vmware | intel

CIO Essential Guidance: Intrinsic Security

How a radical shift in thinking can lower your business risk

Table of Contents

Executive Summary

Despite massive spend to protect enterprise digital assets, security breaches are still on the rise. The disconnect between the level of investment and the volume and impact of attacks is largely attributed to outdated approaches that favor perimeter protection and point solutions despite a digital supply chain that is more distributed than ever.

For these reasons and more, enterprises need to start thinking differently about cybersecurity. Security doesn't need new products. It needs a new model. One that applies the principles of **intrinsic security** across the fabric of the organization, from the sales floor to the C-suite, from the infrastructure to the endpoint device. In this Essential Guidance executive brief, learn how intrinsic security differs from traditional security methods, and the steps CIOs need to take to operationalize this model for greater business agility without greater risk.

vmware® | intel®

A New Approach to Cybersecurity

Traditionally, cybersecurity strategies have focused on protecting the perimeter infrastructure and layering in multiple point solutions to identify and block threats. This approach remains essential, but it's not enough. Multiple security point solutions, agents, and management interfaces create opportunities for mistakes and misconfigurations. Also, apps are no longer just in your data center. They're highly distributed across on-premises data centers, public clouds, containers, mobile, and edge environments.

Leading organizations know this—which is why they're shifting from a hyper-focus on threats to a more holistic strategy that doubles down on reducing the attack surface by protecting from the inside out. They are operationalizing the concept of intrinsic security—and experiencing growth in return.

A case in point: According to a 2019 Forbes Insights study, 41 percent of enterprises considered cybersecurity "trailblazers" report annual growth rates exceeding 20 percent, compared with just 4 percent of their lagging counterparts who saw such breakthrough numbers.[1] The report goes on to define the characteristics of a cybersecurity trailblazer, described as a company that devises security strategies with business objectives in mind and views security as having a direct impact on brand reputation, customer experience, growth, and innovation.

CYBERSECURITY TRAILBLAZERS ARE COMPANIES THAT

1. Devise security strategies with business objectives in mind
2. View security as having a direct impact on brand reputation, customer experience, growth, and innovation

1. Forbes Insights. "*Cybersecurity Trailblazers Make Security Intrinsic to their Business.*" Joe McKendrick, 2019.

"Intrinsic security requires a radically different approach, with a much higher degree of automation, to put up security guardrails that protect infrastructure, applications, and users alike."

TOM GILLIS, SENIOR VICE PRESIDENT AND GENERAL MANAGER OF SECURITY, VMWARE

What once was considered a technology problem has become a business *imperative*. Protecting from the inside out means aligning security to your primary assets in addition to your compute, network, storage, endpoints, and end-user devices across a heterogeneous infrastructure. It involves a deep understanding of your applications—topology, processes, acceptable state, who's using them, from what devices, and so on—and their behavior across users, machines, data, and networks interacting in the normal course of business. An intrinsic security strategy also incorporates three distinct characteristics:

- Embedding security controls directly into the infrastructure, networks, and cloud workloads—the places where your applications and data live
- Adding automation to streamline security policies across infrastructure, applications, workloads and users
- Taking advantage of built-in protections via the infrastructure to safeguard your most precious digital assets

TRADITIONAL SECURITY	INTRINSIC SECURITY
Deploy firewalls, web application firewalls (WAFs), intrusion prevention systems (IPSs), security information and event management (SIEM) solutions, and identity and access management (IAM) tools.	Deploy a defense-in-depth strategy that layers security mechanisms everywhere throughout your infrastructure and applications.
Perform penetration tests.	Apply micro-segmentation to on-premises and cloud workloads.
Implement vulnerability management.	Follow Zero Trust principles, and give only "least-privilege" access to users of all kinds.
Practice security incident response.	Reduce your attack surface and proactively remediate with machine learning.
Go with a "protect-and-respond" model.	Partner with risk management and business executives to devise a comprehensive, enterprise-wide security plan.

Table 1. Differences in traditional versus intrinsic security

Gaining Organizational Alignment

Leading-edge organizations know that improving security is not just about technology. It's about culture. Which is why it's so important to gain organizational alignment when building your strategic plan and IT roadmap.

Perhaps your organization's IT and security teams operate separately. This siloed front between the CIO and CISO no longer works. The rising breach numbers attest to that. Regardless of reporting structure, it's critical that the CIO and CISO build a single, integrated roadmap together. This is no easy feat—the CIO is typically focused on making forward-looking technology decisions while the CISO is often dealing with issues related to previous technology investments and processes. Despite this disconnect, having these two positions in lockstep is essential for addressing and mitigating cyber risk. Together, the CIO and CISO can reconcile past investments with future plans and build a roadmap that is directly aligned to securely take the organization from its current state to its future state as envisioned by the CIO.

"With a collaborative model, the security team becomes a 'center of excellence' that acts as a trusted partner, mentor, and guide to all other departments in the organization. The security team knows where the skeletons are buried and is there to smooth things out for everyone else."

MATTHEW TODD, PRINCIPAL CONSULTANT, FULL SCOPE CONSULTING

Security also must become part of your culture, starting with collaboration at the highest levels, and embedded throughout the company—from DevOps, HR and finance to manufacturing and other functions. As you plan for the next 3 to 5 years, make sure your security pros are in on early decisions about architectures and decisions to move to new apps and development tools. While most organizations' security architectures are due for an overhaul, it's also important to operationalize new tools and policies without alienating existing security staff.

Getting your board on board

As important as it is to gain alignment across the C-suite, Office of the CISO, and staff, getting buy-in from the board often requires a different approach.

Oftentimes, gaining budget and setting security strategy follows one of two scenarios:

- Prepare for the worst and invest in point solutions that can insure against particular scenarios.
- Spend roughly the same amount of budget as in previous years, without any hard change to vendors, providers or products.

Either approach yields dozens, if not hundreds, of point security products to manage, and getting them to work together for holistic coverage is a major headache. Plus, cybercriminals are simply moving too fast. Maintaining the status quo doesn't account for evolving attack vectors and methods to get around existing defenses. You're always one step behind.

Instead, CIOs should leverage a *risk model* when negotiating budgets and planning for the next year. This model forces leaders to identify what's really important to the business and where the real risk lies, and it's unquestionably the way organizations should be making decisions about cybersecurity investments. By reframing security in that vernacular, you're more apt to get board and C-suite buy-in to protect the company's most critical assets.

Shifting Your Mindset

The security industry still focuses the majority of its investments and innovation on preventative models as a way of reducing risk. Modernizing your security strategy means adapting to the highly distributed world that apps and data now live in. Your strategy won't be based on a set of products or tactics, but rather an approach that involves a three-point change in execution based on a new mindset: **protecting good versus chasing bad.**

When organizations focus attention on what a workload is supposed to be doing, the lens for seeing malicious activity is much more focused and, as a result, teams can narrow the exploitable attack surface of the workload down to what it's supposed to do—its intended state. Once "known good" or "intended state" is captured, detection and response is faster and simpler. This new approach applied to infrastructure, applications and users lowers enterprise risk.

Here's how each contributes to operationalizing intrinsic security.

Protect infrastructure

Infrastructure is the critical underlying component of everything running today's digital businesses. No infrastructure component should ever be deployed without security in mind.

Modern intrinsic security addresses the network, data center endpoints, and the data itself by shifting focus to securing traffic *inside* the IT environment so that attackers who make
it past perimeter defenses cannot move laterally across the environment. This is achieved by defining security policies at the individual VM or container level of an application and is similar to locking every door to every room inside your house. If burglars manage to pick the front-door lock, they still have to get through other locked doorways—none of which connect to each other—to steal anything of value. Once your network and virtual machines have been micro-segmented, you can assign fine-grained security policies to applications, down to the workload level, to ensure that nothing or no one can enter unless specifically authorized.

Oftentimes, efforts to quickly modernize or innovate deteriorate security operations. Critical to infrastructure security is rigid standardization from an operational perspective. What does this mean? That although security policies may differ depending on varying regulations around the globe, security operations are enforced the same way everywhere. A standardized security footprint also encourages deployment and incident response teams to adhere to governance and policy at a corporate level. If a security alarm goes
off in China at 3 AM, a responder from another geography knows exactly what they are faced with when they enter the environment.

It's also essential to have robust change control around infrastructure, so that you can easily perform traces and incident response, and inject controls as necessary. Rather than having individual silos of operational practices, you have a global model that enforces security policy at the workload level no matter where it lands.

INTRINSIC SECURITY STRATEGIES FOLLOW THREE GUIDELINES

- **Security is aligned to your primary assets**—applications, data and users—and requires deeper visibility into application topology, processes, acceptable state, who's using them, from what devices, and behavior across users, machines, data and networks in the normal course of business.
- **Security is simplified.** Because it's built into the infrastructure, security becomes an intrinsic component of your compute, network, storage, endpoints, and end-user devices. Leveraging the infrastructure means installing and managing fewer point solutions, and a less complex security environment.
- **Security is end to end**. Virtualized infrastructure enables greater visibility across heterogeneous infrastructure while enabling a high degree of automation for security policies and controls.

"Application awareness isn't just port and protocol. It's understanding business processes through and through, including all of the users, machines, data and networks interacting in the normal course of business."

TOM CORN, SENIOR VICE PRESIDENT, SECURITY PRODUCTS, VMWARE

TIPS FOR USER PREPAREDNESS

- Require targeted, short bursts of training for all users in all departments.
- Deliver in-person training including phishing simulations for highest risk groups (professionals in finance and HR, and administrative assistants to executives, for example).
- Closely monitor VIPs and most-targeted employees.
- Install best-of-breed secure email gateways.
- Deploy two- or multi-factor authentication for all users' email accounts and other privileged access accounts.
- Install a "report phishing" button for users in email client.

Protect applications

Shrinking the attack surface includes a full understanding of your applications, your environment, what everything is supposed to be doing, and what everything is doing. It's an effective component of intrinsic security strategy because any deviation from normal or "intended" application behavior indicates a threat.

Application protection also relies on knowing that applications and policies change frequently, and you'll constantly define, deploy, change, and remediate policies based on these dynamics. For example, new cloud-native apps being developed in containers and deployed in multi-cloud environments must begin with a conversation with developers and the infrastructure and security teams. Again, collaboration is key. The infrastructure team informs developers of the protections and controls the application needs, developers build applications with security in mind, and the IT team segments the network to further reduce the attack surface. And since many of these applications are being developed within a continuous integration and continuous deployment DevOps pipeline, it's possible to secure them from the get-go.

Protect users

People are wired to trust. Unfortunately, human nature becomes a problem when it comes to cybersecurity. Most of the major breaches over the past 5 years have been because of people. Employees were the root cause of security breaches in 40 percent of companies, according to *Shred-it's 2018 State of the Industry Report*.[2]

Training, of course, is important. That means frequent, repeated, short bursts of training, not just once-a-year online training that users can click through. Face-to-face—even one-to-one—training is most effective, and should be delivered to the users most likely to be targeted by cybercriminals. This includes the C-suite, HR and finance professionals, and administrative assistants to top executives.

Still, technology should be as "user proof" as possible. Intrinsic security addresses this challenge by operating under the principle of "Zero Trust" when granting users access to systems or data. Zero Trust means setting strict access controls and not trusting anyone—or anything—by default. Even if someone is already inside the network perimeter, he or she does not have access to anything other than what they strictly need to do their job. This is achieved by adhering to the principle of "least privilege," and rigidly restricting access rights for users (and systems and processes) to only those applications and data that are absolutely required to engage in legitimate activities. By exercising Zero Trust and least privilege principles, you greatly reduce the risk that users can cause or contribute to a breach.

2. Stericycle, Inc. "*Shred-it's 2018 State of the Industry Report*." 2018.

Operationalizing Intrinsic Security

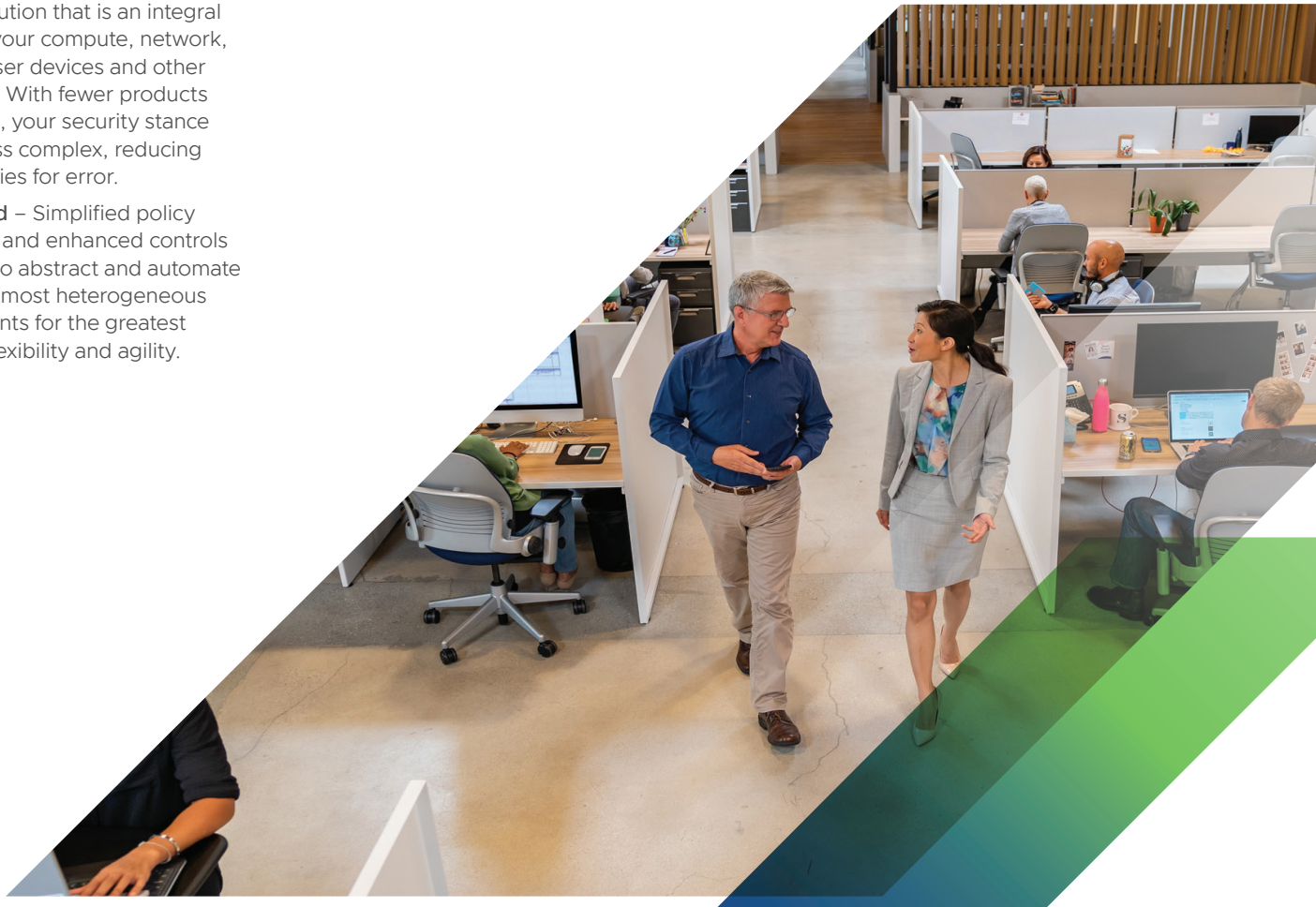
Intrinsic security means embedding security controls directly into application infrastructure, layering protection, visibility and control at points farther past the infiltration point of your perimeter. The layer of software that sits between the heterogenous components in your infrastructure and end-user devices was created specifically to serve your applications and data, which means your existing virtualization infrastructure is the ideal foundation for deploying intrinsic security because it offers built-in visibility and control points for applications from the data center to the cloud to the device.

Leveraging virtualization as the architectural foundation for application security makes security an intrinsic component of the environment, rather than a bolted-on afterthought. Doing so also gives you the advantage of ensuring that security is as agile as the applications and data it protects.

THREE ATTRIBUTES OF INTRINSIC SECURITY

You know you've achieved intrinsic security when you can claim the following:

- **Aligned** – Security is aligned to your primary assets: applications, data and users. You have deep visibility into all of these assets, including who is accessing what, from where. Your policies are simplified and operationalized across your entire infrastructure—including heterogeneous environments encompassing on-premises, public and private clouds, cloud-native applications, mobility and edge.
- **Simplified** – Rather than hundreds of point solutions, you have a holistic solution that is an integral aspect of your compute, network, storage, user devices and other endpoints. With fewer products to manage, your security stance is much less complex, reducing opportunities for error.
- **Automated** – Simplified policy definitions and enhanced controls allow you to abstract and automate across the most heterogeneous environments for the greatest visibility, flexibility and agility.



vmware | intel

VMWARE AND INTEL DELIVER

VMware and Intel provide IT organizations a path to digital transformation, delivering consistent infrastructure and consistent operations across data centers and public clouds to accelerate application speed and agility for business innovation and growth.

Making Security Intrinsic to the Business Wherever the Business Goes

Adopting intrinsic security represents a major shift for CIOs. Yet, it's not the technology as much as your organizational culture that will require the most care and attention. There is a direct correlation between business agility and cybersecurity strategy. Once you've implemented the core principles of intrinsic security—simplifying security models; relying on core infrastructure to extend granular protection to applications, data, and users; and automating security policies and controls end to end—you're able to aid your organization in responding to new business opportunities swiftly, flexibly, and more decisively.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
 Item No: FY21-5908-VMW-CIO-ESSENTIAL-GUIDE-INTRINSIC-SECURITY-WP-USLET-WEB-20210218 2/21