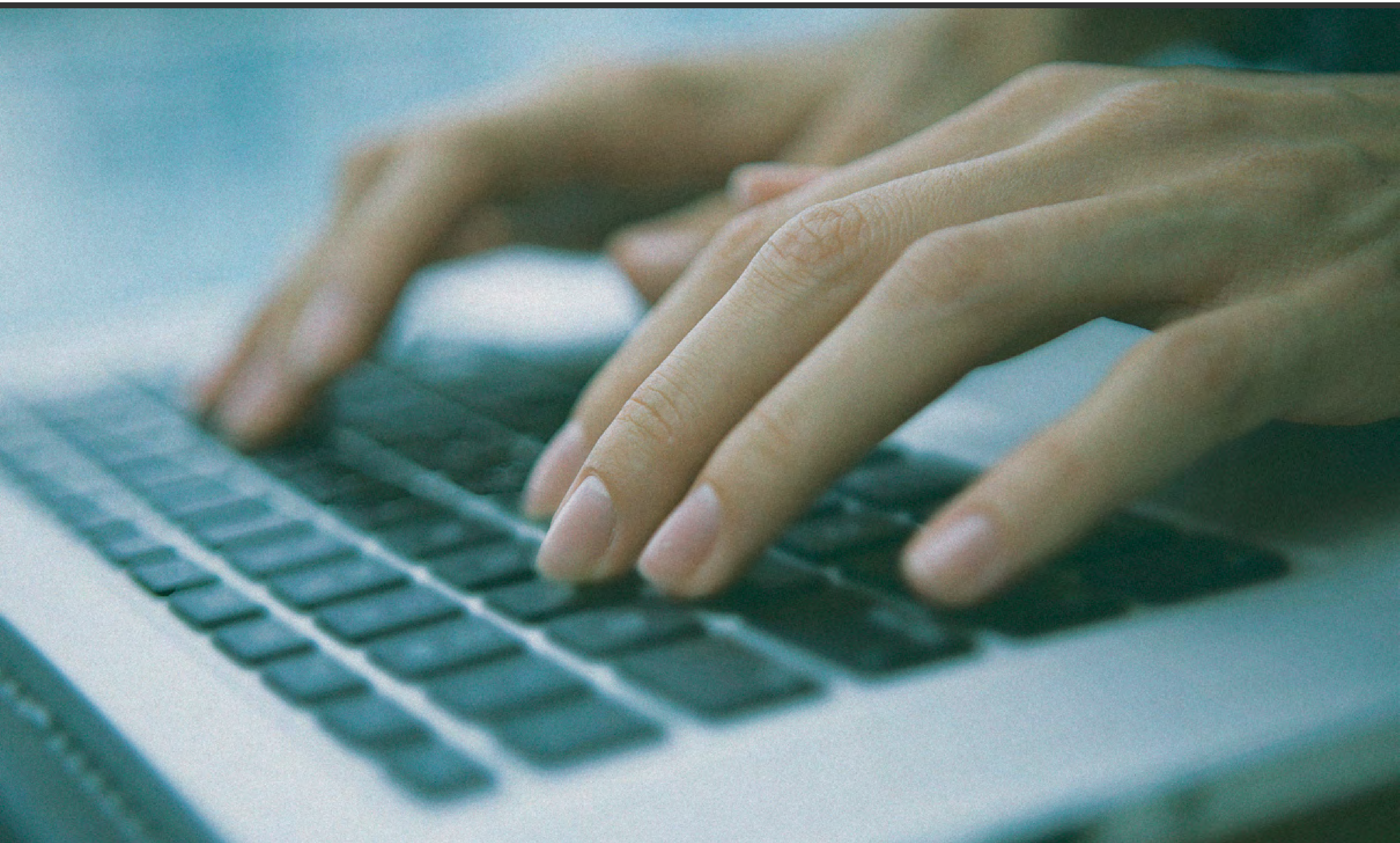
ARMOR™

BETWEEN YOU AND THE THREAT

Is the cloud secure? That's the wrong question.

CSO VANTAGE POINT

JEFF SCHILLING | **CHIEF SECURITY OFFICER | ARMOR**



Sony Pictures. Chick-fil-A. Xbox Live & PSN.

Even in the final hours of the year, data breaches and cloud security remained the hot topics of conversation. As a result of this trend, during interviews and radio segments I'm asked the same question over and over: "Is the cloud secure?"

Unfortunately, I normally only get a five- to 10-minute segment on each show, so my answer is invariably, "It depends." So, let's unpack the specifics of that very general answer.

First, let me point out that the question, itself, is wrong. What everyone should be asking is, "Is my cloud secure?" Because, yes, the cloud can be secure.

Armor knows this — and you know this if you're our customer — because our infrastructure is designed, from the ground up, to be secure.

To achieve this, we integrated industry expertise, best practices and technology into a hosting environment with advanced protection. It's a feat that has yet to be duplicated in the industry.

"What everyone should be asking is, 'Is my cloud secure?' Because, yes, the cloud can be secure."

The 3 major cloud components

Not all clouds are created equally. This is a critical understanding. They're only as strong as the skill, training, management and effort put into them.

Instead of blaming the cloud for breaches, it's far more useful to look at the providers involved and the bolted-on infrastructures they created.

There's just no excuse for vendors and providers who say that they're trying to become more secure. Either they invest in the right staff and the right tools or they don't.

When these components are connected — allowing a user to receive, input or change data — that is the definition of the cloud. The original purpose of cloud topology was to replace the network-centric model of data exchange with a more efficient data-centric model.

Essentially, this means data is stored in one or more central locations, providing ubiquitous access to it from anywhere from any end-user device.

A good cloud security team will apply controls at each connection point, bet"ween the three major components, to establish a hardened end-to-end" infrastructure that's tough to breach.

Cloud ecosystems include three major components:

The servers inside a perimeter that store and manipulate data.

The path established between the user and the applications, as well as data stored inside the perimeter.

The end-user device.

Telling questions to ask your cloud provider

How do you know which approach your cloud provider takes? Ask them. To find out if your hosting provider is secure, pose these questions:

Q Does the architecture allow for a firewalled segmentation between the Web server (which interacts with the user), the application server (where the software that interacts with the data is hosted) and the database server (where the data is stored)?

Q Is there a defense-in-depth approach? This includes hardened operating systems, Host-level defense (e.g., AV, HIDS and FIM) and perimeter inspection (e.g., NIDS/NIPS, Web application firewall, IP reputation management or blackholing).

Q Is the data encrypted at rest so even if a threat actor is able to gain access to the server, they won't have access to the real data?

Q Is the connection between the data and end-user encrypted?

Q Is user authentication rigorous and difficult to breach? This includes strong two-factor authentication, user login anomaly detection and a hardened password-reset process.

Q Most importantly, is there a security team proactively monitoring and patching these systems to ensure they are protected from known threats? Are they ready to detect and respond quickly to new or unknown threats?

If your hosting provider can answer "yes" to these questions, congratulations. You have a secure partner who is above the commodity-hosting level. You're also well on the road to being HIPAA- or PCI-compliant, which is no small feat.

Unfortunately, most hosting providers' responses will be quite telling: No. Most simply don't prioritize delivering end-to-end security.

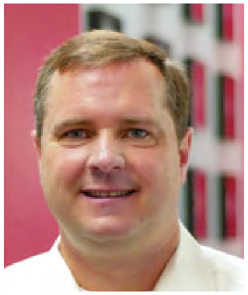
'Does my business need a secure cloud?'

This is the other question. It's time that organizations are proactive, smart and stop storing regulated data and applications with nonsecure providers who can't protect them.

A competent and reliable cloud provider will build security into their infrastructure from the ground up. But that's just the first step. It's critical this is balanced with properly educating their customers on safety in the cloud.

These are perilous times we're living in. Enough is enough: it's time for the industry to make security a priority.
Not an after-thought.

> "A competent and reliable cloud provider will build security into their infrastructure from the ground up. But that's just the first step. It's critical this is balanced with properly educating their customers on safety in the cloud."

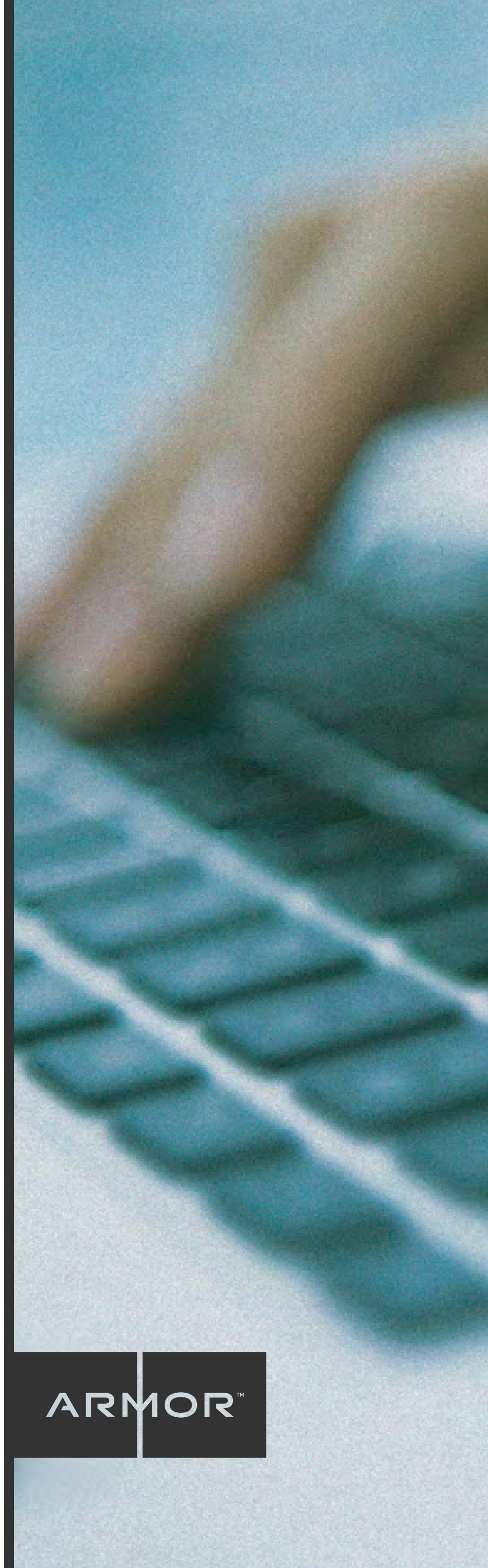


About Jeff Schilling

Jeff Schilling (Ret. Col., U.S. Army) is Armor's chief security officer and is responsible for the cyber and physical security programs for the corporate environment and customer-hosted capabilities.

Schilling retired from the U.S. Army after 24 years of service in July 2012. In his last assignment, Schilling was the Director of the U.S. Army's global Security Operations Center under U.S. Army Cyber Command. In this position, he was responsible for synchronizing the global security operations/monitoring and incident response for over 1 million computer systems, on 350 wide-area networks, supporting all U.S. Army organizations in more than 2,500 locations.

Previous to this position, Schilling was the Director of the Department of Defense's (DOD) global Security Operations Center with Joint Task Force Global Network Operations, where he managed security operations and global incident management for over 4 million globally connected computer systems.



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™

BETWEEN YOU AND THE THREAT