|  |  |  |
| --- | --- | --- |
| UNIVERSITY NAME  Business Justification for Cloud Security and Governance  [June 22, 2017] | | |
|  |  |  |
|  |  |  |

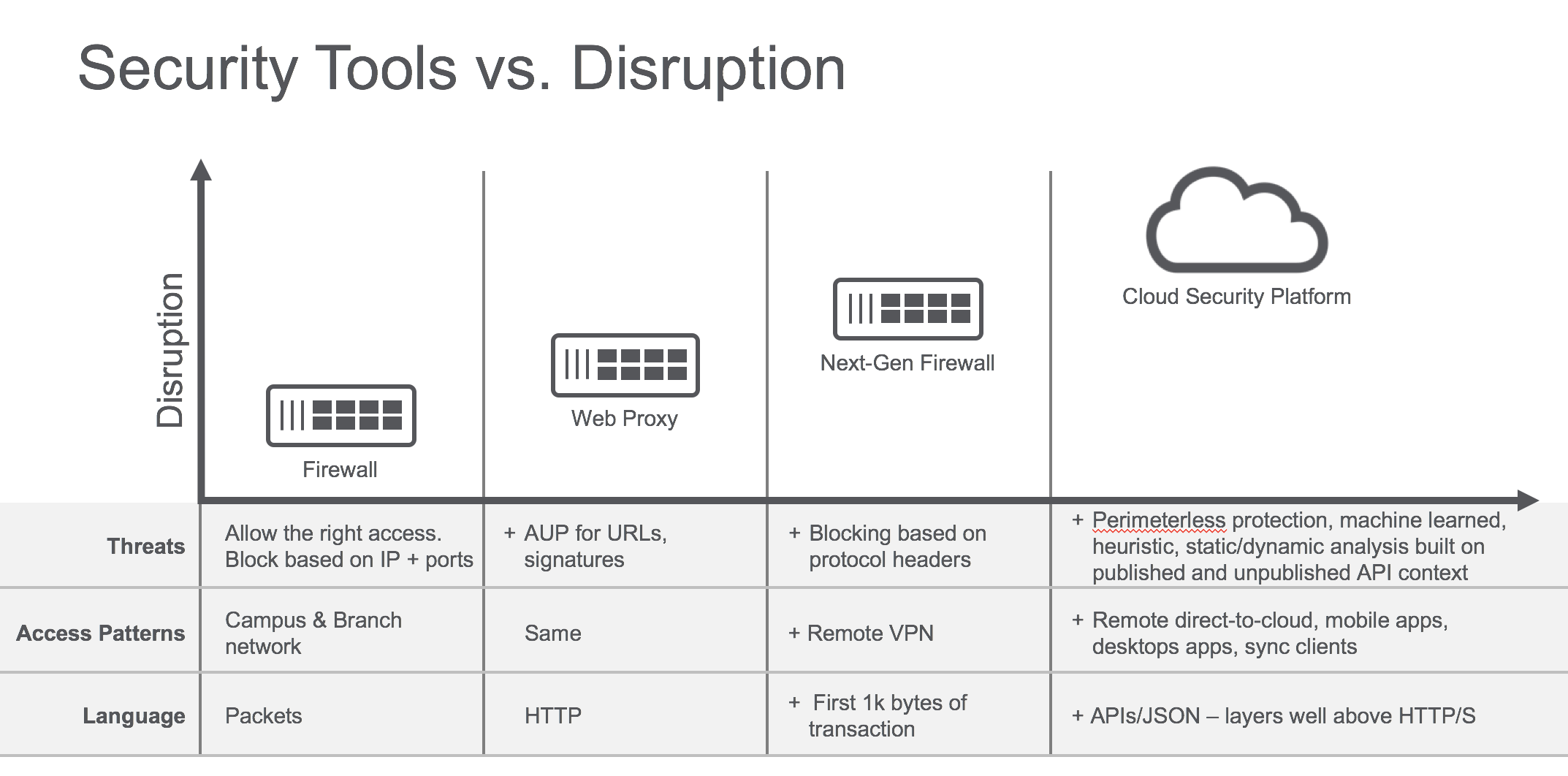
**Executive Summary**

Like many higher education institutions in the United States, <UNIVERSITY NAME> has made significant strides to adopt modern information technology tools and methods. One such area, of course, is the use of cloud computing. Within this category, <UNIVERSITY NAME> is currently leveraging infrastructure as a service (IaaS) and software as a service (SaaS) tools of all sorts to further advance the university’s interests. Whether this is for inter-departmental collaboration amongst faculty, student enablement, or simply to leverage more cost-effective and cutting edge compute and storage capabilities, the cloud has become an integral piece of <UNIVERSITY NAME>’s IT strategy.

Of course, the benefits are doing so are high and for purposes of this proposal, we have assumed that the university will continue to embrace the cloud going forward. With that in mind, we will outline some of the core security challenges the cloud presents, which serves as the backdrop for our recommendation that the university develop and adopt a cloud security and governance strategy.

**Why the Cloud Has Disrupted Security**

Scan the modern workplace or university setting and you’d be hard pressed to find an area that hasn’t been transformed from a computing perspective. Manifested in mobile devices, applications, and social media, it’s a “wild, wild west” era. Underneath these visible cues are new computing languages, networks, and cloud services that are purpose-built to be built and deployed at a rate that eclipses what was considered “cutting edge.” Relatively speaking, these changes have occurred quite recently and the disruption has rippled in such a way that the legacy security tools that were quite effective 10 years ago are quickly becoming obsolete. The technical reasons for these challenges can be captured in three buckets – the language these new services speak, the access patterns that now exist, and the threats that have come onto the scene. The disruptive moments can be marked by the security tools as depicted here:



**The Challenges Introduced by the Cloud**

*Lack of Visibility*

As organizations’ productivity tools move to the cloud, new security tools and processes are required to accommodate that shift. Today, IT and IT security have little or no visibility into what cloud services are being used, much less the ability to audit usage and detect things like data leakage or exfiltration. This is particularly relevant to SaaS, where the term “shadow IT” has been used to describe the 1,000+ services that used, on average, in every organization. Sometimes referred to as “the Dropbox problem,” this challenge has stemmed from the ease of procurement that has persisted for the last decade. The lack of visibility has also crept into IaaS usage within the last two to three years as these services have become the development and deployment environments of choice for custom application development. Provisioning an Amazon Web Services (AWS) environment is quite simple and requires little or no IT intervention.

*No Policy Compliance*

Beyond visibility, much of the cloud lacks the standard security controls that exist in traditional network and application environments. As such, enforcing policies such as different access levels to users on university versus personally owned devices, govern cloud activities such as “share” and “download” for users in different directory groups or university departments, and control activities and data in different instances of the same app (such as a university-sanctioned version of Office 365 or Box versus the many personal instances that users access). The network/campus perimeter tools in place cannot address these challenges.

*Risk of Data Loss or Exposure*

The lack of visibility and policy enforcement means the university cannot see whether and how much sensitive or regulated data our faculty or administration have in university-sanctioned or unsanctioned cloud services. IT security personnel need to be able to find and protect sensitive content in university-sanctioned apps as well as detect sensitive content on its way to unsanctioned apps and block the activity or encrypt the content on-the-fly. Up to now, many organizations have responded to this risk by attempting to apply brute-force blocking of the cloud, but by all measures this tack is ineffective as it creates an “exception sprawl” problem and forces users to find an alternative (often lower-quality) service, forcing us into a vicious cycle.

*Cloud Malware and Other Threats*

According to a study from the Ponemon Institute, one out of three organizations have cloud malware and don’t know it. Moreover, 31 percent have experienced one or more data breaches involving cloud. Hackers are going where the data are, and today that’s cloud. <Partner> are seeing a growing number of malware and ransomware incidents involving cloud, and we believe that’s because malware can hide in plain sight in many cloud services. To make matters worse, organizations can’t protect themselves because they either don’t know about the cloud service or they’re not inspecting it when it comes into the network due to performance degradation issues.

**The University’s Unique Cloud Security Considerations**

As we touched on earlier, <UNIVERSITY NAME> sees cloud is a key component of its IT strategy that’s closely connected with the guiding objectives of the institution. In particular, IaaS initiatives like the expanded use of tools like AWS will lead to advantages over other institutions that have been slower to move in this direction. <PARTNER> contends that this will have a ripple effect in the university’s ability to attract talent as well as the computer sciences and related programs. In addition, like most institutions around the world, <UNIVERSITY NAME> is adopting SaaS at a rapid pace, which will also result in benefits in every corner of the university – from faculty to the student body itself.

Within the scope of that mentioned above, <PARTNER> sees the following practical needs for <UNIVERSITY NAME>

* The university needs techniques/tools that will allow them to gain visibility and control of user activities across AWS IAM, S3, and EC2 for custom apps and services,
* University personnel must be able to run compliance reports and audit activities in one dashboard, with Amazon CloudTrail integration,
* The university needs to protect sensitive data contained in AWS S3 buckets. To do so will require cloud DLP and an integration with the university’s on-premises DLP system,
* IT and IT security must be able to reign in access controls for university-sanctioned AWS accounts and block unsanctioned, non-university-sanctioned AWS accounts
* The university needs to be able to derive policy based on managed vs. un-managed (BYOD) devices.
* Security personnel need the ability to detect and remediate cloud threats like malware and anomalous behavior.

**Emerging Technologies that Address Cloud Security Challenges**

<PARTNER> works with a broad ecosystem of technology vendors and has built a center of excellence in emerging technology. One such area is our’s cloud access security broker (CASB) partnership, which focuses on the exact area of need that <UNIVERSITY NAME> is experiencing when it comes to the use of cloud. After an extensive search we decided to partner with Netskope, Inc.

A leader in the cloud security space, Netskope that has been in business since 2012. Headquartered in Los Altos, California, they currently employees more than 350 personnel and was recently featured in publications like the New York Times after having received $100 million in financing from some of the top venture capital firms in the country. They’ve won numerous awards and were named a “Cool Vendor” by Gartner a few years ago and are deployed in some of the most well-respected brands in the world, including Staples, Starbucks, Nike, Dignity Health, Kaiser Permanente, Caterpillar, and Charles Schwab. In the university setting they have been deployed at the Icahn School of Medicine and Johns Hopkins University.

From a product point of view, Netskope is known for several things:

The first of Netskope’s differentiators is that they have a biased towards cloud enablement and the ability to take action. Unlike early vendors that focused on discovery and blocking services, Netskope sees discovery as the first step and provides granular visibility and control of both sanctioned and unsanctioned services by default and doesn’t care if users are on-premises, remote, on a mobile device, or accessing services via a native or sync client. Unlike vendors whose architectures limit IT to seeing only 5-10 percent of all cloud activity, Netskope enable you to see – and take action on – all of it.

The second difference Netskope brings is their advanced, enterprise DLP. Unlike other vendors whose data protection options are either too simplistic or bury you in false positives, Netskope offers the market’s most robust DLP engine combined with filtering mechanisms to achieve very high levels of accuracy. This will let you e-discover – and protect – the university’s most sensitive data in the cloud.

In addition, Netskope separates itself from its competitors through its advanced threat protection capability. Beyond looking for routine anomalies or blocking access from users with compromised credentials, Netskope uses static and dynamic analysis of files to detect if malware and ransomware are coming in to the university via cloud services.

Finally, Netskope’s architecture is built for any situation. Even if you’re starting with cloud services discovery, Netskope’s architecture supports modes such as an on-premises appliance that supports your data privacy and residency requirements. As you grow, Netskope will support the added deployment modes, services, apps, and devices that make up the university’s requirements.

**Next Steps**

<Partner> recommends that <UNIVERSITY NAME> conduct a cloud risk assessment as a first step in understanding the scope of challenges the university will need to address. Upon completion of the cloud risk assessment, <Partner> asks that the senior executives with responsibility for security and cloud services make themselves available for a formal review of the findings and presentation of recommended actions.