**Draft 1 – Transforming Security Video**

Hello [add speaker info]

The digital transformation continues to accelerate.

Businesses are becoming digital businesses and business outcomes are changing.

Customers tell us that they want more rapid innovation and greater agility. They want to deliver exceptional mobile experiences. And they want to protect their brand.

For the next few minutes, I’d like to focus on how VMware is transforming security and what we’re doing to keep our customers’ data, apps, devices, data centers, and clouds compliant and secure.

Our customers’ infrastructure, applications and end-users are changing rapidly.

IT infrastructures have left the boundary of physical data centers and are extending into the cloud. Apps are evolving from monolithic structures to become distributed and multi-tiered, and data is being hosted everywhere. And, of course, end-users don’t sit in front of corporately managed desktops, but instead do their work from any device, anywhere.

The digital transformation also means that the attack surface is expanding, so the old ground rules of network security simply don’t apply anymore

With monolithic applications, it was like having an entire application in a single skyscraper: it was the only tenant. This meant that no one could touch any part of that application without going through the front door.

But applications don’t look like that anymore. Now, they are distributed across different floors, across different buildings and across different parts of the virtual city. So we need to create a virtual skyscraper around these critical applications and data – a virtualization layer that creates a logical boundary that can adapt as data and applications move and expand.

By micro-segmenting this virtualization layer – essentially reducing the infrastructure’s attack surface – we can more effectively prevent threats from breaching defenses

VMware’s location within the infrastructure gives IT the best possible control point to enforce security policies. It lets the policy follow the application as it moves across private and public clouds.

A virtualization layer between applications and the underlying infrastructure helps IT avoid attacks and also provides an ideal point to encrypt stored data. By encrypting data at rest, organizations can be sure that their application data is safe, even if it falls into the wrong hands.

For endpoints, organizations can employ a single VMware solution to protect smartphones, tablets, laptops, wearables and IoT devices.

This approach lets IT deploy any app – native, web, remote, virtual apps and Windows desktops – with built-in single sign-on, data security, and endpoint compliance.

And since every business has its unique security needs, we can customize environments to align with our customers’ priorities.

But customers’ priorities continue to change, and we are working to anticipate these changes. For example,

* Roadmap example 1
* Roadmap example 2
* Roadmap example 3

As traditional infrastructure, applications, and workforce models evolve, IT is under increasing pressure to protect against emerging new threats.

Our holistic approach to security and compliance – a ubiquitous software layer across application infrastructure and endpoints – is an example of how VMware is transforming security.

Thank you.