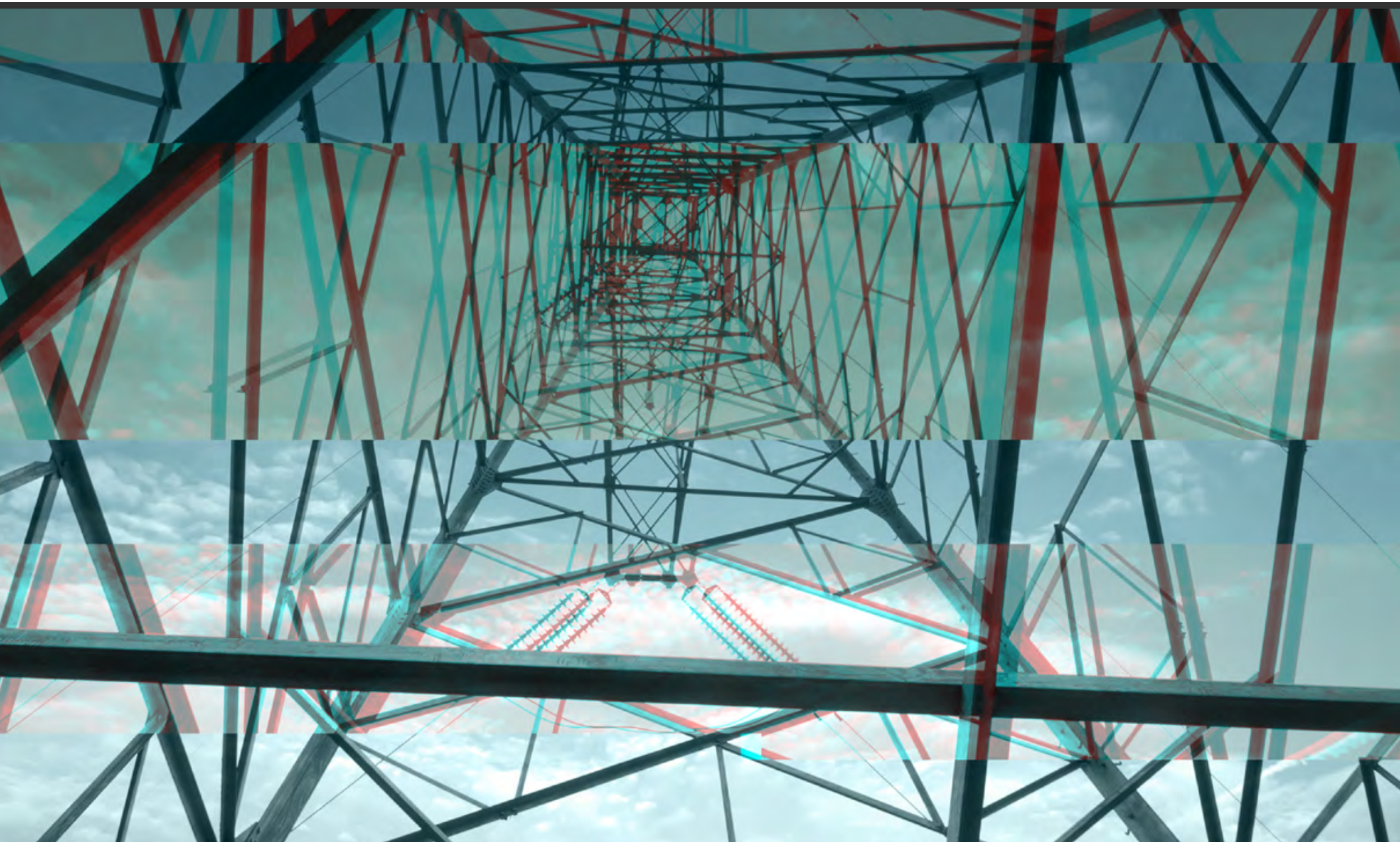
ARMOR™

BETWEEN YOU AND THE THREAT

# Securing from the inside out

## UNDERSTANDING BIG DATA, CONTESTED SPACE & PROTECTING WHAT MATTERS | CSO VANTAGE POINT

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



The cybersecurity industry is often tight-knit. I collaborate with many CSOs and CISOs of major corporations. In a majority of these conversations, I hear the same analogy: "My network is like a chocolate M&M. It is has a hard outer shell, but is soft on the inside."

What do they mean? Simply, they are reiterating that, to date, their specific corporation has focused solely on securing from the outside in to "stop the bleeding." Most security strategies attempt to detect and stop threat actors at the edge and provide limited security between VLANs and limited hardening and detection capabilities on the host itself, which is what the threats are targeting.

This is the exact wrong approach. And many of these smart, educated C-level executives understand the problem. But the security industry hasn't aligned in a way to make it easier for them to defend from the inside out.

Many battlefield examples helped me reach this conclusion. As we reached new understandings of our battlefield and areas of operation (specifically during operations Enduring Freedom and Iraqi Freedom), we strategically made dramatic improvements on the survival of the soldiers. And it happened in layers, from the inside out.

We began by protecting soldiers with personal body armor that could safeguard them from a direct hit from small arms. When you encapsulate that same armor-protected soldier in an armored vehicle, and then provide air cover to eliminate over-the-horizon threats, you have a well-protected soldier.

Should we apply this inside-out strategy to cybersecurity? My opinion: absolutely.

"Should we apply this inside-out strategy to cybersecurity? My opinion: absolutely."



## Big data, bigger vulnerabilities

The major trends in security technology lean heavily on big-data analytics. Most of our boundary network security tools — where we create the big-data problem — look for the proverbial needle in a haystack flowing through the network stream.

From this, we attempt to correlate the data (many times unsuccessfully) with host-level events to build a forensic story of what is happening. This granular focus causes gaps in our security visibility, which threat actors leverage to infiltrate networks and steal credit card data, ePHI and other sensitive information.

We've created a complex condition. Our security tools identify large amounts of threat activity at the boundary of networks. But without host-level visibility, we lack the ability to add context about the status or success of the attack. In the end, we're looking for so much — with so many point solutions — we fail to actually analyze or comprehend any of it.

> "In the end, we're looking for so much — with so many point solutions — we fail to actually analyze or comprehend any of it."

# 98 versus 2

Successful criminals always have a target. The malicious groups that attack major organizations are trained, well funded and have diligently prepared for a successful data heist.

Capable threat actors are only targeting about 2 percent of the data on a given network — basically, where email servers, customer information, intellectual property and regulated data are stored.

Unfortunately, they are savvy enough to use the other 98 percent of your network (e.g., employee workstations, websites) to gain illegal access to that 2 percent.

This begs the question: "Why don't I start by protecting that 2 percent and make sure any connections coming over from the other 98 percent of my network are authenticated as legitimate traffic?"

By now, you are rolling your eyes and saying, "It's not that easy." Yes, it is. But only if you think about how soldiers are protected from the inside out. Here are four initial steps to re-imagining your security strategy.

## 1 Classify data, then protect

First step: identify that 2 percent. Start with the obvious (e.g., regulated data such as PCI) then progress through a maturity model that identifies which data is most sensitive.

Categorize this data based on risk, sensitivity, compliance requirements, etc. These categories will be unique to your company and its business objectives.

Ensure this 2 percent of data is running on hardened operating systems. And always make this data set the priority for patching, which remains the best method of keeping even the most sophisticated actors off your hosts.

The result of this exercise ideally will be what most security professionals believe to be unachievable: a true data loss protection program.

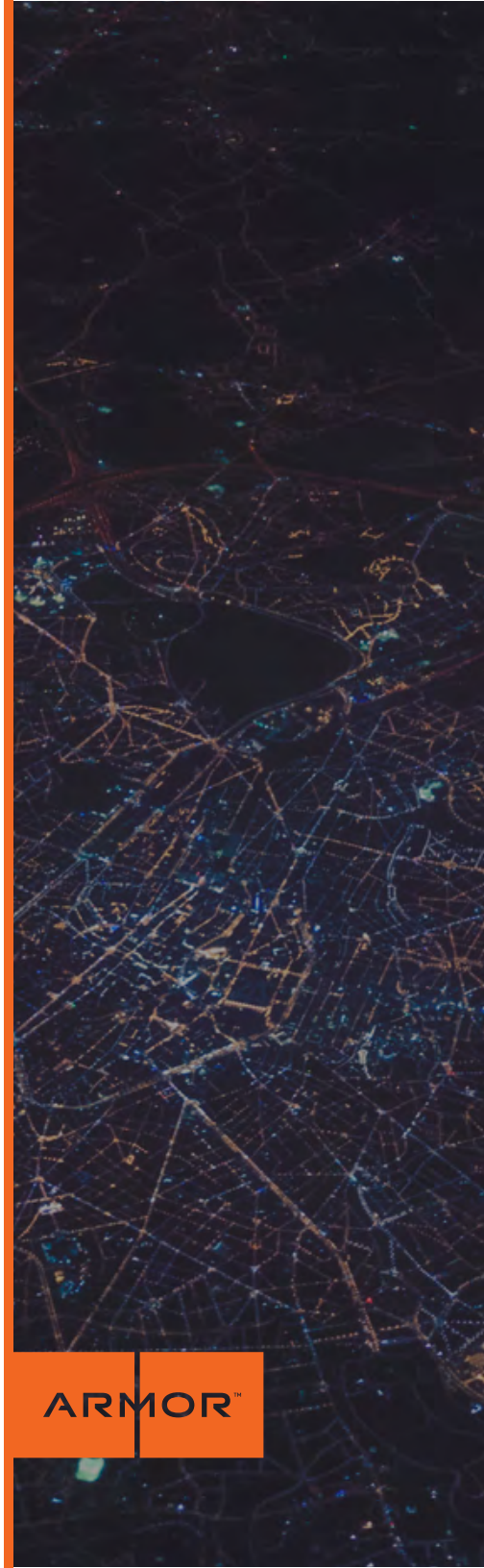
## 2 Build a host-level strategy

Next, select a host-level detection strategy that provides a strong opportunity to catch the threat actor early in the kill chain: at the moment of exploitation.

You'll hear many security professionals scoff at antivirus solutions as old technology and a losing strategy. What they don't realize, however, is that antivirus controls now do much more than just matching bad binaries.

Capable AV technology will provide host-level intrusion prevention systems (IPS), as well as URL- and IP-blacklisting. Many AV products also monitor memory for symptoms of a compromised host. And that's the one place a threat actor has to reveal his/her actions.





### 3 Encrypt data at different levels

Next, be sure you're encrypting data — the right way. Most security professionals think only of disk encryption. This is a sound approach for laptops that could get stolen. But when was the last time a criminal organization broke into a well-guarded co-location facility and ran out with a disk array under their arm? Maybe in the movies, but not in reality.

A different approach must be used for data encryption. Apply file- and application-level encryption with the keys stored in a secure location. When executed correctly, this tactic will stop threat actors from accessing data in a readable format.

Truthfully, I am very surprised at the few options available for strong encryption tools that can protect data at multiple levels.

### 4 Establish a protected enclave

From here, segregate the targeted 2 percent of data from the other 98 percent. This can be achieved via a number of secure architectures such as virtual private clouds or dedicated private clouds. The innovative CIOs and CISOs I engage with treat that 98 percent of data as contested space.

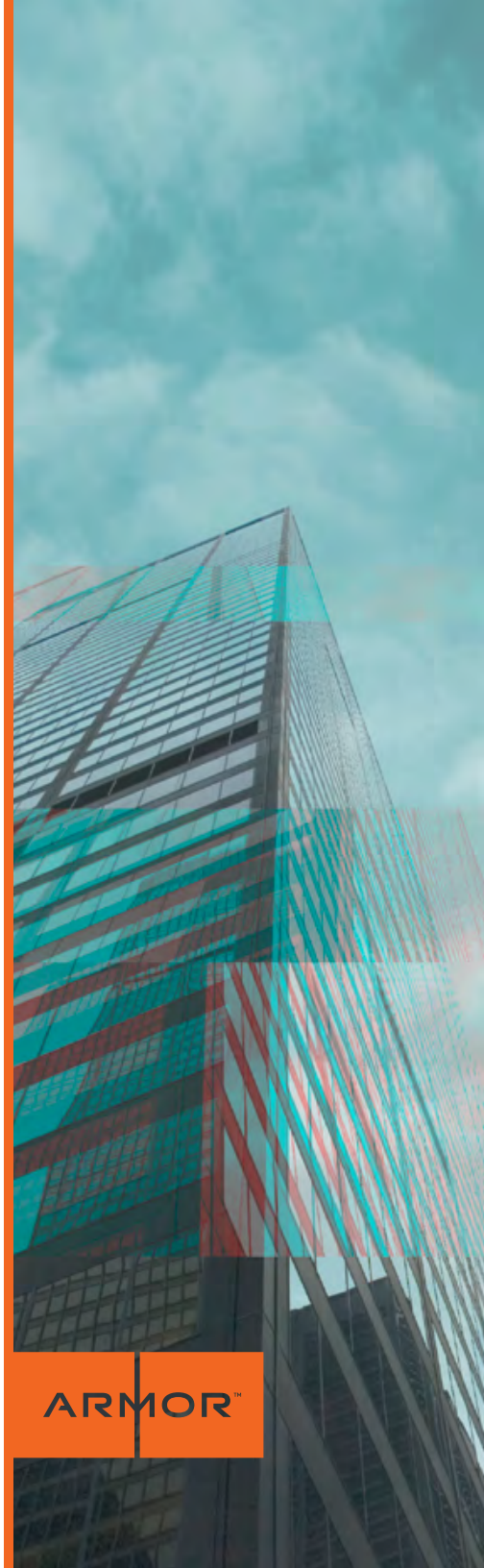
What does this mean? Simply, they don't trust any hosts or systems in that contested space. From there, they require strong authentication (in most case two-factor authentication) for a host in the 98 percent to connect to that critical 2 percent of data.

Smart organizations don't stop there. Data also is forbidden to flow from the 2 percent to the 98 percent. Conversely, the 98 percent is only authorized to view or interact with the other 2 percent. If an unauthorized user attempts to move data against its established path, the connection is dropped and actions halted.

## Defend from all angles

The battlefield lessons that help protect soldiers via multiple layers, from the inside out, may be applied to the digital threat landscape as well. This allows organizations to flip their current model of leveraging big data analytics in the network stream to focus detection efforts at the host level. From there, use the network data to confirm or correlate that a host is compromised.

**It's time we transform big data problems into a small data solution.**



## 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