IT SECURITY: FROM POINT SOLUTIONS TO AN INTEGRATED APPROACH

Close Gaps and Reduce Risk with a Unified Platform

vmware® | intel®

The Only Constant Is Change

Today's security landscape is highly complex and evolving fast. From sophisticated threats to consumer behaviors that put data at risk, IT has the unique challenge of protecting the business without slowing it down.

Digital transformation is occurring at a rapid pace.

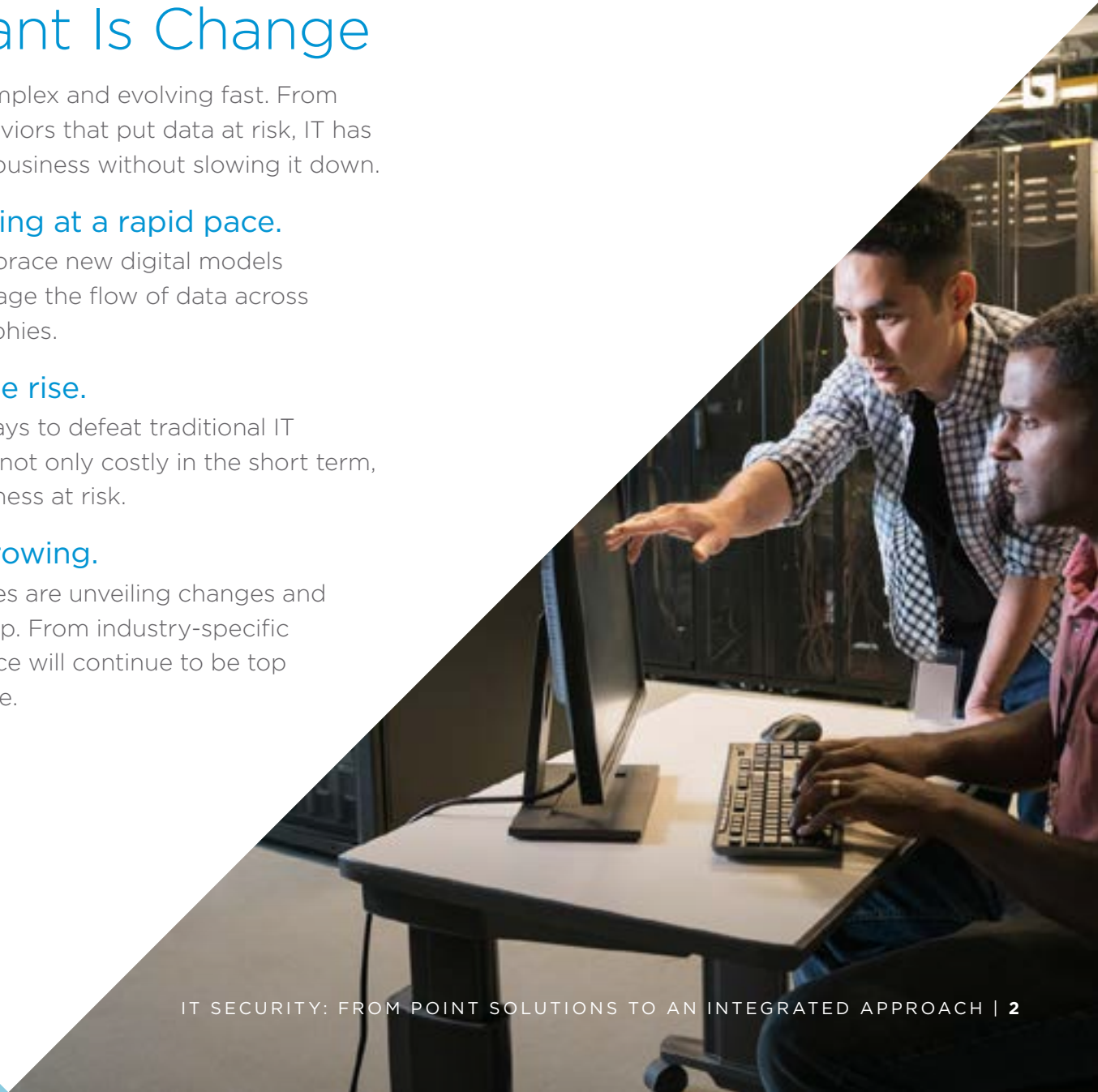
As both businesses and consumers embrace new digital models for products and services, IT must manage the flow of data across a dizzying array of devices and geographies.

Cybersecurity threats are on the rise.

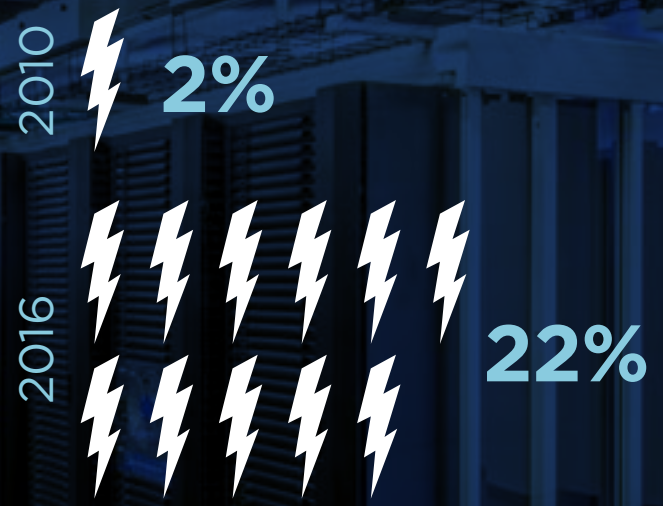
Attackers are savvy, developing new ways to defeat traditional IT security measures. A breach or lapse is not only costly in the short term, but also puts the reputation of the business at risk.

The burden of compliance is growing.

As cyberattacks rise, regulatory agencies are unveiling changes and new compliance standards at a rapid clip. From industry-specific regulations to sweeping laws, compliance will continue to be top of mind for IT organizations of every size.



Cybercrime represents the fastest-growing cause of data center outages, rising from 2% in 2010 to 22% in 2016.[1]



1. Cost of Data Center Outages, Ponemon Institute, January 2016

The Many Components of IT Security

Modern security is multidimensional. IT must take into account the different types of protection needed for different users and situations. Four key areas of focus are:

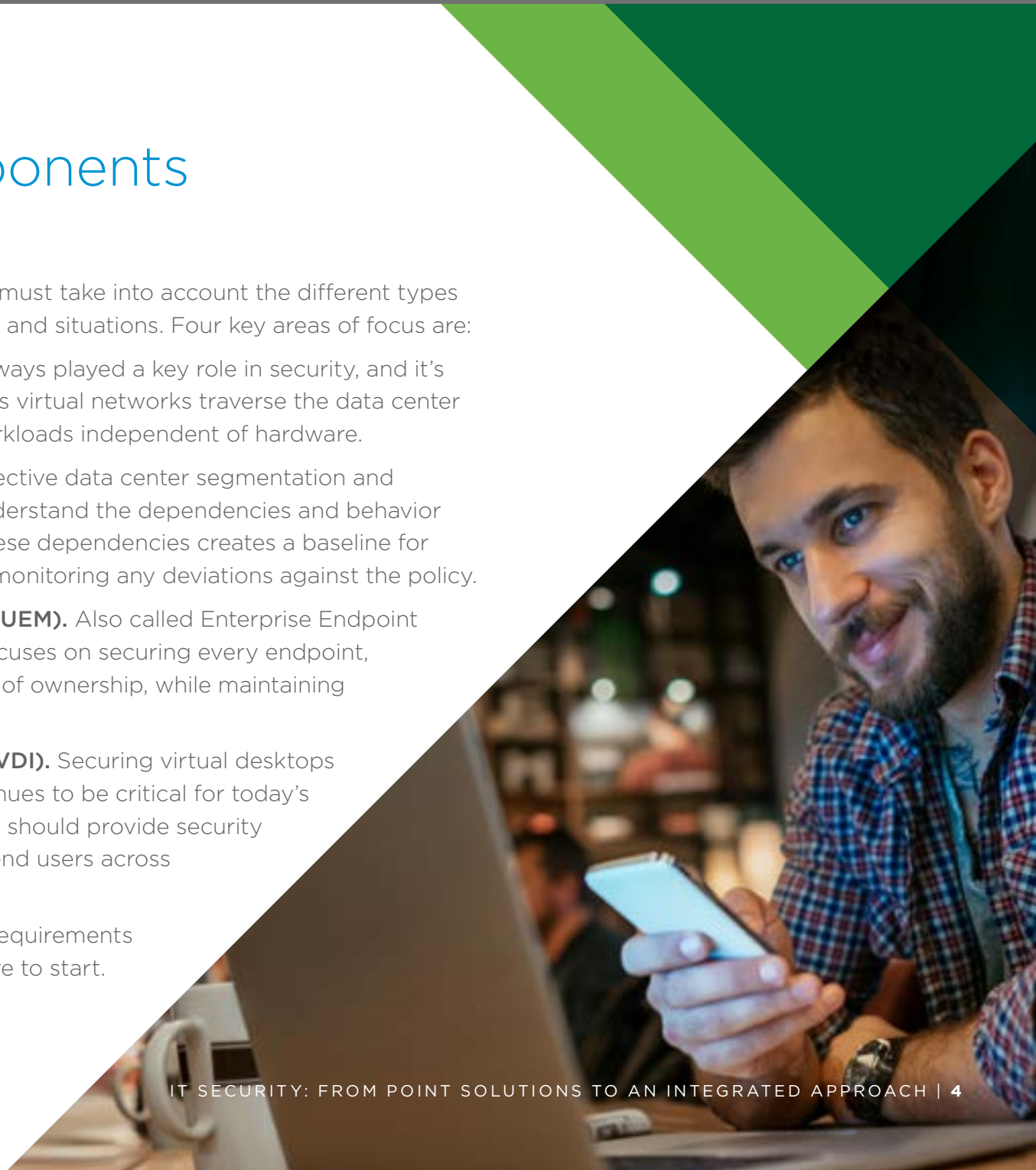
Networking. The network has always played a key role in security, and it's now more important than ever, as virtual networks traverse the data center and public cloud, supporting workloads independent of hardware.

Applications. To establish an effective data center segmentation and security policy you must first understand the dependencies and behavior of your applications. Mapping these dependencies creates a baseline for defining an effective policy and monitoring any deviations against the policy.

Unified Endpoint Management (UEM). Also called Enterprise Endpoint Management (EMM), this area focuses on securing every endpoint, from apps to devices, regardless of ownership, while maintaining employee privacy.

Virtual Desktop Infrastructure (VDI). Securing virtual desktops and published applications continues to be critical for today's highly distributed workforce. VDI should provide security policies that dynamically follow end users across devices and locations.

With so many security challenges and requirements to address, it can be hard to know where to start.

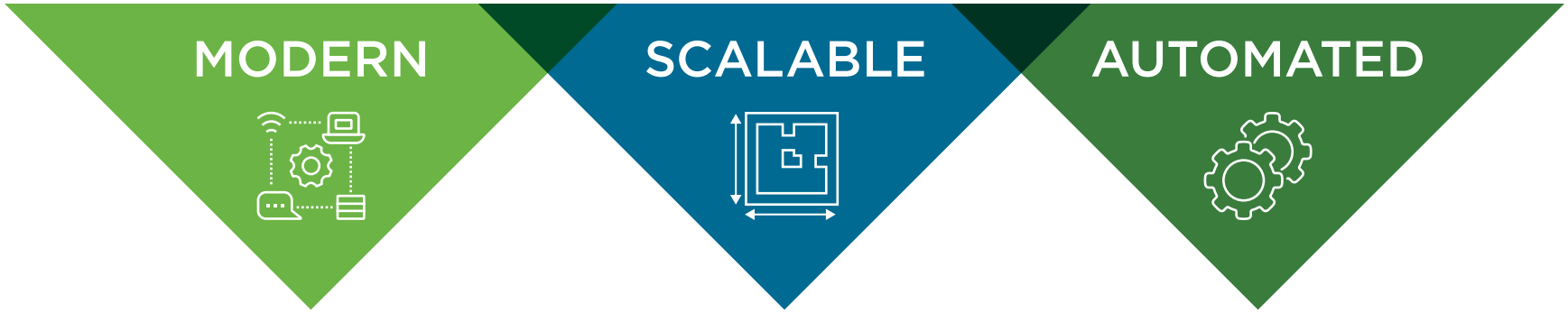


The Importance of a Cohesive Approach

Keeping pace with modern security can be complex, costly, and time-consuming. But cobbling together point solutions isn't the answer; it leads only to new complications, alerts, and tasks. Even worse, a patchwork approach can create unforeseen vulnerabilities, causing even more risk to the business.

What IT needs is an integrated approach to security that addresses all of these areas and more. A unified platform can scale seamlessly with the business, addressing risk and exposure in a holistic way.

An integrated approach to security is:



Let's take a closer look at all three.

MODERN

Address Evolving Security Issues with Modernization

Traditional hardware-centric infrastructure is a huge liability in the digital era. Besides being reliant on time-consuming, manual labor, it doesn't allow IT to respond quickly to the evolving threat landscape.

A modernized, software-defined infrastructure gives you the flexibility to adapt as new threats and security challenges emerge. A modern infrastructure addresses identity and access management, enterprise mobility management, networking, virtualization, and cloud services—all critical components of the digital enterprise.

Look for an infrastructure that allows you to:

- **Secure users everywhere.** Federate identity and integrate that with mobility, so users are secured as they move between locations and devices.
- **Secure all endpoints.** Extend security beyond the data center, from mobile devices to IoT products to wearables to containers.
- **Secure application infrastructure.** Deploy any app through one catalog and align security controls with applications, while encrypting data at rest.

SCALABLE

Improve Agility with a Scalable Solution

It simply isn't feasible or effective to continually build new security solutions to address different types of attack vectors and threats. Today's security teams must implement scalable solutions that enable rapid response and risk reduction, even as attackers evolve.

There is no "one size fits all" approach to security, as needs vary based on your industry, end users, and potential stress points. You need a platform that can be customized to meet your specific needs—providing multiple lines of defense for multiple lines of attack.

A scalable security solution extends far beyond the data center, addressing every user, endpoint, and infrastructure component in every location. This ubiquitous approach helps you maintain control, and allows you to insert security as needed.

AUTOMATED

Ensure Ongoing Protection with Automation

Maintaining secure environments across users and endpoints requires continuous, around-the-clock vigilance. Automation helps solve this problem, allowing you to quickly deploy security services across organizational and geographic boundaries.

Automating core tasks like denying access, remediation, and micro-segmentation works to stop attackers and prevent potential data breaches while allowing your team to stay focused on the bigger picture. Automated security services also detect anomalies and flag potential threats that might otherwise go undetected.

Today, automation is a critical tool for every IT organization, helping to keep security standards high without taking a big bite out of the budget.

How VMware Approaches Security

VMware takes the stance that security should be everywhere. An industry leader in virtualization, VMware builds security into the software layer, making it persistent and pervasive across devices, users, and endpoints, from the data center to multi-cloud environments.

Virtualization technology from VMware provides the ability to create a local level of separation to help improve security, allowing you to create different "zones" based on trust level to protect sensitive information.

VMware solutions help you to:

- Keep up with digital transformation
- Better anticipate and respond to cybersecurity threats
- Stay in compliance with changing laws and regulations

Security Solutions from VMware

VMware offers several products to help organizations deal with new and emerging security threats:

VMware Workspace ONE™
A digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multi-platform endpoint management.

VMware NSX®
A network virtualization and security platform that enables the creation of entire networks in software. All network components can be provisioned in minutes, and micro-segmentation can be used to isolate specific workloads for greater security.

VMware Horizon®
The leading platform for virtual desktops and applications, Horizon lets you provide end users with access to all of their virtual desktops, applications, and online services through a single digital workspace.

VMware AppDefense™
A data center endpoint security product that protects applications running in virtualized environments. Rather than chasing after threats, AppDefense understands how applications are supposed to work and monitors for changes to that intended state that indicate a threat. When a threat is detected, AppDefense automatically responds.

Sharpen Your Defenses for the Digital Age

A rigorous security strategy adds immediate value to the business—and VMware can help you develop one. With a ubiquitous software layer that integrates security across applications and endpoints, VMware offers the solutions you need to move forward with confidence.

VMware and Intel transform security by providing comprehensive security measures based both in software and hardware across application infrastructure and endpoints, maximizing visibility and context of the interaction between users and applications, aligning security controls and policies to the applications they are protecting, and enabling the insertion of additional third-party security services for additional intelligent protection.

GET STARTED TODAY

Learn how VMware can help you transform security >

Join Us Online:

vmware® | intel®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmware-it-security-from-point-solutions-to-an-integrated-approach-TS-0354 02/18