Connected™
OFFICIAL TECHNOLOGY BLOG OF CONNECTION

**Creating a more Secure Remote Workspace with Intel (**Creating a more Secure Remote Workspace with Intel – Connected IT Blog (connection.com)**)**

**Shannon Barnes** December 30, 2020


More people are working remotely than ever before, which leads to increased demands on IT and end users alike. And while employees are working machines harder, companies are pushing PC refreshes further out. Simply stated, IT is being asked to do more with less.

Hear from Yasser Rasheed, the global director of Enterprise Endpoint and Security Products from Intel, and Stephen Nardone, Connection's director of Cyber Security Solutions Practice, on the state of security in the workplace and the vulnerabilities that should be addressed—and avoided—in today's environment.

Learn why software security might not be enough to protect company assets and information and how end users can open up vulnerabilities. Discover how IT's role of managing so many endpoints presents the challenge to maintaining a secure network and how IT should plan for the future when it comes to investing in technology that takes an active role in security.

***What should IT directors consider when contemplating software security vs. hardware security for their devices? What's the case for both?***

**Stephen:**
You can't start this conversation without just a brief visit through history. When software firewalls first came out, it was pretty much concluded that they were a big mistake, right? So, the key consideration here is of all this software. Coding

techniques have evolved. Things have gotten better in the software world in general. Strength of mechanism—what we like to talk about in the cybersecurity world—has been built in.

The key thing is that we're using the devices. And the other thing is testing, to make sure that there are no software flaws. So maybe do secure code reviews on devices that you're more concerned about—certainly do some level of security testing—to ensure there aren't weaknesses in the interfaces. But other than that, hardware security gives you a lot of flexibility and scalability. It also gives you some of the autonomous capabilities that we're starting to see in networking. It certainly is the direction the industry is going.

**Yasser:**
I totally agree. We know that—for the last decade or so—many companies have been spending more and more on software security. Yet the problem is getting bigger and bigger. The last data point I heard was that 75 percent of companies attacked by ransomware were running up-to-date software security. Software alone is not sufficient anymore. I think everybody realizes that. We now need to look at how to get hardware to supplement and support software in the right way. But hardware will not replace software. However, it will augment, support, and strengthen software security. Ideally the transition is to do both together rather than have hardware-based security replace software.

***How does end user indifference to or naivety about malware impact IT's ability to maintain a secure infrastructure, and what are you seeing in your respective roles?***

**Yasser:**
The end user is the weakest link in security management. People don't want to think about security and safety in general—they prefer to believe that everything is going to be well. And the attacker just needs to see a point of weakness somewhere—a 1 percent crack in the dam. That's what they are going after. The defender needs to protect against everything 100 percent. And that's a much harder task to do. But it starts with education and awareness at the end user level. Whether it's the typical case of opening up an email or clicking on a bad link; the rest is history. It could also be someone who writes down their password—say consisting of their dog's name and a couple of digits—on a piece of paper and making it easy for an attacker. A line of defense is critical.

**Stephen:**
As Yasser indicated, security users are the weakest link in the security chain. There is a huge problem that exists when trying to educate users on making good decisions. We now refer to users as human firewalls, which really covers the expectation. There are policies and controls that a firewall has to be able to enforce. Users need to understand that their capability to do the same thing is critically important. But what we've seen with the vastly increased remote workforce is a 600 percent-plus increase in phishing attacks—specifically targeting users with false COVID-19 information. They are trying to coerce users into clicking on links or open objects that are malicious.

Constant vigilance is what's really required to help users understand what they need to be doing. There will be some level of consistent training to make sure they're aware of what's going on. We must make them aware of the latest attacks out there and what they might need to do to protect against them. You also need to run consistent phishing, envisioning, and testing in the environment to see if you have weaknesses in your employee base. It is critical to do all of that.

***Are you finding that guidance is being impacted because a remote workforce is not as tangible as it is in the office, making them a little more relaxed? If so, how do you change that?***

**Yasser:**
They may be more relaxed because they are working outside of the physical confines of the enterprise. The IT administration or the information security teams now have to defend and protect the users and their devices in an environment that is not controlled anymore. This is critical. In every household, there are other people who may be trying to access other websites or bringing in different entry points, if you will, into an environment, which operates as a work environment. Whether it's a teenager playing games, or someone else trying to access Wi-Fi in the same house, they need to now consider this as part of the perimeter.

***With those complexities in mind, whether it's a home office, on-site, or hotels/airports/restaurants, what security struggles are you seeing that are here today or could come tomorrow?***

**Yasser:**
One, of course, is how are users connecting to the corporate environment? In reality, everybody's really good at doing that. We're using VPNs—encrypted, secure tunneling. Some are doing network access control to validate user access. That has been in the industry for quite a while. The remote worker adds another interesting twist on that since the network is now the home network that they're on.

We just recently did a red team/blue team exercise to put a video together. One of the issues we addressed was the impact of the user being breached on the home network. That's something that's feasible, as the malicious actors out there are 10 steps ahead. Now that corporate asset is also compromised, and it's connecting securely to the corporate network. But is the malware on that system capable of compromising the network? Once it's securely connected, can it escalate privilege based upon what the user's privileges are? What can it do to wreak havoc in the network and so on? That's really the huge, fundamental issue.

Security, in terms of that component, is not something that we typically think about. That's what the workforce introduced. It's really important. The concept of zero-trust networking is huge.

**Stephen:**
Zero trust was a concept but is now a necessity for every organization. They can no longer depend on a perimeter that is within the physical confines of the work environment. Now that the perimeter has eroded, businesses need to defend at the device level. And they need to divide to defend the human level as well. Organizations really need to educate everyone on how to do the right level of protection in the right way, every time, every minute. COVID accelerated that, but COVID did not really introduce the challenge. It's just an acceleration. Frankly, even after COVID is behind us, we won't go back to where we were. Security standards are going to new places. And that new norm is in the making today.

***Here's a question for our Intel expert. Yasser, regarding hardware-level security, what impact do Intel vPro® and Intel® Hardware Shield have?***

**Yasser:**
The Intel vProplatform is designed to offer the best security for business environments. Intel vPro includes built-in security capabilities—such as Intel Hardware Shield—as well as remote management support through **Intel® Active Management Technology** (**Intel® AMT**). This gives organizations the ability to detect threats and react to them.

As you know, that can be a key component of a business continuity plan as well. There are technologies built into the Intel vProplatform that can be leveraged to provide remote administration and remote support as well as more security on those devices. That's something to take into consideration.

***In closing, when it comes to cybersecurity, what best practices have been identified in 2020? What should leadership consider when strategizing their future IT investments?***

**Yasser:**
To summarize in three steps, I would look at the process in the following way: First, modernize the infrastructure. Get the right devices in place and the right infrastructure on the networking side. Otherwise, you're dealing with old technology, which is a lot easier for the attackers to break.

Second, keep it current and manage that infrastructure with the right updates and patches and the right hygiene in place to have the right infrastructure in place.

Third, layer in the right level of security with zero-trust techniques—and be sure to educate your users on how to deal with keys, what to encrypt, and what to protect.

**Steve:**
Those are all really great points. The biggest issue—and what businesses have learned in 2020—is the concept of

business continuity. That's been the biggest flaw that we've seen, in general, especially in the small- and midmarket space. Companies did not have any type of a business continuity plan. When they were forced to move workers out of the corporate environment, they essentially didn't know how to do that well. That was the case for system performance, operational performance, and security.

One of the beauties of the continuation of the remote work or strategy is that companies that weren't doing that are sort of continuously operating in business continuity mode anyway. They now have the tools, the techniques, and the strategy to be able to do that. It's a huge focus, and it's certainly something that every company needs to be evaluating right now.

**What's next?**

Employee diligence in helping prevent malicious access is the first line of defense—but not the only line of defense. As we look to business continuity, users working in an environment not controlled by corporate IT needs to be considered. Invest in the right technology—both hardware and software—to provide barriers against malicious access. For more information on how Intel® technology can take an active role in security for your organization, go to connection.com/brand/intel.

**Notices & Disclaimers**

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.