SECURING YOUR REMOTE WORKFORCE IN THE CLOUD

GUIDEPOINT CLOUD SECURITY SERVICES

A WORD FROM OUR DIRECTOR

JONATHAN VILLA

What has fascinated me about cloud computing over the past 14 years is watching it evolve as quickly as new ideas are conceived. Recently, what has made me proud to work in the cloud computing space is seeing how quickly and efficiently the delivery model stepped up to support the business world. Within one week, one fifth of all students worldwide were out of school and within the next two weeks nearly one third of the world's population was living under varying levels of restrictions. These were extreme changes in our physical world for which we were unprepared. However, in the digital world cloud computing scaled quickly to provide the dependencies needed to support a new remote workforce, deliver remote learning, process and share vital research data, and even help us feel close to our friends and family, albeit on a computer screen.

This pandemic also reminds me of when I realized I knew how to swim. Standing at the deep end of the pool, I was pushed in and quickly put into motion what I learned in my swimming classes. This pandemic has done the same for many organizations. There are security leaders that were adverse to moving to the cloud, but then 2020 happened. Finding themselves forced to secure a remote workforce and maintain business continuity, they are quickly putting their skills into motion by looking to maintain confidentiality, integrity, and availability in their new cloud datacenters.

Fortunately, the cloud has been ready for such a time as this. With services ranging from virtual desktops (AWS Workspaces), securing a disappearing perimeter (Zero Trust), and centralizing management of remote assets in the cloud (Intune), cloud service providers seem to have been sitting on the sidelines calling out, "put me in coach". Join GuidePoint's Cloud Security Practice as we explore some of the solutions that have stepped up to the plate during a time when the digital world needed an almost overnight solution.

CHAPTER
ONE
ZERO TRUST

CHAPTER
TWO
DEVICES

[1] https://www.thinkglobalhealth.org/article/updated-timeline-coronavirus

CHAPTER ONE

Zero trust, that's where we are now. This does not apply only as cybersecurity professionals, but as humans; humans tackling something that the world has not experienced in recent memory. The global pandemic known as COVID-19 caused a monumental shift in how businesses, and the world, operate. Suddenly, security and risk management are no longer the domain of certain professions, but risk calculations now inform every choice people make in their day-to-day lives.

THE SOCIAL (DISTANCE) NETWORK

Why must we all wash our hands? Because we have to assume they've contacted hidden threats: zero trust. Why should we all wear masks? Because the infection can spread before we know it is there: zero trust. Why can no one go to work? Because we could be a risk to our freinds and peers and not even know it ourselves: zero trust. In our day-to-day lives, we have been thrust into a zero trust model. Ironically, this is a term that has become increasingly popular in the security community as well, and we should take this paradigm shifting opportunity to integrate zero-trust into our organizations. The cloud can help!

Millions of organizations around the globe have been forced to rethink their assumptions of how they operate. Gone are the controlled corporate networks, the VPN for all, as well as the company owned and operated endpoint. Organizations are faced with the need to enable employees workers who must be able to work whenever, wherever, on uncontrolled networks, driving the necessity of Zero Trust models to secure our organizations.

Cloud technology is the ultimate enabler of Zero Trust Architecture...

Zero Trust Architectures are those that focus on securing the data and authorizing each request to access that data, there is no assumption of a trusted endpoint, device, or network. The NIST Special Publication Draft defines Zero Trust as an ever-evolving security paradigm that protects organizational resources over network segments, particularly as more organizations move their infrastructure to cloud assets as opposed to a physical, enterprise-owned, network perimeter.   "... an evolving set of network security paradigms that narrows defenses from wide network perimeters to individuals or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary."

Cloud technology is the ultimate enabler of Zero Trust Architecture by enabling straightforward deployment of software defined perimeters. Those are networks built on the concept of securing access to the data rather than securing access to the network. Organizations can leverage the cloud to enable a remote workforce at a speed that was never possible before while simultaneously decreasing their risk by moving away from the "trust by verify" model to one of Zero Trust. The Cloud facilitates easily provisioning only necessary access to organizational applications and resources that are required for specific employees to complete their work function. This reduces risk and minimizes the possible attack surfaces that could compromise the network.

For example, IT managers can quickly provision ephemeral, self-contained, limited virtual desktops that can be securely accessed fromover untrusted networks on commodity hardware. Backing these virtual desktops with services such as AWS WorkDocs and Azure File Storage, confidential company data can be stored in a way that limits its distribution, guarantees integrity, and increases availability; CIA Triad achieved.

DevSecOps teams operating in the cloud can build out highly scalable, ephemeral infrastructure that can respond to sudden changes in demand through the use of elastic compute services. This flexibility enables the organization to quickly adapt to changing customer needs while minimizing costs through on-demand pay as you go services that only bill for compute and network actually used. Great examples of this are both the increased needs for video conferencing as well as watching streaming videos during, say, a global pandemic. Video conferencing solutions can scale their resources quickly to support a sudden influx of new users, and your Netflix streaming has been enabled by Cloud Architecture for years. No longer must an organization forecast demand 6 months forward just to spend capital on hardware of which 30% will sit comatose, they only have to spin it up, and secure it, pay for it, when the need arises.

Organizations that embrace cloud technologies and Zero Trust architectures are laying the foundation that will enable them to face the next great calamity. The ability to quickly respond to events unknown will help them to weather the storm while keeping their customers happy and their employees and partners safe and secure. The way the world thinks about security, risk and trust is changed, and make no mistake it will not be going back.

Be prepared, be agile and stay safe.

DEEPER DIVE

To read more about NIST guidance SP 800-207 with the zero trust architecture visit their site at:

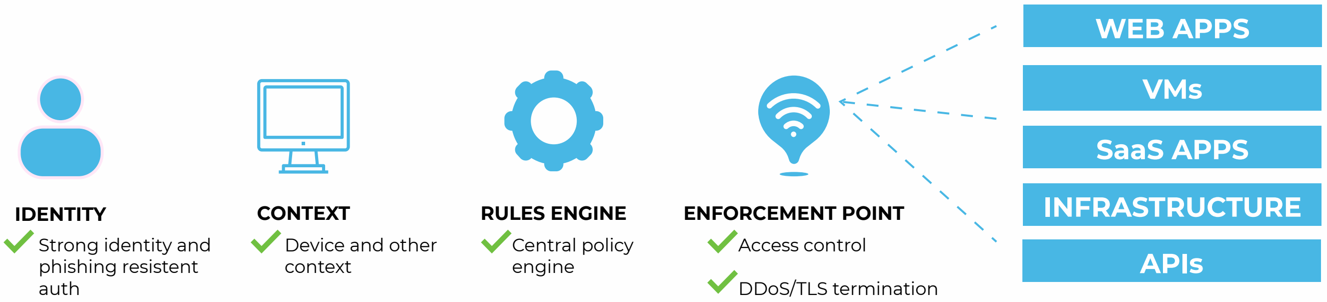
https://csrc.nist.gov/publications/detail/sp/800-207/draft

GuidePoint SECURITY
TOPIC: THE FIVE PHASES OF CLOUD SECURITY ARCHITECTURE
Now On-Demand
Presented by Jonathan Villa
Director, Cloud Security, GuidePoint Security

While the cloud enables and simplifies the implementation of Zero Trust architectures, there is still work to be done to put it in practice.

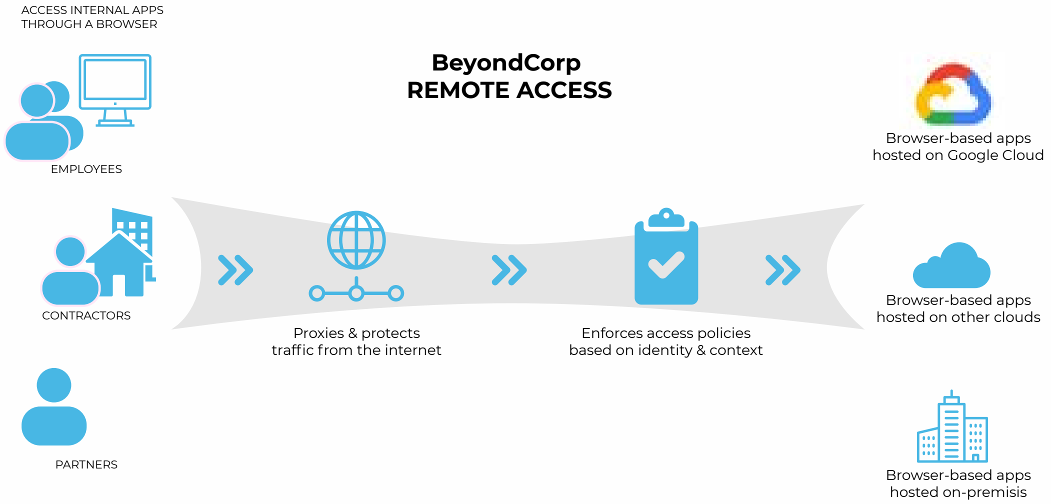
The typical corporate approach to the need for secure access to data from anywhere is still the Virtual Private Network. This solution often requires an agent to be installed upon the endpoint, introduces high amounts of latency to the connection, and is challenging to scale and secure. Let's examine a Zero Trust alternative to this often problematic VPN implementation, BeyondCorp.

BeyondCorp was developed by Google in 2011 as a response to incidents of nation state supported attacks against major silicon valley companies in years prior. Google's stated goal at that time was "to enable Google employees and our extended workforce to work successfully from untrusted networks on a variety of devices without using a client-side VPN". BeyondCorp takes this concept and expands it far beyond the basic capabilities of a VPN. Google's solution has been tested, at scale, by its employees for the last 9+ years. During that period Google has demonstrated that these solutions are scalable, maintainable, and most importantly, secure.



BeyondCorp Remote Access's high-level architecture.

BeyonCorp utilizes a collection of systems to provide identity aware access to systems, applications, data, and even APIs.


ACCESS INTERNAL APPS THROUGH A BROWSER
BeyondCorp REMOTE ACCESS
EMPLOYEES
CONTRACTORS
PARTNERS
Proxies & protects traffic from the internet
Enforces access policies based on identity & context
Browser-based apps hosted on Google Cloud
Browser-based apps hosted on other clouds
Browser-based apps hosted on-premisis

BeyondCorp's high-level architecture.

IDENTITY

This is a combination of the user and a device such as a FIDO Security Key, the usage of a physical token prevents phishing of One Time use Passwords.

CONTEXT

This is a combination of device information, location, time, IP, session age, and more.

RULES ENGINE

Management plane which allows organizations to configure their own rulesets for what combination of Identity and Context can access the applications, infrastructure, APIs, and data.

ENFORCEMENT POINT

This is the control point which implements the Rules Engine decision, provides DDoS and TLS termination.

DEPLOYING A ZERO TRUST APPLICATION

Let's walk through a proof of concept application enablement of the internal Acme "Unicorn App". This application was developed in house, run on the cloud, and is key to the sales organization who previously had worked out of regional offices. A disruption has occurred resulting in the entirety of the sales organization working remotely. Due to this IT is tasked with quickly provisioning access to this app so that the sales team is not disrupted.

The first step is to identify the users, for this Acme will leverage Google Identity, though any SSO provider with support for Multi-Factor Authentication would be a reasonable choice. As an extra layer of authentication Acme also chooses to deploy Google Endpoint Verification, this supports both the company owned assets deployed via G Suite control panel and provides the opportunity for employees to add it to their personal devices. Combined these systems provide the data to power the context based access controls Acme will configure in the next step.

Step two is to configure the rules that will allow or reject incoming connections based upon the user and device context. Acme is all in on Google and selects Access Context Manager rules engine. This allows the IT Admins to create policies to allow access, or disallow access when specific user and device context is matched. Admins have the ability to craft one set of rules and apply them across a variety of applications or organizations. Rules can be based on OS version, browser patch level, location, network, local time or a wide selection of other metadata from the device. With the sensitive nature of sales data Acme has decided that only company owned devices, with current patches, and disk encryption enabled, connecting from the Americas and EMEA will be authorized. In order to protect against phishing attacks they have provided the sales team with FIDO keys and enabled MFA as a required connection component.

> *While Google pioneered the concept of Zero Trust with BeyonCorp, industry adoption was quick and there are a multitude of vendors offering services to enable your organization to move to a Zero Trust model.*

Step three is the Identity Aware Proxy that sits in front of every connection request, this applies the context-aware ruleset, enforces encryption, and provides DDoS protection and TLS termination. IAP's are near zero latency solutions that don't impact the user experience while greatly enhancing the security of the services provided by the organization.

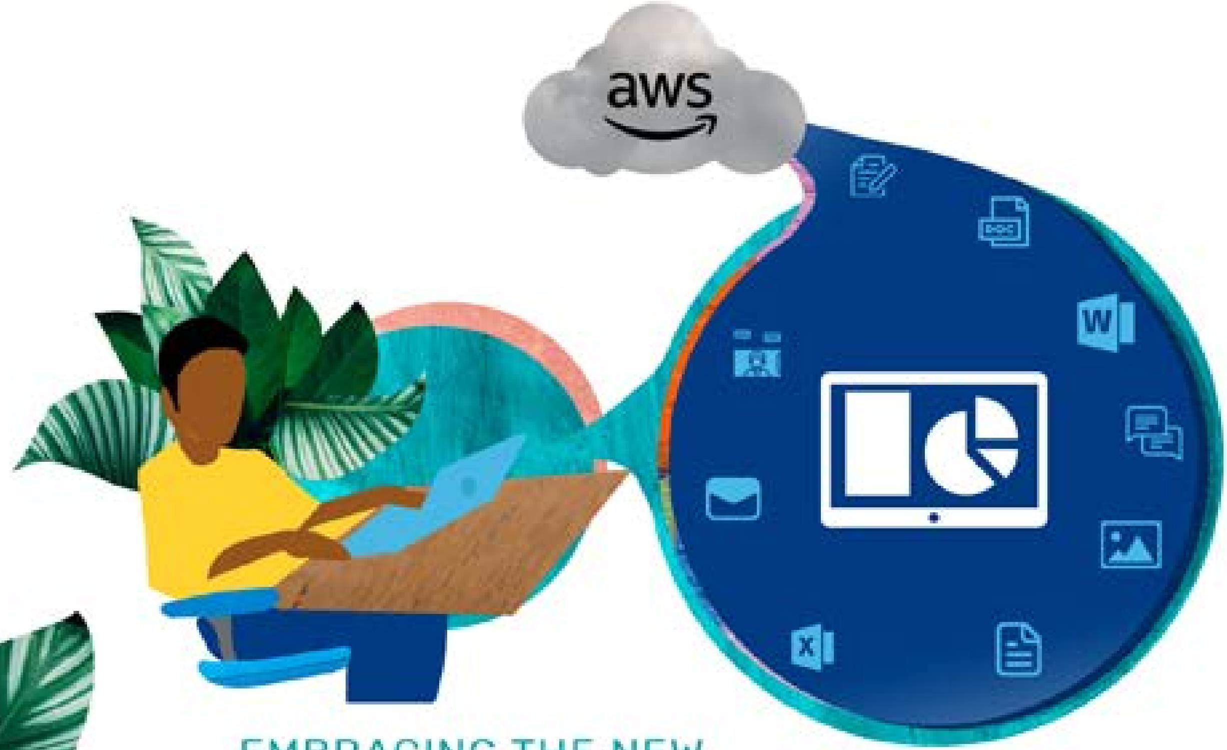
The final step is the connection to the Unicorn App, no changes were required to be made to this app, it is not exposed externally, it is the same application that was deployed previously and exposed to the internal network.

All of the above systems and services can be quickly provisioned with minimal IT overhead and limited configuration of employee endpoints. These features allow an organization to quickly roll out Zero Trust networks to allow secure, context aware access to a variety of applications both internal and external.

While Google pioneered the concept of Zero Trust with BeyonCorp, industry adoption was quick and there are a multitude of vendors offering services to enable your organization to move to a Zero Trust model.

CHAPTER TWO

Over the last two months IT administrators have battled with the need to move a majority of their organization to a remote workspace. The speed of the response is instanious adding security to that problem has been challenging to organizations across the globe. Let's explore a few platforms that help IT not only deliver a successful remote workplace program, but ensure it's security posture is strong.



EMBRACING THE NEW CLOUD CULTURE

Now that working from home has become a necessity for businesses across the globe, organizations are facing the need to adjust to an almost completely remote workforce, one they may not have previously planned to support. Such drastic implementation forces many organizations to answer questions such as “How do you enable employees to securely work from home with the same protections they had in the office?” and “How do you ensure that employees’ access to corporate networks are coming from secured and healthy devices?”

As with many challenges, AWS has long provided a solution that has been purpose-built to help customers with their remote workspace needs, Amazon WorkSpaces. Amazon WorkSpaces is a cloud-based managed Desktop-as-a-Service (DaaS) solution that allows organization administrators to provision Windows or Linux virtual desktops in a matter of minutes with all the necessary operating system, compute, and software resources identified by corporate requirements. In addition, administrators can integrate with an organization’s existing Active Directory environment through an AD Connector or deploy a fully managed Active Directory instance in AWS so that employees can continue using their existing credentials. This provides administrators the ability to provide seamless access to corporate resources or create a standalone managed directory. If the current needs are short term or need to be available

ASAP, Amazon WorkSpaces provides a standalone managed directory to facilitate a quick deployment. Additionally, Amazon WorkSpaces provides IT administrators with an application catalog, the ability to control application versions, and tracking to monitor application usage. Additionally, Amazon WorkSpaces serves as a cost-effective solution with AutoStop capabilities where the Workspace stops when it is no longer being used and starts automatically when a user logs on.

Once the Amazon Workspaces are provisioned, administrators can secure the overall process beginning with access governance and network security to workstation compliance. Users can connect to a WorkSpace through the Amazon WorkSpaces client application that installs directly on the users device (a laptop or a tablet). Organization administrators can specify what device can be trusted to access corporate data through valid certificates. Once configured, user device access can be managed based on IP address and client device type such as Windows PCs or macOS.

> *“With a few steps and clicks, organizations can start embracing this work-from-home journey immediately with Amazon WorkSpaces.”*

To meet compliance requirements, Amazon WorkSpaces can be set up to meet HIPAA-eligibility and PCI compliance standards such as multi-factor authentication. Data that resides within WorkSpaces is not sent to nor stored on the end-user device, but rather encrypted and integrated with the AWS Key Management Service (KMS). Administrators can encrypt a WorkSpace and it’s root volume using KMS customer master keys(CMK), this will ensure that the data stored at rest and snapshots created from the WorkSpace volume are all encrypted.

Shared data is managed in a similar fashion through Amazon WorkDocs, allowing collaboration across an organization via encrypted cloud storage leverage the same tools and services outlined in WorkSpaces above.

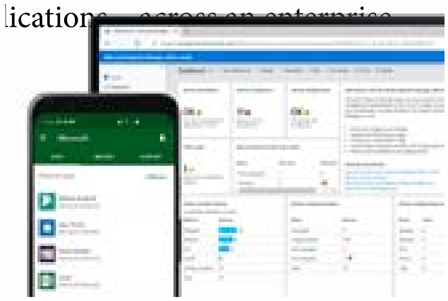
With a few steps and clicks, organizations can start embracing this work-from-home journey immediately with Amazon WorkSpaces. Enable employees to continue to focus on critical tasks and be productive while doing so securely. If you have any questions around AWS WorkSpaces, feel free to reach out to us @guidepointsec on twitter or email us at info@guidepointsecurity.com.

GETTING TO KNOW ENDPOINT MANAGER

Microsoft had been looking, since 2011, for a better way to manage devices beyond the basic software push. The then current solution, System Center Configuration Manager (SCCM), had worked well to manage software and devices, but it had limitations. Microsoft introduced Intune in 2011 in an effort to work around these limitations. The adoption rate of InTune was slower than a snail crawls, and the actual use case for it wasn’t adopted by the IT world. Was Intune a great product for managing devices? Yes. Did it lack features and functionality found in SCCM? Yes. So, what is Microsoft to do when they have two products that do almost the same things with a few key differences? Get rid of the weaker one and only the strong survive? No way! Microsoft pushed ahead and decided to join the two tools in order to create a more robust solution that can handle the emerging markets.

The truth is the business world is composed of Company Owned Devices (COD) alongside the growing Bring your Own Device (BYOD) trend, as well as Mobile Devices (iPhones, iPads, Android devices). Microsoft Intune can handle the mobile devices with no issues, so that’s a plus to Intune and no need for SCCM, right? Well, no Even though mobile devices are growing in numbers they still haven’t replaced the full functionality of a laptop. Regardless of the tablet marketing campaigns that ask“What is that?” and answer with “ It’s a computer” at the end of the day, current tablets haven’t crossed over to fully replace laptops. Without creating new restrictions, what can an organization do to manage mobile devices along with BYOD laptops they allow? Intune can in fact manage all of these devices. Sounds great so far, why not continue to push Intune? The issue here is that the key features, policies and management details that are provided via SCCM do not exist in Intune. Real, full, and thorough management cannot happen without SCCM in addition to Intune.

What is Microsoft to do with two products in the same space that they are constantly developing? Their decision was to integrate them into one superior system, Microsoft Endpoint Manager. IT teams that manage laptops, mobile devices, COD, and BYOD now have one single unified platform they can go to in order to manage all of these devices. Need a single console where you can access application management for laptops and mobile devices? No problem uses the new console. Want company portal branding for your management portal in place of Intune? No problem, use the new console. See where this is going? Now Microsoft has created a place where companies can use tools like ConfigMgr, Intune, Device Management Admin Center, and Desktop analytics. IT admins now have a console and the tools needed to manage both on-premises and cloud devices as well as co-management options to provision, deploy, ma lications – across an enterprise.



In today's connected landscape the movement of sensitive corporate data into the cloud enables companies to scale as it allows for remote workers to maintain productivity. How does an organization maintain security when a growing number of companies are allowing users to access company data from cell phones and personal laptops and from dynamic locations? The need to create dynamic access policies to protect confidential data on any employee owned device makes Microsoft Endpoint Manager (MEM) a key service offering. MEM enables control of devices in a transparent way, allowing employees to work securely on personally owned hardware without the fear of "Big Brother" watching their every move. This new tool will allow for secure management of devices without the need for multiple consoles and multiple subject matter experts from various disciplines.

GuidePoint
SECURITY

www.guidepointsecurity.com