Global Information Assurance Certification Paper

Shall We Play a Game?: Analyzing the Security of Cloud Gaming Services

GIAC (GSEC) Gold Certification

Author: Adam Knepprath, adam.knepprath@student.sans.edu
Advisor: *Bryan Simon*

Accepted: *September 2nd 2020*

Abstract

The adoption of cloud gaming services is quickly growing. Like many services that are eager to go to market, cloud gaming services lack strong security measures. This paper provides an analysis of three cloud gaming service providers' privacy policies, out of the box security, and mitigations end-users should consider.

1. Introduction

Gamers are a large population and an attractive target for adversaries. The video gaming market in the United States alone is 164 million people ("2019 essential facts about the computer and video game industry," 2019). This is roughly half of the U.S. population ("Census - Geography Profile," n.d.). Activities like circumventing copy protection and pirating games are high-risk behaviors because the download sources cannot be trusted. Also, the games may have been modified with any variety of malware. Assuming one could verify the original game files validity, the copy protection circumvention tools could contain any payload beyond its purported use. This high-risk activity contrasts with purchasing games through trusted retail and online sellers or using a cloud gaming service from a reputable company, where genuine licensed games are expected.

In 2016, the now-defunct LiquidSky released the proof of concept for delivering a virtual machine streaming service to gamers. LiquidSky provided a gaming computer hosted in their data center on a high-speed, low latency network and streamed audio and video to their customers' devices. This service enabled gamers that otherwise would be excluded because they lacked a powerful enough PC, access to the latest and the most resource-intensive games. LiquidSky was appealing for many reasons, such as playing PC games on a MacBook, iPhone, Android device, Chromebook, or under-powered desktop or laptop computer. This cloud gaming service is useful because the hosted gaming hardware and software resources, local device's specifications. Gamers using the LiquidSky app on their device send mouse, keyboard, and controller inputs to the cloud gaming virtual machine and receive a gaming-optimized video and audio stream in return. This cloud gaming service is akin to Infrastructure as a Service (IaaS), and the application used for streaming is like a Remote Desktop Protocol (RDP) application in enterprise information technology. IaaS cloud gaming services delivered as a Windows virtual machine offer complete control of the Windows environment. These services provide the most flexibility but also require the most upkeep.

Not all cloud gaming is delivered via an IaaS solution. Services like Google's Stadia, Nvidia's GeForce Now, and Microsoft's Project xCloud provide a Software as a

Service (SaaS) model to gamers. Similarly, streamed game audio-visual output and controller input exist; however, visibility and control over the underlying operating system are not available or required. This method of only delivering video game audio-visual stream to the gamer puts the onus of cloud system security on the provider and leaves little for the gamer to decide. The SaaS gaming solution may be preferred by some gamers, especially those who do not want to manage the underlying operating system.

There are several drawbacks to the SaaS model. One drawback is that gamers are limited to the game library that the service is offering. For instance, when Nvidia's GeForce Now cloud gaming service launched, the popular video game Halo was unavailable. Nvidia later added Halo to their library to have it removed this past April (Marshall, 2020). Another drawback is that gamers may have to repurchase games they already own. Google's Stadia requires gamers to purchase games in their store to play them, even if they already own a licensed copy. Finally, none of the SaaS cloud gaming services would permit gamers to install games with self-contained installers, such as vintage or retro titles.

When commercial cloud services were first released, there was an assumption made about the provider's responsibility in the management, monitoring, and security of the cloud services. From the commercial customer's perspective, the assumption was that the provider was responsible for network security along with the provisioned resources, despite the provider clearly defining terms of service. Commercial customers using cloud services have learned this reality and better understand the shared security model. The gaming community likely assumes that its cloud gaming service is secure and private.

Gamers who use these cloud gaming services face risks, such as; theft of games or game registration keys, theft or denial of access to video game libraries, and theft of in-game assets or currency. With access to video game libraries, forms of payment are often stored, and therefore, unauthorized purchases could be made and gifted to a third party or transferred off the account for resale.

When the gamer uses their IaaS cloud gaming service for activities other than gaming, they introduce additional exposure. This exposure includes the invasion of privacy by unauthorized access to the cloud gaming virtual machine via a breach of the

data center or their assigned cloud gaming virtual machine. This exposure may include access to the virtual hard drive of the cloud gaming virtual machine, including access to browser history with saved passwords or forms, chat logs, and other private data. It can also include remote access to the cloud gaming virtual machine or networking monitoring from improperly compartmentalized resources. These threats are not novel and exist without the IaaS model cloud gaming services. The misunderstanding of the shared security model of cloud services can be compounded by improper advice resulting in increased exposure to the gamer.

This paper focuses on Blade's Shadow, Paperspace's CORE, and Parsec running on Microsoft Azure. These three currently operating cloud gaming services are delivered as an IaaS, remote Windows desktop. Each service has gaming optimized streaming clients that gamers install on their local computer, tablet, or mobile device. These streaming clients are similar to RDP but use protocols selected by the respective service provider. The IaaS model gaming services present more risk, require more decision-making, and offer more opportunity for mitigating actions by the gamer.

2. Research Method

Three IaaS cloud gaming services were selected for review: Blade's Shadow, Paperspace's CORE, and a marriage of the Parsec client running on Microsoft's Azure. Blade and Paperspace offer very similar products. They both provide a streaming client to install on a device and a single-step process to set up and provision a Windows virtual machine in their respective data centers. Parsec only authors the streaming client and leaves the gamer to decide which cloud virtual machine to use.

At Blade, the Shadow Boost product advertises four cores up to 3.4Ghz, 12GB of RAM, 256GB of SSD storage and, an Nvidia GTX 1080 (actually a Quadro P5000). Blade shows two additional configurations of their Shadow product, but they are currently not available for purchase. The provisioned cloud gaming virtual machine runs Windows 10 Home.

A Paperspace, the CORE product, advertises four cores up to 2.8Ghz, 8GB of RAM, 50GB of SSD storage and, an Nvidia GRID K120Q. Paperspace allows for adjustment from these base specifications with three alternative packages as well as independently upgrading storage. Paperspace also installs a customized version of Windows Server 2019 Datacenter edition, the operating system on this cloud gaming virtual machine.

With Parsec, gamers can follow a guide and a script developed by Parsec to deploy the cloud gaming virtual machine. If gamers choose to use Microsoft Azure to host their virtual machine, they must use the NV6 instance type, as it is only one supported by Parsec ("Required dependencies to set up your own cloud gaming PC without parsec templates," n.d.). The Microsoft Azure NV6 cloud virtual machine is Microsoft's graphics-accelerated offering with dedicated GPU resources. The Azure NV6 cloud virtual machine has the following standard specifications: six vCPUs, 56GB of RAM, 128GB of persistent SSD storage and, an Nvidia Tesla M60. Unlike the Blade or Paperspace cloud gaming virtual machines, the Microsoft Azure NV6 also has 320GB of temporary space, which has limited usefulness to gamers. Gamers may attach additional persistent storage or migrate to higher spec cloud virtual machines. While gamers can choose from any operating system offered by Microsoft Azure, Windows 2016 is recommended in the Parsec guide.

In order to strictly comply with acceptable use policies, only the observations of the presence of Blade, Paperspace, or Parsec-authored applications installed on their respective cloud gaming virtual machines were recorded. The exact function that these applications performed was not derived. No reverse engineering, disassembly, or memory inspection was performed. Once set up, third-party software or scripts were not brought to the cloud gaming virtual machines; only built-in Windows applications and utilities were used to make observations. Also, no additional Windows features or roles were installed. The tools used to collect information are common and well-known applications typically used by individuals trying to troubleshoot Windows.

For each of the cloud gaming services researched, a review of the service policies and account security was performed. A thorough analysis of these published policies

often reveals concerning elements ("Dangerous terms: A user's guide to EULAs," 2018). Furthermore, the average consumer rarely reads these policies, much like the quickly dismissed end user license agreements (Böhme & Köpsell, 2010). In addition to the review of the policies, the implementation of account security controls was analyzed.

3. Findings and Discussion

3.1. Service Policies and Account Security

All software users are regularly bombarded with use and access policies that they rarely read before accepting (Böhme & Köpsell, 2010). These policies and agreements are present in every application on a computer, including the operating system itself. These cloud gaming services are no different; the cloud gaming service providers are also geared to insulate themselves from litigation and limit their responsibilities.

The published policies from Blade, Paperspace, Parsec, and Microsoft's Azure policy were reviewed. While each service contains similar language and expectations, each one has critical terms that gamers should review and understand.

3.1.1. Blade Shadow

Blade currently has three links at the bottom of the main Shadow web page titled, "Terms of Use," "Privacy Policy," and "Terms of Service." Their Frequently Asked Questions (FAQ) also contains information that is sometimes in direct conflict with their other documents.

The Terms of Use contains the bulk of the essential information. The first section in this document is titled "User names and personal passwords" ("Terms of use," n.d.). Instead of discussing password requirements or security measures, this section is only about the expectation that a single gamer will use this account. Additionally, it also states that if a user shares the account password, they are still responsible for their account since Blade has disallowed this practice.

The Code of Conduct section immediately follows and touches on some, perhaps obvious, but necessary statements. There is an extensive list of prohibited activities,

including hacking, probing, crypto mining, or using Blade's "computing power to break encryption keys" ("Terms of use," n.d.). Blade Shadow is sold as a service for primarily playing video games and limited other activities. The billing method for Blade's Shadow is a flat fee, so they are interested in minimizing gamers' consumption to keep costs low. Blade also institutes an idle detection mechanism to force shutdown on their cloud gaming virtual machines that don't appear to be in use. Circumventing this idle detection mechanism is a breach of the code of conduct.

In the following section, titled "User Data," Blade clarifies that "The User is responsible for taking all necessary measures to back up and protect his or her Data, in particular against viruses circulating on the Internet" ("Terms of use," n.d.). They go on to also notify gamers that "Blade may remove User Data from the Services" ("Terms of use," n.d.). There should not be an expectation of data privacy on a user's cloud gaming virtual machine from Blade.

Regarding the Privacy Policy, it shouldn't come as a surprise that a large amount of personal data is collected from many services. Blade's Shadow is no exception. Gamers should expect Blade to retain personal details when provided to them at sign up, such as payment information, contact information, etc. What gamers may be less aware of is Blade's aggregation of supplied data, observed both in the VM and the computer/device they are connecting from, as well as "messages on social networks or forums" ("Privacy policy," n.d.). It cannot be derived from a policy review of what mechanisms they have to correlate gamer's satisfaction, reviews, or other social media comments. However, gamers certainly provide all the necessary personal information at signup to make this trivial.

In the "Purpose of processing of data" section, it is explicitly stated that Blade may be "following the navigation of the User" to improve and optimize the service ("Privacy policy," n.d.). Consider that this recording of user navigation may be automated and stored. Gamers should be careful not to presume that they have privacy while chatting with friends, reading emails, browsing sensitive personal websites, or opening a password manager to reveal a password. It is not made clear under what conditions navigation will be followed, reviewed, or audited. If navigation is recorded, it is unclear

how those recordings are kept private from accidental or purposeful dissemination. Finally, the “Terms of Service” is a concise paragraph about the use of the website and contains very little information other than contact information ("Shadow - Legal," n.d.).

The FAQ provides a more definite statement about Blade’s role in securing the cloud gaming virtual machine. It states, “With Shadow, you are the security and anti-virus handler, exactly as you would be on a regular PC” ("Shadow - FAQ," n.d.). Blade’s Shadow support articles recommend, “To prevent potential issues, do not install a third-party antivirus or firewall on Shadow” ("Using an antivirus or firewall with shadow," n.d.). In another support article, “When using Shadow, we recommend temporarily disabling your antivirus.” ("Using an antivirus or firewall with shadow," n.d.). Blade has assigned the responsibility of security to the gamer only to then recommend against running anti-virus software.

Gamers will use the same password for the Blade Shadow website and the streaming application to connect to the cloud gaming virtual machine. There is no option to enroll in any form of multi-factor authentication (MFA). The first time the user logs into the Blade Shadow application, a six-digit numeric code is sent to their email address, which needs to be entered into the app. This challenge is presented only once per unique device. The list of previously connected or actively connected devices is not available to the gamer anywhere on the Blade website or Shadow application. There is no password age or complexity requirement stated in the policies, FAQs, or support articles. While the information on changing one’s password can be found in the website’s account section, a gamer can click a question mark for tips on picking a password, and there is a password security meter. The only actual requirement is that the password is at least eight characters (See Figure 1). Gamers can change their password to “password,” despite the error message saying it was not complex enough. The password was accepted and worked for both the website and streaming application. Blade does not generate a notification email when the password is changed.

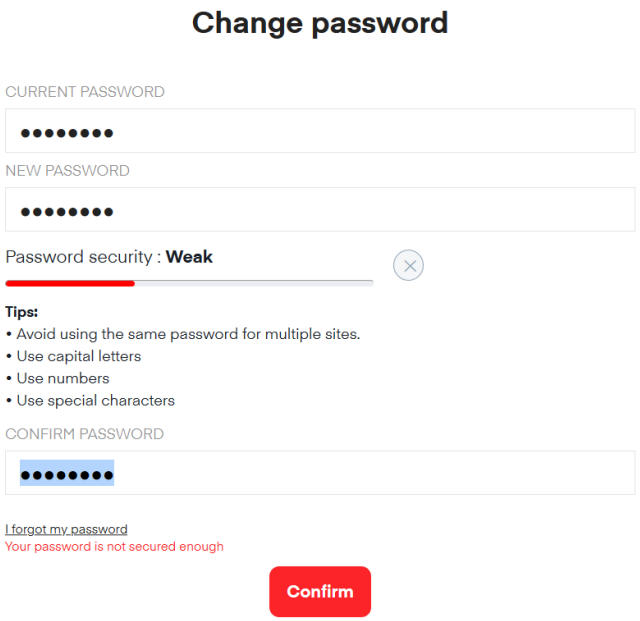

Figure 1. Blade Shadow Password Change Dialog

3.1.2. Paperspace

Paperspace's Privacy Policy, Acceptable Use Policy, and Terms of Service are not prominently linked on their main web page. Links to this information must be requested via Support. A gamer's data may exist anywhere Paperspace or its third-party affiliates, process, or store data ("Paperspace - Privacy policy," n.d.). Paperspace's privacy policy has an opt-out section containing suggestions about adjusting browser settings to stop trackers and cookies to minimize personal data collection and storage ("Paperspace - Privacy policy," n.d.). Additionally, the length of time that a user's data will be stored is indeterminate, even if they stop using the service and close their account.

Paperspace offers cloud virtual machines for other workloads, so the language used in their Acceptable Use Policy is not explicitly directed at gamers ("Acceptable use policy," n.d.). They also utilize a consumption billing method, whereas the more hours a gamer uses, the more the gamer is billed. Therefore, minimizing the gamer's use isn't in Paperspace's best interest.

Paperspace has an extensive Terms of Service and begins with a clear position on accessing of customer systems:

> Paperspace does not and will not access or use Customer Content except as necessary to maintain or provide the Services, or as may be necessary to comply with the law or a binding order of a governmental body." ("Paperspace - Terms of service," n.d.)

Paperspace goes on to say that the gamer is responsible for the security of their content and should make use of the systems provided by Paperspace, including multifactor authentication, protecting and rotating passwords, encryption technologies and encrypting backing up their content ("Paperspace - Terms of service," n.d.).

There is a single account for both the website and the streaming application. Paperspace offers MFA using Time-based One Time Password (TOTP) via an authenticator application of the gamer's choice. They do not provide Short Message Service (SMS) text or create printable codes for backup. Without backup codes, losing the primary MFA device would make disabling MFA impossible without administrative help.

Enrolling in MFA requires the gamer's password twice, first to generate the barcode and again when providing the first token. The gamer is required to enter their password to disable MFA. The process of disabling MFA could be improved by requiring an MFA token during the disabling step. Disabling MFA usually happens when an individual loses control or possession of their primary MFA device. Another improvement would be to include notifications for enrolling in MFA or disabling it.

More critically, the password requirements are even less strict then Blade's. While Paperspace "…*recommend[s]* 8 characters or more", they only *require* six characters (See Figure 2). There is some complexity required, but the rules could not be located. The input validation looked for more than just two complexity factors from the standard list: uppercase characters, lowercase characters, numbers, and symbols. A series of numbers or letters resulted in an error "This password is likely compromised. Please choose another." (See Figure 3). I could not use '123123', or 'aaaaaa,' but 'aaSaaa' was accepted, which is a terribly short password. Changing the password does not generate a notification email.

Paperspace also has integrations with Google and Github for Single Sign On (SSO). Gamers that choose to go this route, can also leverage the additional MFA

features of those accounts. These third-party identity providers come with their additional risk exposure that gamers should consider before using. Namely, the Google MFA solution is also flawed in the same manner as Paperspace, in that it does not require an MFA token to be disabled and does not send a notification for the action of disabling MFA ("Beware the Google password manager," 2020).

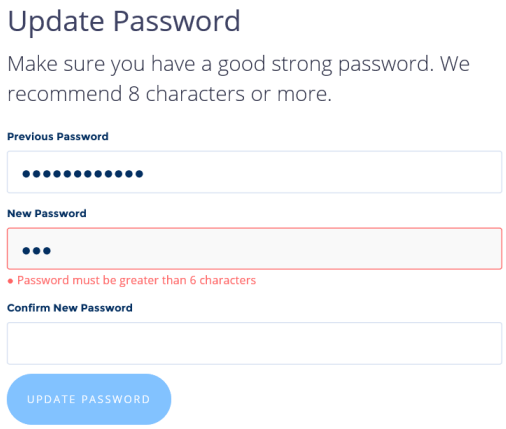

Figure 2. Paperspace Update Password

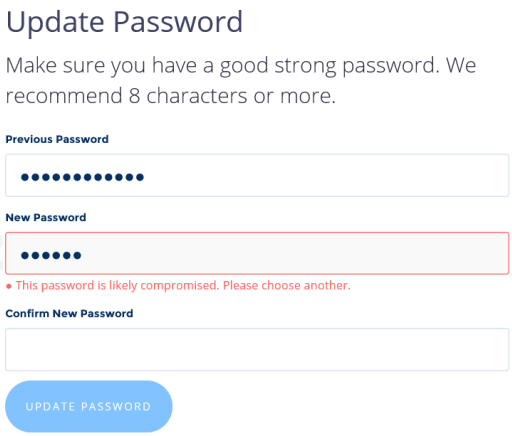

Figure 3. Paperspace Update Password

3.1.3. Parsec running on Microsoft Azure

Recall that Parsec can run on top of many different cloud virtual machine providers. Therefore, gamers should also review the available and relevant policies of the provider they are considering. Parsec's language is clear and leaves little to interpretation. The Terms of Service is extensive and outlines that the gamer is: responsible for account confidentiality, provided no support, and subject to typical acceptable use expectations ("Terms of service," n.d.). It continues, "You are responsible for the User Content you make available…and are responsible for determining the appropriate access settings…." ("Terms of service," n.d.). Furthermore, Parsec states that they are not responsible for monitoring the gamer's content, nor will they monitor a gamer's cloud gaming virtual machine.

Parsec's Privacy Policy is written with easily understood language. They are upfront with what they collect and how they collect it. They specifically request that "We ask that you *not* provide us with any sensitive personal information" ("Privacy policy," n.d.). Also, they have a provision for updating, deleting, and erasing personal data, and

they provide a specific guide on opting out of their website trackers ("Privacy policy," n.d.).

Microsoft's Azure unabridged policy library covers an enormous range of products that quickly diverge from this review's scope. There are certain parts worth highlighting. The Microsoft Azure virtual machine password requirements are published clearly. These requirements are also the strongest ones out of those reviewed ("FAQ about Windows VMs in Azure - Azure Windows virtual machines," n.d.). They publish a shortlist of specific complex passwords that are still not allowed while they meet complexity requirements, are still not allowed, as they are all too common.

Additionally, Microsoft recommends using antivirus software, whether gamers use Microsoft's Windows Defender or a third-party. They also offer optional features, including a hardware security module, disk encryption, and a paid backup service. None of these are options with the other providers.

It is cumbersome to manage the additional accounts in this implementation. Users will have a Parsec account, a Microsoft Azure account, and a Windows account. The Parsec script will, for better or worse, offer to set up the Windows account to automatically log on when the cloud gaming virtual machine is started. With this option, the gamer will only regularly have to interact with the Parsec account information. Parsec does have MFA support using TOTP tokens. A password is required to generate the code, but not to accept the first code. Backup codes are generated, which may be printed for potential future use if one loses their authenticator. A gamer's password must be entered to remove MFA, but no MFA token is required. There is no email notification for enabling or disabling MFA.

A tooltip for Parsec explains that gamers will need to use seven characters or more; the string '1234567' was not complex enough. Four unlabeled bars light up to indicate the password's security level, but this is unintuitive (See Figure 4). A string of fourteen numbers was sufficient, as long as it wasn't a single number. Also accepted was a password made up of eight lowercase letters or seven characters with at least one uppercase, one lowercase, and one digit. Changing the password does not generate a notification email. Logging into the Parsec client on a new device will produce a

verification email, which provides a link to confirm that a user allows enrollment of this new device.

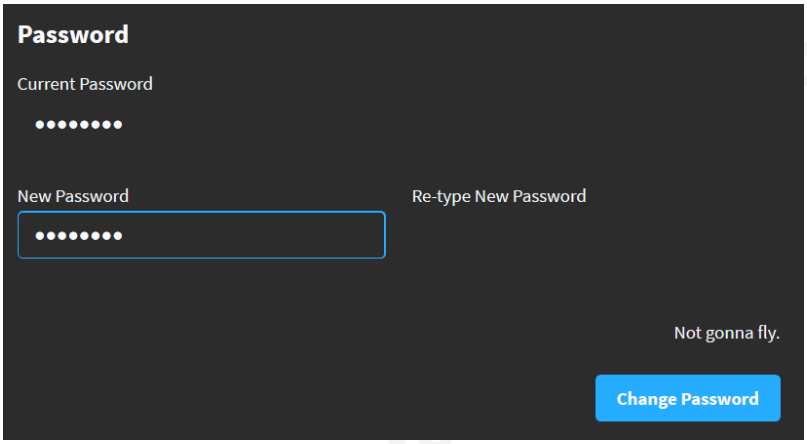

Figure 4. Parsec Account Settings

3.2. Windows Settings and Configuration

3.2.1. Network Configuration

Blade's Shadow virtual machine is behind a firewall using Port Address Translation (PAT). PAT allows for many computers to access the Internet using only a few public IP addresses by sharing them between the computers behind the firewall. This network configuration is very typical for organizations large and small, as well as home users. Blade's customers do not have access to the firewall device to review or adjust settings associated with the gamer's assigned cloud gaming virtual machine. A gamer might desire to change firewall settings if they wanted to host a game server for friends or to audit which ports may be exposed to the Internet. The fewer network ports open to the Internet, the better, because these open network ports offer an attack vector.

Blade's Shadow virtual machine starts with a dynamically assigned private IP address and a 24-bit subnet mask. A 24-bit subnet mask means that the gamer's virtual machine may share a subnet with other gamer's virtual machines, potentially 252. Although Blade may have multiple virtual machines in a subnet, it does not mean that they must. If Blade instead configured the network mask to use 30-bits, this configuration would only allow two hosts. Using a 30-bit subnet mask would indicate that there could be only one other host besides the Blade Shadow virtual machine, and it would likely be

a router or firewall device. Windows Network Discovery and File and Printer sharing are turned off by default, so turning it on will likely produce no results since other gamers would have to do the same.

Blade's Shadow has assigned Google's publicly available DNS server. Using Google's DNS server indicates that Blade is not controlling the resolution of hostnames. Additionally, there were no entries in the Windows hosts file, which is another place to manage hostname resolution. Blade could still collect DNS traffic to build a marketable database attributed to individual gamers or as a collective group. Placing their DNS server in line would provide a much easier method of collecting data versus capturing all network data and filtering it for DNS traffic.

Comparing the list of certificates installed in the Blade Shadow virtual machine to a fresh install of Windows reveals no additional certificates added. If Blade was interested in monitoring the SSL traffic on their network, they might use SSL decryption. For SSL decryption to work with minimal impact to the end-user, a certificate needs to be installed in the Windows certificate store. If not, a gamer browsing a website using https would receive constant warnings about the site's validity.

Paperspace, like Blade, also uses PAT behind a firewall. The Paperspace CORE virtual machine is dynamically assigned a private IP address with a 16-bit subnet mask. Gamers don't have direct access to the firewall interface. This subnet is large, and like Blade's Shadow network configuration, it does not indicate that there must be other customers virtual machines sharing the subnet space. The primary Cloudflare DNS server is configured, taking Paperspace out of the loop of easy DNS data collection. The hosts file is empty, and Paperspace has not installed any additional certificates in Windows. Finally, the Paperspace CORE virtual machine has Network Discovery, and File and Printer Sharing are turned off by default.

Viewed through the Parsec client, the Microsoft Azure cloud gaming virtual machine will look very similar to Blade's and Paperspace's implementations. The Azure virtual machine has a private IP address with a 24-bit subnet mask, no entries in the hosts file, and no additional certificates added to the Windows certificate store. The Windows Network Discovery and File and Printer Sharing are disabled.

The Microsoft Azure virtual machine uses a Microsoft Azure DNS server. Microsoft states clearly in their privacy policy that they collect data from their users employing various technologies to do so. This data may be used to advertise to users ("Microsoft privacy statement – Microsoft privacy," n.d.). Gamers can change this DNS server address to a free public DNS server of their choice and opt-out of Microsoft's advertising.

Where this cloud gaming virtual machine is significantly different is its access to the firewall. During the initial set up of the Microsoft Azure virtual machine, the Parsec-provided guide does not cover the topic of configuring the Microsoft Azure network security controls except to mention on a step labeled "Optional" that you could delete the Azure network firewall rule ("Required dependencies to set up your own cloud gaming PC without parsec templates," n.d.). The gamer is responsible for setting up all IaaS components of the Azure virtual machine in the Parsec implementation.

There is a critical step during the Microsoft Azure virtual machine's initial provisioning, where the default configuration opens port 3389 to the Internet. This port's purpose is to allow the gamer to access the virtual machine via RDP for subsequent configuration steps. Opening RDP to the Internet is very dangerous, which is compounded by using the default port. The Microsoft Azure tooltip tries to draw attention to this configuration issue and suggests using advanced controls, which can be seen (See Figure 5). This tooltip is perhaps a suitable warning when presented to a cloud administrator who understands the implications.

RDP is a commonly attacked service that can invite virtual machine compromise via vulnerabilities in the service or brute force password guessing ("4 ransomware trends to watch in 2019," 2019). Ideally, this network configuration should be significantly narrowed to just the IP address that the gamer is currently using. Once the initial virtual machine provisioning is complete, including all of the Parsec guide steps, the gamer should delete the Azure network firewall rule. Gamers can always return to the Microsoft Azure control panel to enable RDP access in the future if required.

Since gamers have full visibility into the networking provided to Microsoft Azure virtual machine, the gamer can see that the Microsoft Azure virtual machine has a public

IP address assigned to it. The gamer may reserve this IP address between shutdowns for a fee. This additional control also allows a gamer to open specific network ports to host a game server and invite friends to connect.

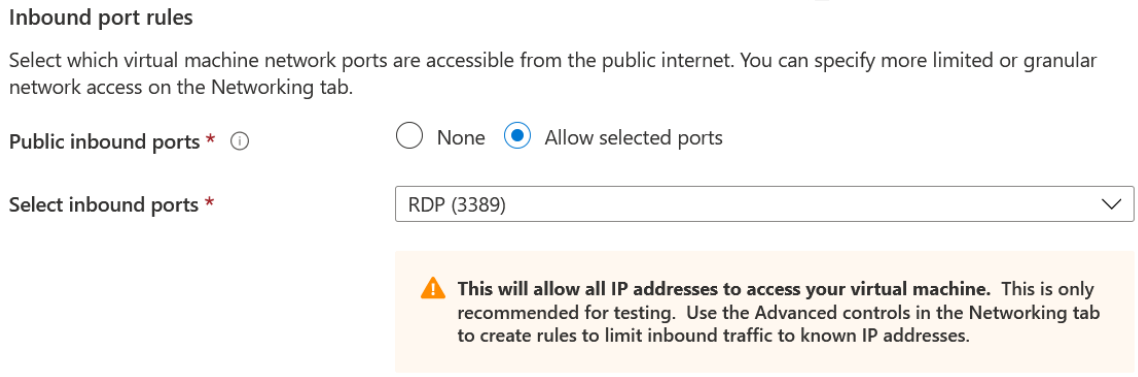

Figure 5. Microsoft Azure virtual machine provisioning

3.2.2. Windows Services

Blade has the highest number of non-default Windows services of any cloud gaming services reviewed, with nine Blade authored services plus the TightVNC Server and Eltima USB Network Gate services. All of the Blade Shadow services are innocuously named, such as 'ShadowStreamer' and 'ShadowController.' The TightVNC service is not started on boot; it must be manually started. TightVNC is a screen sharing application that allows for remote viewing and control. It has both a server application and a client application. The server component is installed, and it allows remote access to the virtual machine when the service is running. The presence of TightVNC isn't immediately apparent. This installation of TightVNC could have been mistakenly left behind and accidentally captured in the operating system image.

Conversely, Blade may still leverage TightVNC for monitoring or interactive troubleshooting. The Eltima USB Network Gate is software for forwarding USB devices from the gamer's local computer to the Blade Shadow cloud gaming virtual machine. It is for the use of gaming peripherals like flight sticks or steering wheels.

Paperspace, because it is running Windows 2019 Server, has a different variety of services compared to Windows 10 Home. Paperspace has the Eltima USB Network Gate

service in common with Blade. Also present are Citrix and XenServer services. These services are an indication that Paperspace is using Citrix on their hypervisor hosts. The Citrix hypervisor hosts are the servers Paperspace is using to provide the CORE cloud gaming virtual machines. Gamers should be aware that these servers are an attack surface, as it is with all three reviewed cloud gaming services. Gamers will need to rely on cloud gaming service companies to keep these underlying systems secure; it is part of the shared security model.

Knowing the cloud gaming service's underlying architecture allows the gamer to react to news of a vulnerability or breach. If the gamer knows that their cloud gaming virtual machine sits on top of XenServer and a vulnerability is announced, they can choose to react. The gamer can contact support and ask when patches or mitigations will be in place. Depending on the specific vulnerability, there may not be mitigations that can be performed on the cloud gaming virtual machine.

Paperspace has a single self-named service running. Also, there is a service named salt_minion present and running. Salt is an infrastructure automation and orchestration tool (*SaltStack*, 2020). This salt_minion service is client software for the endpoint to be managed, rather than the server software used for managing endpoints. Salt may be left over from the virtual machine's initial configuration, or Paperspace may continue to use Salt to take future actions on the virtual machine. Finally, Paperspace also leverages a Razer Surround Audio service to provide audio to the streaming client.

Parsec has the lightest load of extra services. On the Microsoft Azure virtual machine, the Hyper-V integration services are enabled and running, whereas these services were disabled with the other two provider's virtual machines. In this instance, because Microsoft Azure was selected as the cloud virtual machine service provider, there is no question of what technology is hosting the virtual machine. Based on observations, there are two nonstandard services running named Parsec and 'RzSurroundVADStreamingService.' The second service is the same Razer audio service seen in Paperspace but with a less human-friendly name. This service is used to bring audio to the streaming client.

3.2.3. Scheduled Tasks

Compared to stock installations of their respective Windows versions, all three cloud gaming service providers maintained the default Windows Scheduled Tasks. Maintaining the Windows Defender and Windows Update tasks in place provides security benefits by keeping the system patched and the Defender signatures current. These security tasks could have been easily disabled in favor of streamlining the virtual machines for gaming performance or deconflicting software issues with the providers' streaming services.

The Blade Shadow virtual machine has a single custom scheduled task named "Paranoid – SafetyNet." It is triggered on startup and runs a Powershell script named "paranoid-script.ps1". This script's path was in the ShadowInstaller folder but was not present when scheduled tasks were analyzed. The Blade Shadow virtual machine was rebuilt to observe the script, but it must purge itself after running.

The Paperspace CORE virtual machine has standard Google Chrome tasks. These are the typical tasks added when Google Chrome is installed. The Chrome browser was installed as part of the default virtual machine image provisioned by Paperspace. Paperspace also has an eponymous startup task called "PaperspaceTask." It runs an executable named PSTaskAction.exe. By using an executable, Paperspace is obfuscating the actual activities that are occurring.

Parsec doesn't add any non-default scheduled tasks to the Microsoft Azure virtual machine. An optional step of the Parsec script will install Google Chrome and Nvidia drivers. If the gamer opts to perform this optional step, then scheduled tasks for Google Chrome and Nvidia will be present on the Microsoft Azure virtual machine.

3.2.4. Windows Policies

Blade's Shadow virtual machine runs on Windows 10 Home and, therefore, cannot be joined to an Active Direction domain to receive group policies. This ability to deploy and update wide-reaching group policies is a common way that Windows endpoints are managed by systems administrators. Blade's choice of using Windows 10 Home means that they cannot use this method to modify gamer's cloud gaming virtual

machines. There are three additions to the local security policy compared to a fresh install of Windows 10 Home (See Appendix A). First, the timeout for idle network sessions has been set to 15 minutes. This setting was designed to reduce resource utilization on unused network sessions. Second, the access to use the SET command in the Recovery Console is disabled. The SET command allows setting environment variables to permit access to system drives and removable media while using the Recovery Console. Last, the automatic administrator login has been disabled from the recovery console. This setting affects whether the Windows operating system will prompt for an administrator password when booted into the Recovery Console.

When configuring policies in a Windows environment, there is always a default setting that reflects the policy's state when Microsoft first created it. If an administrator makes no changes to a given policy, the policy is in this default state called "not configured", either enabled or disabled, depending on the policy. The last two settings are also the default setting when not configured. Blade may have set them explicitly to ensure the disabled value rather than “not configured.” It’s unlikely that a gamer subscribed to Blade’s Shadow cloud gaming service would ever access this menu because the Blade Shadow streaming services would not be running in the Recovery Console.

Paperspace also had three items configured in the computer policy on their CORE virtual machine (See Appendix A). The first two settings are for suppressing the shutdown reasons dialog. Since this is a server version of Windows, gamers may not be familiar with that dialog box, and disabling these policies is likely a quality of life change. The last policy change ensures that Microsoft installer package files would be permitted to run. This policy may be set to minimize issues with Paperspace’s software installs, perhaps via Salt.

Also, in the local security policy, adding a Microsoft account to Windows is disabled. This prevents syncing Windows settings and preferences, using the Windows Store, and some features of OneDrive.

The Microsoft Azure virtual machine running Parsec had only one group policy adjusted under computer configuration. The shutdown scripts section has a script named ‘NetworkRestore.ps1’. This policy gets configured by the Razer audio software installer,

which Parsec includes in their setup script. The local security policy was identical to a fresh Windows 2016 Server Datacenter install.

3.2.5. Windows Logon

The Windows account credentials in each of these cloud gaming services are separate from the streaming providers' website and streaming application login credentials. For Blade's Shadow, by default, logging in to the streaming application and connecting to the virtual machine automatically logs the user into the Windows desktop. The username utilized is 'Shadow,' and the password is blank, no characters. Gamers may configure a password, after the initial log in, as an additional layer of security. If they choose to set a password, they will be prompted to log in to Windows after connecting to the cloud gaming virtual machine through the Blade Shadow streaming application.

Paperspace automatically logs into the Windows virtual machine and presents a desktop to the gamer after authenticating the gamer in the Paperspace streaming client. This user is named 'paperspace' and has a long, complex password preconfigured. Based on the observed presence of the registry keys used by the Local Security Authority (LSA), Paperspace is leveraging LSA secrets to store login credentials for automatic Windows login ("Credentials processes in Windows authentication," n.d.). Credentials stored in the LSA secrets are easily obtainable with free tools. Anyone with physical or remote interactive access could access these credentials.

Lastly, using Parsec with Microsoft Azure allows users complete control of their cloud gaming virtual machine. During the initial setup process, gamers are required to enter an initial administrator account name and password. Gamers can also create, add, and modify Windows accounts and passwords in the Microsoft Azure portal. The portal is helpful should a gamer forget their Windows username or password. By following the guide from Parsec, users can use the instructions to make a second Windows account. During execution, the Parsec script prompts the gamer with the choice to store the Windows username and password. If the Windows credentials are stored, the Windows desktop will be displayed after logging into the Parsec streaming application without

entering a second set of credentials. Reviewing the Parsec script reveals that the author leverages the LSA secrets store (See Appendix B).

3.3. Windows Security Software and Settings

3.3.1. Defender

Windows Defender is enabled and up to date on all three cloud gaming service providers. All Windows Defender features, including the Real-time Protection, Cloud-delivered Protection, and Automatic Sample Submission, are enabled. There were no exclusions, even of the service providers' third-party applications and folders.

3.3.2. Firewall

The Windows Firewall is enabled and running on all reviewed cloud gaming virtual machines. All three providers had default firewall logging settings, implicitly deny inbound, and implicitly allow outbound rules.

Blade's non-default inbound firewall rules are mostly three duplicated rules for 'ShadowController,' and 'VNC TCP rule.' There are eleven copies of each of these three rules. The duplicate rules are redundant and could be reduced to just three: one copy of each rule. The 'VNC TCP rule' is for the TightVNC server discovered in Section 3.2.2. There is a single rule named 'Crashpad Uploader,' which specifies a path to an executable inside a 'Blade Group' folder in Program Files.

Further analysis reveals that this executable is for uploading crash dump files to a developer feedback SaaS company called Sentry.io. There was also an inbound rule for Eltima, the USB peripheral forwarding service discussed in section 3.2.2. This is an expected addition to the firewall since the default firewall rule in Windows is to deny inbound connections.

Paperspace only had four non-default rules for their streaming software, and instead of specifying addresses and ports, they allowed all communication inbound to their streaming executables. Parsec defined a single non-default inbound rule, and they allowed any IP address and any port but specified their streaming executable.

3.4. Third-Party Software

3.4.1. Blade

Blade has a collection of self-authored software on their virtual machine, likely focused on management and monitoring. The main concern is with TightVNC. TightVNC may be helpful to receive support from Blade, but because this isn't explicitly mentioned in the policies or FAQs, we can't know that is the purpose for TightVNC's presence.

Furthermore, the password set TightVNC is stored in the Windows Registry. This password is easily decoded, with easy to find, free tools. The encoded registry value for this password is the same each time the virtual machine is reset. Another gamer using Blade's Shadow was polled, and the gamer's registry value was the same. Potentially, this password is statically set across all of Blade's Shadow virtual machines. An attacker knowing that there is a static password for VNC software across the whole Blade infrastructure would have at their disposal another remote access tool that is expected in the environment. VNC traffic would likely be allowed by network firewalls and would not be considered anomalous to network intrusion detection systems.

There is also an artifact in the Windows environment variables for Chocolately, a package management software, but the path displayed is no longer on the disk. Because Chocolately is used to install or uninstall software, its existence is concerning. The presence of the 'Red Hat VirtIO Ethernet Adapter,' 'QEMU QEMU HARDDISK SCSI Disk Device,' and 'Red Hat VirtIO SCSI pass through controller' devices in Windows Device Manager indicates that Blade Shadow virtual machines run on top of the Kernel-based Virtual Machine (KVM) hypervisor.

Recall that there was a firewall exception for Crash Uploader in section 3.3.2. A Powershell script named 'safetynet.ps1' has an API key stored in it for Sentry. At first glance, this potential mistake could allow access to what should likely be secured data. After researching the tools Blade uses on the Sentry's site, the concern for data exposure by leveraging these credentials is diminished. Sentry provides instructions for uploading a crash dump that is consumed and then destroyed. Sentry's Application Programming Interface (API) does not allow for retrieval of uploaded crash dumps ("Minidump," n.d.).

Although an attacker may not be able to retrieve the crash dumps from this service, the crash dumps' contents and how their output is handled are of concern. Because Blade writes the software, the crash dump produced could contain anything on the virtual machine, such as files, whole or partial RAM contents, etc.

3.4.2. Paperspace

While Paperspace does perform some customizations to the Windows user interface, it is only cosmetic. Paperspace does leave “Paperspace-Password-Tool” on the root of the main drive that a gamer can use to lookup the current Windows credentials. Gamers can also set a new password for the Windows account with this tool.

3.4.3. Parsec on Microsoft Azure

The Parsec install script does not bring any unnecessary third-party software to the cloud gaming virtual machine. Microsoft builds the install from a stock install of Windows Server. There aren’t artifacts of deployment, package management, or monitoring tools.

4. Recommendations

4.1. Service Policies and Account Security

A service provider with clear language and few exceptions in their policies is an excellent start in a gamer's search for the most secure cloud gaming choice. It is a tedious exercise to review these terms before using a new service, but it a buyer beware situation.

Gamers should demand that cloud gaming services provide MFA for any account they hold and avoid SMS because it is widely considered an insecure method of receiving a token. The best MFA solutions will include a requirement to provide a token to disable MFA.

While it is in both parties’ best interest to have long, complex passwords to ensure account security, we have not reached a point where we can rely on service providers to enforce it. Mandating secure passwords is likely seen as a speed bump on the path to setting up a new account and earning a paying customer, so the loose requirements continue. Gamers should take it upon themselves to use a unique complex password for

each account they have. Also, gamers should make use of a password manager to assist in maintaining passwords.

It may be that Paperspace's maturity in the cloud virtual machine market has prepared them well for delivering cloud gaming virtual machines. Paperspace's policies are respectful and fair. They encourage backup, encryption, and adequate password security.

4.2. Windows Settings and Configuration

Gamers should set a Windows account password and consider changing the username, regardless of which cloud gaming service is selected. Every Blade Shadow and Paperspace CORE virtual machine initially has the same username, respectively. Blade's Shadow starts with no password; if an attacker could bridge the private network used by a virtual machine, having an eponymous username without a password provides zero resistance to lateral movement.

4.3. Windows Security Software

Windows Defender is a viable anti-virus and provides basic coverage. Defender is undoubtedly a world of difference from having no antivirus software. If gamers are the responsible party, then advice to disable security software should not be accepted. Furthermore, Blade's Windows firewall settings are sloppy and could stand a reduction of the duplicates at a minimum. It is much easier to audit three rules than thirty-three.

Conversely, Paperspace and Parsec had narrowly tailored firewall rules for their streaming and third-party applications. Particular attention should be paid to how the firewall in the virtual environment selected is configured for Parsec users. The Microsoft Azure default network firewall configuration, which allows RDP connections from anywhere on the Internet, is exceptionally unsafe and, the default setting should never be accepted.

Controlled Folder Access (CFA) is not enabled on any virtual machines reviewed and would provide additional protection from ransomware. CFA is available on Blade's Shadow and Paperspace's CORE virtual machines. Controlled Folder Access is not available on the Parsec Microsoft Azure virtual machine because it is Windows 2016

Server, where CFA is unsupported ("Prevent ransomware and threats from encrypting and changing files - Windows security," n.d.).

4.4. Third-Party Software

It can't be overstated that a significant impact on the Blade Shadow cloud gaming virtual machine's security is TightVNC. Blade controls the hardware and hypervisor software. If Blade wants access to a gamer's virtual machine, they don't need TightVNC.

If Parsec with Microsoft Azure is selected as the cloud provider, do not accept Microsoft's default RDP settings. During those initial setup steps, gamers should lock down the network firewall rule for RDP to their current IP address. Once they have the Parsec streaming service configured, then disable the RDP networking configuration. If future access is required, the firewall rule can be configured in the Microsoft Azure portal.

5. Conclusion

Selecting a cloud gaming service based on security is not at the forefront of a gamer's mind, in an industry where hardware specs and cost reign supreme. These considerations pale in comparison to the default security posture of some of these services. This cloud virtual machine will have access to a gamer's entire game library, saved games, forwarded keystrokes, web browsing history, and potentially more. Mitigating steps should be viewed through the acceptable use policy and terms of service author's lenses.

The trade-off of a couple of dollars a month is not worth risking a gamer's library, character progress, assets, or access to any private data that finds its way over to the cloud gaming virtual machine. If a gamer is comfortable starting from scratch, they will have the best starting security posture. If gamers want a turn-key solution, be prepared to file down the rough edges while staying inside the bounds of the policies they accept.

References

2019 essential facts about the computer and video game industry. (2019, August 19). Entertainment Software Association. https://www.theesa.com/esa-research/2019-essential-facts-about-the-computer-and-video-game-industry/

Census - Geography Profile. (n.d.). https://data.census.gov/cedsci/profile?q=United+States. Retrieved July 17, 2020, from https://data.census.gov/cedsci/profile?q=United+States

Required dependencies to set up your own cloud gaming PC without parsec templates. (n.d.). Parsec. Retrieved July 17, 2020, from https://support.parsecgaming.com/hc/en-us/articles/115002701631-Required-Dependencies-To-Set-Up-Your-Own-Cloud-Gaming-PC-Without-Parsec-Templates

Dangerous terms: A user's guide to EULAs. (2018, January 18). Electronic Frontier Foundation. https://www.eff.org/wp/dangerous-terms-users-guide-eulas

Böhme, R., & Köpsell, S. (2010). Trained to accept? *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. https://doi.org/10.1145/1753326.1753689

Terms of use. (n.d.). Transform your device Into a Gaming PC!. Retrieved July 17, 2020, from https://shadow.tech/usen/legal/terms

Privacy policy. (n.d.). Transform your device Into a Gaming PC!. Retrieved July 17, 2020, from https://shadow.tech/usen/privacy

Shadow - Legal. (n.d.). Transform your device Into a Gaming PC!. Retrieved July 17, 2020, from https://shadow.tech/usen/legal

Shadow - FAQ. (n.d.). Transform your device Into a Gaming PC!. Retrieved July 17, 2020, from https://shadow.tech/usen/faq/security/what-are-your-guarantees-about-account-hacking

Using an antivirus or firewall with shadow. (n.d.). Shadow - Support (EN). Retrieved July 17, 2020, from https://help.shadow.tech/hc/en-gb/articles/360012648294-Using-an-Antivirus-or-Firewall-with-Shadow

Paperspace - Privacy policy. (n.d.). Paperspace: Cloud Machine Learning, AI, and effortless GPU infrastructure. Retrieved July 17, 2020, from https://www.paperspace.com/privacy-policy

Acceptable use policy. (n.d.). Retrieved July 17, 2020, from https://www.paperspace.com/acceptable-use-policy

Paperspace - Terms of service. (n.d.). Paperspace: Cloud Machine Learning, AI, and effortless GPU infrastructure. Retrieved July 17, 2020, from https://www.paperspace.com/terms-of-service

Beware the Google password manager. (2020, July 2). fasterthanli.me. https://fasterthanli.me/articles/beware-the-google-password-manager

Terms of service. (n.d.). Parsec Gaming. Retrieved July 17, 2020, from https://parsecgaming.com/terms/

Privacy policy. (n.d.). Parsec Gaming. Retrieved July 17, 2020, from https://parsecgaming.com/privacy/

Microsoft privacy statement – Microsoft privacy. (n.d.). Privacy – Microsoft privacy. Retrieved August 18, 2020, from https://privacy.microsoft.com/en-us/privacystatement

Adam Knepprath

FAQ about Windows VMs in Azure - Azure Windows virtual machines. (n.d.). Technical documentation, API, and code examples | Microsoft Docs. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq

4 ransomware trends to watch in 2019. (2019, February 13). Recorded Future. https://www.recordedfuture.com/ransomware-trends-2019/

(2020, August 6). SaltStack. https://www.saltstack.com/

Credentials processes in Windows authentication. (n.d.). Technical documentation, API, and code examples | Microsoft Docs. https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication

Minidump. (n.d.). Sentry Documentation. Retrieved July 17, 2020, from https://docs.sentry.io/platforms/native/minidump/

Prevent ransomware and threats from encrypting and changing files - Windows security. (n.d.). Technical documentation, API, and code examples | Microsoft Docs. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders

Appendix A
List of Added or Modified Windows Policies

Blade	MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\ AutoDisconnect=4,15
	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
	MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
Papersp ace	Software\Policies\Microsoft\Windows NT\Reliability\ShutdownReasonOn
	Software\Policies\Microsoft\Windows NT\Reliability\ShutdownReasonUI
	Software\Policies\Microsoft\Windows\Installer\DisableMSI
	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ NoConnectedUser=4,3

Appendix B
Snippet of PostInstall.ps1 from Parsec

```
function Set-AutoLogon {
    [CmdletBinding(SupportsShouldProcess)]
    param
    (
        [PSCredential]$Credential
    )
    Try {
        if ($Credential.GetNetworkCredential().Domain) {
            $DefaultDomainName = $Credential.GetNetworkCredential().Domain
            }
        elseif ((Get-WMIObject Win32_ComputerSystem).PartOfDomain) {
            $DefaultDomainName = "."
            }
        else {
            $DefaultDomainName = ""
            }

        if ($PSCmdlet.ShouldProcess(('User "{0}\{1}"' -f $DefaultDomainName,
$Credential.GetNetworkCredential().Username), "Set Auto logon")) {
            Write-Verbose ('DomainName: {0} / UserName: {1}' -f
$DefaultDomainName, $Credential.GetNetworkCredential().Username)
            Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' -Name "AutoAdminLogon" -Value 1
            Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' -Name "DefaultDomainName" -Value ""
            Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' -Name "DefaultUserName" -Value
$Credential.UserName
            Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' -Name "AutoLogonCount" -ErrorAction
SilentlyContinue
            Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' -Name "DefaultPassword" -ErrorAction
SilentlyContinue
            $private:LsaUtil = New-Object ComputerSystem.LSAutil -
ArgumentList "DefaultPassword"
            $LsaUtil.SetSecret($Credential.GetNetworkCredential().Password)
            "Auto Logon Configured"
            Remove-Variable Credential
            }
    }
    Catch {
        $Error[0].Exception.Message
        Throw
        }
}
```

https://github.com/parsec-cloud/Parsec-Cloud-Preparation-Tool