5 WAYS TO SECURE APPLICATIONS WHEREVER THEY LIVE

MODERN APPLICATIONS ARE VULNERABLE TO HACKERS AND MALWARE.

Launching a cyberattack is easier than ever, and security losses are on the rise.

2% TO 22%
rise in data center outages between 2010 and 2016.[1]

257 DAYS
is the average amount of time it takes to detect & contain a breach.[2]

$740,357
was the average cost of a data center outage in 2016.[3]

APPS ARE AGILE. SO ARE THE THREATS CHASING THEM.

In today's hyper-connected world, apps are widely distributed across locations, clouds, and branch networks—making the attack surface larger and adding more risk.

To complicate things, applications and data are continually on the move.

Sophisticated and targeted attack vectors, methodologies, and technologies can exploit apps and data.

HARDENING THE DATA CENTER PERIMETER IS NO LONGER ENOUGH.

- Legacy security technologies can't stop threats from spreading laterally after they've breached the data center perimeter.
- Bolted-on security technologies that require manual deployment and configuration can't keep pace with dynamic, distributed applications.
- A modern approach to security must be just as ubiquitous and agile as the applications themselves.

"To create a more secure network, companies must restructure their infrastructure in a way that allows all data to be protected regardless of where it sits in the network."

— Forrester Research, Enabling Zero Trust Security Through Network Virtualization and Micro-Segmentation, 2018

5 WAYS VMWARE SECURES THE APPLICATION INFRASTRUCTURE.

- **Intrinsic security.** Applications and data are secured by default, which eliminates the gaps caused by point solutions.
- **Ubiquitous app visibility.** Application-layer communications and dependencies are visible across public, private, and hybrid clouds.
- **Reduced attack surface.** Micro-segmentation and least-privilege principles shrink the available surface of applications and data.
- **Consistent security from data center to cloud to edge.** A unified, automated platform helps to secure the entire infrastructure, with one policy defined and enforced throughout.
- **Isolation from the threat surface.** Built-in security helps to prevent attackers from turning off controls.

75% OF ORGANIZATIONS

surveyed in a recent study are pursuing network virtualization and micro-segmentation as a key strategic security initiative.[4]

VMware shrinks the application attack surface by delivering consistent, intrinsic security from the data center, to the cloud, to the edge.

- **VMware NSX® Technologies: Enable micro-segmentation on the network to prevent the lateral spread of threats.**
- **VMware AppDefense™: Enforces application intended state and behavior on data center endpoint.**
- **VMware vSphere® and VMware vSAN™: Deliver at-rest data encryption.**

LEARN MORE

Download the White Paper
Core Principles of Cyber Hygiene >

Join Us Online:

Computerist Inc

For more information contact: Tony Camilleri

tonyc@computerist.c
19732260100
www.computerist.cor

1, 5 Cost of Data Center Outages, Ponemon Institute, January 2016
2 Cost of Data Center Outages, Ponemon Institute, June 2017
4 Forrester Research, Enabling Zero Trust Security Through Network Virtualization and Micro-Segmentation, 2018