PAT GELSINGER
CHIEF EXECUTIVE OFFICER
VMWARE

WHY TECH HAS FAILED ON CYBERSECURITY

It's time to acknowledge that the tech industry has failed our customers when it comes to cybersecurity and data protection.

Our industry is built on trust. Trust that our software and hardware products work. Trust in the confidentiality of customer data, and trust in our ability to safeguard the integrity and availability of mission-critical systems. We earn that trust every day, by protecting our customers' critical applications and sensitive data in an increasingly mobile and cloud world. The challenge is only intensifying, as application architectures evolve rapidly and as the apps themselves become a primary target for cyber criminals.

Albert Einstein said, "The definition of insanity is doing the same thing over and over again, but expecting different results." Unfortunately, that's a good summary of our current approach to cybersecurity. Until we re-engineer our fundamental security model, we will be unable to dig ourselves out of this hole.

Transforming Cybersecurity: From Chasing Bad to Ensuring Good

The problem is not a lack of innovative products. In fact, there's tremendous innovation happening in cybersecurity today. The problem lies in our foundational approach, which is rooted in "chasing bad." It's a never-ending arms race, and we always seem to be rushing to catch up. When you're chasing bad, you're constantly looking for the proverbial needle in a haystack, across a very large attack surface.

But what if we took the opposite approach? What if, instead of chasing bad, we flipped the entire model on its head and focused our efforts on "ensuring good"? When you focus on ensuring good, in effect you remove all the unnecessary hay, because you narrow down the exploitable attack surface exponentially. How?

At the heart of ensuring good is a revival of the age-old cybersecurity concept of "least-privilege," where users and system components are given the absolute minimum level of access, function, and interaction required. In other words, unless you explicitly have access, you don't. The big difference today—and the big breakthrough—is that we now have the ability to enforce least-privilege at scale, without slowing down the pace of innovation or the businesses we serve.

Ensuring good goes far beyond the rigid "lockdown" methodology of deny-by-default. We're talking about an approach that's far more nuanced and sophisticated. When we harness least-privilege to ensure good, it's about striking the right balance between security and the need for fast, flexible service delivery. In other words, we're making security empowering rather than confining. Just like brakes on a car: the purpose is not to slow you down, it's to allow you to go fast.

Three Core Tenets of Ensuring Good

There are three core tenets behind ensuring good. First, leverage a secure infrastructure to build least-privilege environments around applications. Second, empower the ecosystem by exposing the boundaries and context of those environments and enabling the ecosystem to align to those boundaries. And third, make it simple and easy to practice good cyber hygiene.

vmware®

Secure Infrastructure

A secure infrastructure changes the rules of the game by enabling you to quickly lock down critical applications and data, architect-in security controls, and facilitate a repeatable and focused cyber hygiene process. This is not simply an infrastructure that is built securely, but rather one that enables you to understand the relationship between applications and infrastructure and create least-privilege environments around them.

Infrastructure centered on ensuring good needs to have native, built-in capabilities that are architected-in from the ground up, with tight alignment to what we care about most: applications and data. Today, too many cybersecurity controls are aligned to pieces of hardware buried deep down in the infrastructure—a router, switch, or server for example. Why? Because in a hardware-driven world, that's the only place we can hang them. In a software-driven world, we have a rich and fluid canvas to work on rather than a rigid set of hardware and edge-based solutions.

Empower the Ecosystem

The ecosystem of security controls needs a privileged position in the environment in order to effectively focus on ensuring good. Those controls must have access to rich context about the applications and data they are trying to protect, and ubiquitous coverage for visibility and control.

Much of the ecosystem is already expressing enthusiasm about the game-changing notion of ensuring good, as it begins looking for bridging methods to sort through an otherwise untenable stack of hay in search of that elusive problem needle.

Cyber Hygiene

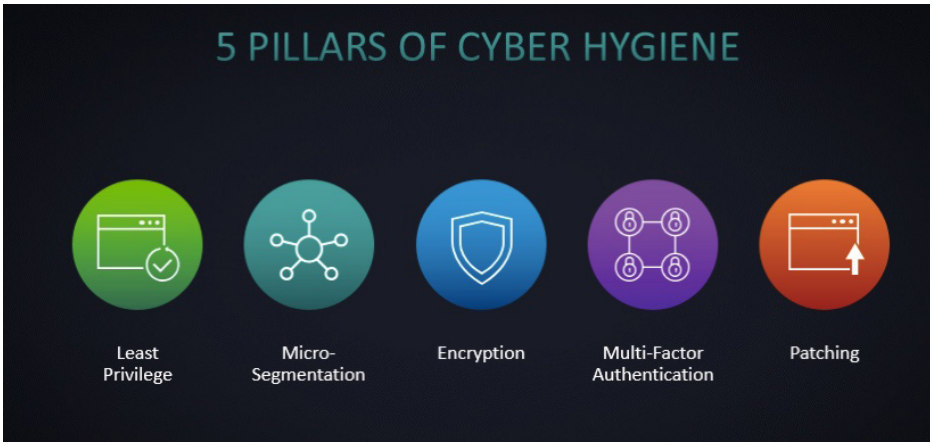
Consistently executed basic cyber hygiene is the single most effective step we can take against breaches and a core tenet of ensuring good.

And yet the only consistency in cyber hygiene is how inconsistent we are; we continue to fail in this space. Not because security teams don't understand what is needed, but because cyber hygiene has become too difficult in a world of constant change. Clearly, we need to make it dramatically simpler and easier to practice the five key pillars of good cyber hygiene, as presented below.

When you examine the major security breaches that made headlines over the past few years, every one of them could have been avoided completely, or greatly reduced in impact if the targeted business had followed these basic principles.

When it comes to security, the question we typically ask is, "How do we secure it?" What we should be asking is, "How can we leverage our IT infrastructure in new ways to transform security?"

In an era when the tech industry has failed on cybersecurity, the time has come to flip the security model on its head.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com