After physical security comes Hitachi ID. This is basically the lock on your front door. A recent survey showed that only 40 percent of companies have privileged access management and about 74 percent have identity management. This is not enough because that is a lot of exposure, and the SLED space is a high-profile target. Hitachi ID provides password privilege and identity solutions across a single platform; this is a total solution where you can identify not only users but devices and applications, on prem and in the cloud.

The third aspect is how to protect your data when someone does get through the door.

Cybersecurity is a big data problem, and Pentaho is the tool for big data. With Pentaho, you can manage all your sources of data, control your data lake, and produce useful outcomes. Hitachi found that data scientists and cybersecurity analysts spend 80 percent of their time just managing, sourcing, and cleaning the data, and only 20 percent of their time actually analyzing it. With Pentaho, those numbers are flipped, and they can spend 80 percent of their time analyzing the data and getting into real-time threat analysis and threat response.

Pentaho is an intrusion detection system, but it is a prevention system as well. For example, one major energy company had done everything ad hoc, writing their own scripts in-house. They re-platformed all of that functionality in Pentaho in one day. Then they were able to do that analysis in real time and keep up with the attackers instead of always coming from behind. What makes Pentaho unique in a crowded field is its flexibility. It can do any kind of data analysis, and it can be based on what your organization needs.

Protecting data from a content perspective is also very important for the SLED space. Hitachi Content Platform Anywhere provides secure file sync and share and a secure dropbox. It's comparable to Google Drive or Dropbox, for example, but the difference is that HCP Anywhere is controlled by your own security team.

It is used by the Department of Defense, which renamed it Mill Drive. Field forces on the ground transmit sensitive data to and from various secret places and back to headquarters for reconnaissance and other missions. On a local level, cities utilize it, transmitting video evidence not only through administration, the police force, and other agencies, but also to the DAs office for evidence management.

HCP Anywhere is built on the Hitachi Content Platform, which is a object storage solution than can run on any storage solution. Instead of overwriting a file, and therefore allowing an attacker to overwrite your file, you make a new version of the file. Then, if you get attacked, you can roll back to an earlier version before the attack happened. Some rating agencies agree that Hitachi's object storage is the best on the market. Out of the box, you get 16 versions of every file, 16 pieces of system metadata, and an unlimited amount of custom metadata tags as well.

Hitachi also has a console for data policy management in addition to the Hitachi Content Platform Gateway, which puts a NAS in front of the object store that can be either NFS or SMB. Added on is Hitachi Content Intelligence; it's a search engine on steroids. You can find any object in your store based on metadata, date, time, etc. It can extend beyond your own physical hardware across multiple objects stores. The search will work on anything. It is also 100 percent compatible with AWS S3.

For SLED customers, there's an opportunity with Hitachi's partner Flexential to provide Hitachi Content Platform as a service. If a city government, for example, does not want to apply their own object store, they can be in a multi-tenant environment through this partnership.

Finally, Hitachi System Security can help you if you get attacked with ransomware. They can provide analysis on the impact and negotiate with the ransomware attackers. They can start building defensive postures around your organization. The attackers are not solo players, but criminal organizations with developers and management, so it requires a professional response. Hitachi System Security can take an organization from start to finish.