Trusted Computing. Trustworthy Computing. Zero-Trust Computing.

What's This All About?

It's a given that all enterprises need computing technology to function. And if everyone needs computing technology to keep the doors open, shouldn't it be a requirement that we can trust that technology? Seems obvious enough, but different interest groups often use different words to talk about trust, which tends to muddy the waters.

Let's start at the beginning with some definitions.

> Trust: assured reliance on the character, ability, strength, or truth of someone or something. The definition of "assured" is "characterized by certainty or security."
>
> Trustworthy: worthy of confidence: dependable. The definition for "dependable," is "capable of being trusted or depended on: reliable."

So we're talking about computing technology we can rely on—a reliance that is based on "certainty." Certainty means "the quality or state of being certain, especially on the basis of evidence." You could say that we should base our trust in computing technology on evidence that the technology is genuine, not counterfeit, and that it does only what the vendor says it does. That is, it has not been modified by any unauthorized agent to perform any other actions. In other words, we bought something that is what the vendor says it is and it does what the vendor says it does, and that is all.

Consider the computer you're using now to read this information. Do you have evidence it is not a counterfeit? That it has not been modified? At this point, if you're telling yourself "there are security packages installed, so of course I can trust it," what evidence do you have that the security is working? If you have no proof that the system is clean, then you merely have implicit trust that everything is fine.

Trusting something ***implicitly*** means to trust it without reservation or questioning.

Now imagine you're walking along a city street. You encounter a vendor offering brand name accessories for a fraction of the manufacturer's suggested retail price. Do you buy something? Do you trust the quality of the products they're selling? Why not? The vendor seems nice.

So why does nearly every business on earth implicitly trust their computing technology? Consider that the crimeware industry is worth trillions of dollars a year—6 trillion if Gartner is right. That's a lot of economic activity that depends on the rest of us continuing to implicitly trust our computing technology.

What's the solution to this problem? Installing security technology helps, but security technology is generally not very good at providing evidence that it has not failed. It's usually very good at providing evidence of all the bad stuff it has blocked or caught. But what evidence do you have that your security tools caught everything?

Isn't this like proving a negative? If you aren't dead, then you must be alive? Ever heard the phrase "dead man walking?" Is that your computing infrastructure right now? How do you know?

That is what all the talk about trust is about – tools and processes that the enterprise uses to gather evidence about the trustworthiness of its computing infrastructure. And it isn't good enough to check trustworthiness once in a while. Evidence that you were trustworthy last week does not prove you are trustworthy right now.

At the moment, there are three main camps talking about trust in computing technology. The oldest is an open standards group called the Trusted Computing Group. They've been around for over 20 years. They write specifications for hardware, software and protocols that can be used to gather evidence on whether computing technology can be trusted (not counterfeit and not modified by an outside actor). Their specifications have been implemented in hundreds of millions of devices.

Then there is a long list of companies that use the word "trustworthy" somewhere in their collateral. There are some pretty big names doing that – Microsoft made a significant commitment to trustworthy computing over a ten-year span. They still build trust into their products. AMD, Dell, HP, Intel, and Lenovo are all examples of hardware companies that build trust technologies into their products. So does Cisco. There are others as well.

The new kid on the block is Zero Trust. Wait a minute, aren't we talking about how to trust our computing tech? Zero Trust sounds like we shouldn't trust any of it. Not so. "Zero trust" simply means we should have no implicit trust in any computing device. Trust in computing technology must be based on a continuous ability to generate evidence that the device is still trustworthy. That means that Zero Trust is no different in its goals than the Trusted Computing Group and all the companies talking about the trustworthiness of their products. As CSO Online says:

> Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

Sounds like a good sound byte to end with, don't you think?