# Case Study

Public Sector
Embracing Digital Transformation

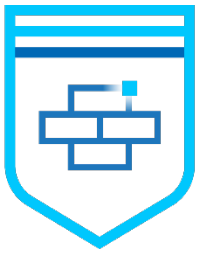
# Securing the Data Center From the Edge

Darren W Pulsipher, Tom Grarrison & Camelli Morhardt – Nov 9, 2021

## Ignoring security at the edge and in client computing is like putting the key in the lock and advertising to the world that you have valuables in your safe.

Sidebar header

In this episode, Darren discusses securing the data center through the edge with fellow Intel executives and podcast hosts Tom Garrison, VP of Client Security, and Camille Morhardt, Director of Security Innovation and Communication.



**Video**: Youtube Channel

**Podcast**: SoundCloud

**Keywords:** IoT, Client Computing, Cyber Security, Cloud, Edge

A holistic look at security includes the whole infrastructure, from within the cloud environment all the way out to the edge. If you can't secure the client, you can't secure the enterprise, so it's essential to have honest conversations in an approachable way, without the jargon, about security.

Gone are the days when an employee would get a laptop shipped to an IT cage, then configured and delivered by IT. Sometimes employees never even come to the worksite, so devices need to show up at someone's doorstep. They must be provisioned to make sure they are safe and haven't been tampered with. From a security standpoint, this is a challenging problem. The supply chain is problematic. There's less control over the devices and how they get deployed.

The sudden switch to working from home because of the COVID pandemic required an unprecedented rapid response to this problem. It may have taken years if it had been a natural progression, but the situation didn't allow an alternative; IT had to rise to the occasion.

When Camille worked in the IoT group, they tried to solve the connectivity and manageability between devices. Complex ecosystems like wind farms, underground mines, implanted medical devices are hard to update when connectivity is sporadic. They were trying to solve these connectivity issues on the edge, and when COVID hit, the intersection between OT and IT suddenly became the center of all enterprise IT departments.

As some of Darren's customers were battling with how best to bridge OT and IT, COVID hit, and some of it collapsed, resulting in security breaches.

Many people quickly rolled out a work-from-home system and dealt with security later, depending on the organization's maturity level. There was also a massive shift to the cloud. Currently, there is a bit of a pendulum swing back because of breaches such as ransomware attacks. Those breaches happened in the cloud, primarily because people did not understand the shared security responsibility. Now, some organizations are thinking twice about moving their critical data into the cloud. They may move workloads there but are keeping the golden data at home.

Another recent shift is the importance of client perception. You may be asking the right hardware questions and software layers of protection questions, but you also have to consider your client's perception about where you are keeping the data and why, who is protecting it, and how they are protecting it.

A bigger problem is organizations that cannot answer any of those questions. Sometimes they don't even know where their data is. These organizations should see this as a starting point for what work still needs to be accomplished.

Some new issues exacerbate this problem that the industry has not addressed yet, such as video conferencing. The meeting recording is saved on a laptop, but it's also in the cloud somewhere. Who has access to it? What are the protections? How long will it be there?

One principle of security is knowledge of whether your device is safe. One of the challenges uncovered with the COVID situation is that many IT shops are hesitant to update systems. They do not want to take a system down, whether it is a server or a client. Not updating for security patches is a mistake.

Intel's job is to work with partners and fellow travelers to make those update a more straightforward, higher trust activity where people will have confidence that it works and something won't go wrong in the process. The industry has made considerable strides in making the update process more systematic and predictable in the last few years.

Another part of the job is training people to understand that security doesn't stop when a device is shipped from the manufacturer to a customer. Security continues over the life of a device. What was world-class security at the time of shipping is not world-class security months or years later. Companies should update their machines twice a year to keep them safe.

People get nervous about doing updates because unexpected things might happen. Intel validates at scale to prevent issues, whether with thousands of machines in their labs or with OEM partners in labs scattered all over the world. The complete validation makes sure the mitigations work to protect against the vulnerabilities and do no harm to the system. Intel has made a significant investment in partnering and collaborating with its ecosystem partners and driving standards across the industry, and looking to improve the user experience in the future by developing the ability to do the updates without a reboot.

Educating customers about why you are asking them to do an update can go a long way, too. If they understand you have found a vulnerability and may be open to a potential attack, they will likely want to do it.

In general, people seem to be willing to update their cell phones because they aren't as worried that something won't work afterward, but it's still a challenge on the PC and server sides. Some of that has to do with usage models. Although it's rare for data only exist on a laptop, that mentality is prevalent. When the data exists in the cloud on a cell phone, the perception is it's always going to be there. In addition, people tend to do more immersive, engaging work on laptops than on phones, so they are more sensitive to it. Once the perception shifts and people realize the data on their laptop also exists in the cloud, the updates are more widely accepted. So, in reality, the industry needs to do a combination of technical solutions and mindset changes when it comes to security.

The way things are evolving is a bit of a hybrid. New learning models like federated learning are rushing in to help address issues like privacy concerns. Models are being pushed to the edge instead of the data moving to the data center. For example, a medical imaging system in a hospital where the data stays put and the model is coming in to look at it. We are starting to see this in industrial applications, where machines are at the edge and become the server. They'll keep data local and do training and updates there. So there will be intelligent devices on the edge, doing things with the raw data, and the question is, how do you secure that?

Another trend in security, one that didn't start with the COVID pandemic but was undoubtedly accelerated by it, is protecting against physical attack. Historically, security has been focused on something that could happen over the wire such as a network attack or a malicious application. With IoT devices out there with no human attached or watching, we have to protect the data and the devices from being tampered with. That's a difficult challenge.

Nowadays, you can't think holistically about security unless you're also addressing privacy. One complication is that privacy can sometimes be in direct conflict with security. There are no agreed-upon regulations or standards worldwide, so organizations have to figure out how to operate: Hit the highest common denominator, or address every geopolitical requirement? To complicate it further, laws and regulations are constantly changing.