The Cybersecurity Industry is Broken

How leveraging your IT infrastructure can overcome security's greatest structural challenges

TOM CORN
Senior Vice President, Security Business Unit

An Industry in Need of Transformation

Investments in cyber technology have grown at roughly twice the rate of IT overall, but we still aren't turning the tide against cyberinsurgency.

A recent report issued by the World Economic Forum states that the dark web will become the third-largest economy in the world by 2021.[1] During the first five months of 2020 alone, cyberattacks against the financial sector increased by 238 percent, compounded by a 900% increase in ransomware attacks. Cybercriminals are demonstrating significant ingenuity to counter incident response efforts. Their methods include ransomware campaigns, business email compromise scams, and access mining. Criminals are increasingly sharing resources and information and reinvesting their illicit profits into the development of new, even more destructive capabilities.

Cybersecurity is a premier domain of innovation, but we are reaching a point of diminishing returns. The complexity of cyberdefense outpaces the innovation of the individual controls, and the problem is more fundamental than products. The answer is not some new feature or a different type of analytics. What's needed is structural and architectural change because what's hurting security—more than anything else—is complexity and fragmentation.

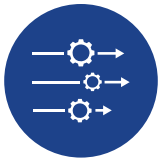
Fragmentation brings a lack of context about the assets and environments we are protecting, while complexity causes too many alerts with decreasing signal-to-noise ratios, and a sweeping misalignment and misconfiguration of controls. That, combined with the seemingly never-ending shortage in talent, is causing a structural issue that cannot be addressed without rethinking how we architect security.

There is hope, some of which comes from the very thing at the root of these challenges: cloud and mobility. What if we can harness cloud's unique properties to improve the way we secure applications and data? That is the promise of intrinsic security.

Recognizing Security's Structural Challenges

As is always the case, the industry's systemic challenges relate to people, process, and technology.

People
Silos between IT and InfoSec are perpetuated by different sources of truth



Process
A narrow focus on the threat and not enough focus on understanding the assets we're protecting

Technology
Dozens of bolted-on security products—each with agents, consoles, policy sets, and workflows

1 People

An InfoSec team cannot secure an organization on its own. Security is a team sport, requiring collaboration with infrastructure teams, network teams, end user services, DevOps teams, and more. IT groups are needed for patching, hardening, and policy changes, and organizations must look for ways to operationalize more and more of security through IT.

This has always proven a challenge. Eighty-three percent of recently surveyed security and IT decision makers report having a negative relationship.[2] Often, organizations chalk this up to different goals, but that's not really the heart of the issue. The reality is that InfoSec teams share many common goals with IT, including protecting the integrity and availability of the systems that process critical data.

The real heart of the matter is that InfoSec and IT speak different languages and operate by different sets of facts. Daniel Patrick Moynihan, the former US Senator and ambassador to the UN, famously said, "Everyone is entitled to their own opinions, but they are not entitled to their own facts." If we are to break down the silos between InfoSec and IT, we must share a common set of facts and semantics.

2 Process

By focusing on threats, InfoSec teams have become far too reactive. It is often said that cyber is an asymmetric battle and that defense is always harder than offense. While that may be true, the one potential home-court advantage we have is an understanding of our own environment—our applications, our data, and how those two elements leverage our infrastructure. This context is central to improving all elements of a security program: hardening, prevention, detection, and response. Ultimately, you cannot secure what you don't understand.

KEY TAKEAWAY

Organizational silos, too much focus on threats, and too many bolted-on security products contribute to the industry's systemic challenges, which affect the integrity and availability of systems that process critical data.

Think of it this way: a burglar knows more ways to break into your house than you can imagine, but you know more about the inside of your house than they do, from the layout to how it's used at different times of day, which floorboards creak, and so on. You can use that knowledge as context to not only shrink the attack surface but also create a disadvantage the moment they're inside. But few of us do.

Nowhere does this hurt us more than with our workloads. Unlike user machines, workloads are single-purpose, part of a distributed system, and admin-controlled. Truly understanding them and the applications they serve can provide tremendous benefit in reducing the attack surface and greatly improving detection and response. But to accomplish this, we need better context about our environment, and we need to focus more on this part of the equation.

3 Technology

We don't lack for products in security. Quite the contrary. We have too many products bolted onto our infrastructure, and the complexity is killing our defense.

We build our infrastructure to accommodate a wide variety of application types. Then we build our applications. Then we tell our security teams to go secure them. It's an impossible position for these teams, and this outdated process shows a lack of understanding about how security works. Furthermore, it has led to dozens of security products in use at every organization. That means dozens of agents and appliances collecting similar data and dozens of consoles with policy sets to reconcile. Each year's RSA conference features hundreds upon hundreds of exhibitors, with solutions designed to solve a specific part of the security problem. I venture to guess there are more than 6,000 of these types of products sold globally.

We must consolidate our security product sets, particularly in products that work in connected-use cases or leverage overlapping data sets. Streamlining the process dramatically reduces complexity and facilitates a process where different parts of a defense-in-depth strategy can reinforce one other. At the end of the day, prevention is there to make up for hardening fails. Detection and response kick in when prevention fails. And we should learn much from detection and response and then leverage those experiences to improve our hardening and prevention. That's much easier to accomplish when they have been designed to do so. Otherwise, we force security teams to become systems integrators.

Security Must Become Intrinsic

The best way to break through these barriers is for security to leverage the digital fabric of your infrastructure—compute, networking, storage, and management—to architect security within. Building security into the infrastructure gets rid of the agents, appliances, and sensors that bog down and disrupt compute capacity, leads to a more efficient way of collecting richer data, and consolidates the controls that really represent interconnected use cases.

Leveraging digital infrastructure is also the key to unlocking greater context: it's through the infrastructure itself where we can best ascertain what a given asset is, does, and serves. Many have tried that before from the security layer by attempting to reverse engineer the context from traffic or other telemetry. But taking data right from the source is both more accurate and far less compute-intensive. Exposing the same context, the same source of truth, to both the security and IT teams is also key to breaking down the siloes between InfoSec and IT and critical to operationalizing more of security through IT. There's still a large and growing cybersecurity talent shortage. We'll never be able to train enough new people to fill that gap in time. Increased automation and operationalization via IT are imperative.

KEY TAKEAWAY

The best way to break through industry barriers is for security to leverage the entire IT infrastructure to architect security within. Doing so unlocks greater visibility, context, and control around the applications and data you're securing.

Leveraging What You Have Today

For IT leaders with virtualized and cloud-ready environments, now is the time to refocus defenses and embrace an approach to security that leverages the infrastructure itself for visibility, context, and control. This approach results in fewer products to manage, less complexity, greater context, and far better collaboration between InfoSec and IT. Cloud can be the root of our solution rather than our problem if we seek ways to leverage its unique properties to secure applications and data. This will be nothing short of a transformation, and we've never needed that more than we do today.

KEY TAKEAWAY

Now is the time to refocus defenses and leverage virtualized and cloud IT infrastructure to build security controls from within and reduce complexity and fragmentation.

TOM CORN
Senior Vice President, Security Business Unit, VMware

Tom Corn leads strategy, product marketing, technical marketing, and the field CTO team for VMware's Security Business unit. Prior to this role, Tom was the SVP/GM of VMware's AppDefense Security Platform. Prior to VMware, Tom was SVP and Chief Strategy Officer of RSA Security, overseeing corporate strategy, M&A, alliances, advanced development, and the CTO Office. He holds a BS in electrical and computer engineering from the University of Waterloo and an MBA from Harvard University.

1 Emilio Granados Franco, "The Global Risks Report 2020," World Economic Forum, January 15, 2020.

2 "Tension Between IT and Security Professionals Reinforcing Silos and Security Strain." Forrester Consulting, 2020.