5 Principles of Effective IT Security

Stop Attacks Before They Happen with Better Cyber Hygiene

vmware®

The Growing Security Challenge

Keeping data, applications, users, and devices secure has always been a top priority for IT security professionals. In the past, its most effective defense tactic was a perimeter firewall established around a physical data center. This line of defense was designed to block threats from outside your perimeter from a massive scale of unknown hosts. But, if an attacker slipped past the initial barrier, the assets in the internal network were at risk.

Chasing threats is an impossible task for already overburdened IT security teams—and the threat landscape continues to multiply in terms of volume and complexity. According to a recent study, 360,000 new malware samples are produced every day.[1]

At the same time, organizations are relying less on physical data centers, as apps move from cloud to cloud to endpoint. Simply spending more money or erecting more firewalls isn't the solution either. IT security teams need to consider a new approach to protect their internal networks. Instead of just chasing threats, they also need to focus on reducing their attack surface. By making themselves less vulnerable and susceptible to attacks, they can reduce their overall risk profile.

84%
of organizations claim that traditional security solutions don't work[2]

197 days
the average length of time it takes to identify data breaches[3]

[1] Infosecurity Magazine, 360K New Malware Samples Hit the Scene Every Day, Dec. 2017
https://www.infosecurity-magazine.com/news/360k-new-malware-samples-every-day/

[2] Cloud Security Report, Cybersecurity Insiders, 2018

[3] 2018 Data Breach Study, Ponemon Institute, 2018

It’s Time to Update Your Security Strategy

Reducing your attack surface starts with understanding what you’re trying to protect: the application. Once you focus on the application, you can build a strategy that enforces known good application behavior, not the threat. Every application has a set of behavior patterns or rules that it follows under normal circumstances. When IT security teams know what to expect, it’s simple to see if something is out of the ordinary, or if the application is deviating from its expected role.

Instead of waiting for threats to compromise applications and wreak havoc across your environment, you can stop them before the damage is done. You won’t stop chasing threats—it’s still important to identify known bad signatures—but by also enforcing known good, you’ll develop a well-rounded approach to reducing your attack surface.

To enforce—or lock down—known good, you need:

Intrinsic security

that’s built into your infrastructure, not bolted on as an afterthought.

A deep understanding

of how your applications operate and behave.

Intelligent automation

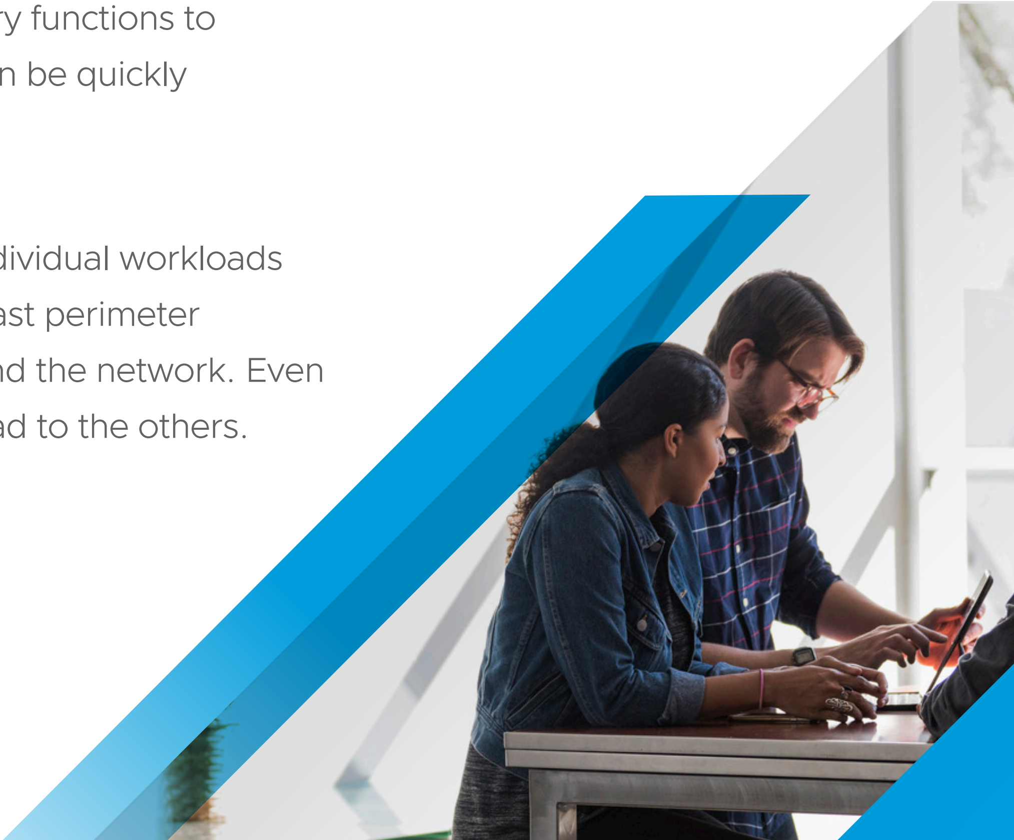
that can keep up with frequently changing applications and policies.

Five Core Principles of Effective Security

There are five core principles to an effective security strategy that organizations should implement. Following these principles well and consistently make cyber attacks harder to carry out and far less damaging. These are also referred to as core principles of cyber hygiene:

1 **Least-privilege computing.** The concept of least privilege is based on allowing applications to do only their intended job, and nothing more. They should be allowed only the minimum necessary functions to perform essential tasks. This way, any deviations can be quickly identified and investigated as soon as they occur.

2 **Micro-segmentation.** With micro-segmentation, individual workloads are protected across the network. If a threat gets past perimeter security, it doesn't have the freedom to move around the network. Even if one workload is compromised, attacks can't spread to the others.



3 **Encryption.** All critical business data should be encrypted both in storage and in motion. If an attacker does manage to steal the files, they'll be unreadable and useless.

4 **Multi-factor authentication.** Passwords alone aren't enough to protect users and data. Multi-factor authentication provides an extra layer of protection, and helps confirm the true identity of anyone accessing data and applications.

5 **Patching.** Things move fast in modern environments—and system requirements and regulations are constantly changing. Consistently patching mitigates the risk of a breach due to out-of-date systems or policies.

Implementing a New Security Strategy

Change can be difficult, especially when it comes to dealing with complex systems. For IT security teams, it is important to lay the foundation while protecting critical applications. Here are the two steps to implementing a new security strategy:

Step One: Implement the core principles of cyber hygiene

It all begins with implementing the 5 core principles of cyber hygiene to set a solid foundation for security. An emphasis on education and familiarization with the 5 principles gets everyone on the same page. They aren't a complete solution, but they will establish a basis for your security strategy.

Step Two: Focus on protecting critical applications

Mission-critical applications are the crown jewels of every organization—and they need to be protected at all costs. Instead of trying to secure the infrastructure as a whole, applications need to be individually secured so that even if a breach occurs, it can only take down one application at a time.

Let's explore each step in more detail.

Step One: Implementing the Core Principles of Cyber Hygiene

One of the most important aspects of this step is knowledge. Here is where you'll learn all about your applications, how they work, and what they are—and aren't—allowed to do. From learning about least-privilege computing to ensuring that everyone understands the importance of multi-factor authentication and consistent patching, it takes the cooperation and education of your entire team to make it work.

It's crucial for everyone in your organization to be educated on modern approaches to security. It's not enough for the IT team or business leaders to stay up to speed. Every single individual plays an important role in maintaining security. For instance:

- **IT professionals** should know how to design security into systems, instead of bolting it on.
- **Developers** should have at least a baseline knowledge of code-security skills.
- **End users** need to know the risks of a security breach and what steps they can take to protect critical information.

Step Two: Focus on Protecting Individual Critical Applications

When you focus on protecting individual applications, it becomes easier to implement the core principles of cyber hygiene. While every workload is important, keeping your eye on the most critical applications can ultimately keep everything safer. Simply relying on protecting the IT infrastructure doesn't have the context you need to truly keep data secure.

Protecting each app requires you to:

- **Take a risk-based approach.** Protect your most sensitive applications first and worry about the infrastructure later.
- **Get specific.** Effective security is granular and protects individual workloads—not just generic, blanket security.
- **Control access to each application.** Set policies in place that ensure an application is doing only exactly what it's intended to do and nothing more.
- **Monitor close to the application.** Traditional security gives an alert when the network has been breached, but it can't tell you which application was compromised. Monitoring close to the application allows IT to quickly identify exactly where a threat is.

Types of business-critical applications

- Enterprise financial applications
- Applications that fulfill customer orders and store credit card information
- HR applications with confidential employee data
- R&D applications that contain trade secrets

Barriers to Implementing the Core Principles of Cyber Hygiene

If cyber hygiene is so important, and so simple to implement, why haven't more organizations taken this approach? It's often because they don't have the resources. Traditional technology and approaches to security aren't compatible with the core principles.

Traditional security approaches can't protect individual apps, because:

- Modern applications are a system of components
- Software functions use a pool of resources like networking, processing, and storage
- Resources are spread across the environment
- Applications share the resource pool, with use changing rapidly over time

Meanwhile, applications continue to evolve

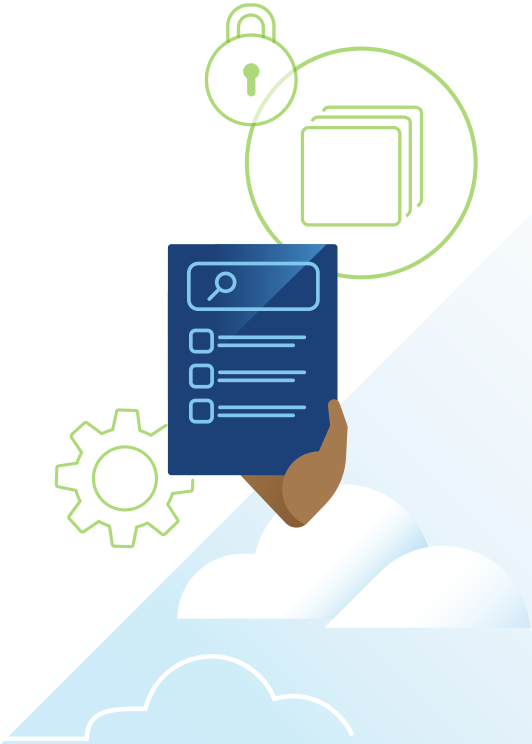
- Applications are moving to a service-oriented approach faster than ever
- Current security that focuses on the infrastructure lacks context and visibility
- As the use of resources vary over time, so does an application's security requirements

Take a Modern Approach to Security

Security in the cloud and mobile era demand a modern approach. By embracing a new approach, organizations will be able to protect individual applications instead of a generalized blanket of security.

In the cloud and mobile era, IT professionals can:

- Leverage intelligent automation that recognizes individual applications and establishes a baseline for behavior and function.
- Create logical boundaries around a group of application components, and then use that boundary to label the applications.
- Protect individual applications with security that follows them across environments and adjusts policies as its requirements change.



Start Your Journey Toward Better Cyber Hygiene

From rapidly multiplying data to ever-changing security requirements and sophisticated threats, trying to keep up can feel like an impossible task. VMware transforms security by using software virtualization to connect and secure applications and data wherever they reside.

VMware builds security into your infrastructure, providing unprecedented visibility and protection for your applications and users from endpoint to cloud. We give you the advantage of certainty, so you can lock down known good application behavior and effectively shrink your attack surface.

Take the Next Step

LEARN MORE ABOUT VMWARE SECURITY SOLUTIONS

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: TNS-0524_VM_Cyber-Hygiene_04/19