SentryBay

Zero-Trust protection for Microsoft Azure Virtual Desktop and Windows 365

SentryBay Limited

UK Headquarters
20 Little Britain
London EC1A 7DH
United Kingdom

p: +44 (0) 203 478 1300

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

p: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
p: +1 (650) 242 8796

Contents

SentryBay Limited

UK Headquarters
20 Little Britain
London EC1A 7DH
United Kingdom

p: +44 (0) 203 478 1300

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

p: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
p: +1 (650) 242 8796

Executive Summary

Azure Virtual Desktop is a scalable and secure cloud-based platform that enables remote working from any device. Remote devices pose a challenge for security teams to enforce a baseline level of security and ensure that only secure and compliant devices can connect. Authenticating the user beyond doubt is an important challenge, authenticating an unmanaged device and ensuring a critical layer of security is in place to protect against insider threats and malware is imperative. Utilizing SentryBay's endpoint access isolation solution to control access and neutralize zero-day threats helps businesses meet HIPAA, LGPD, PIPL and GDPR laws and comply with standards such as PCI DSS & FFIEC to protect personally identifiable information (PII) and protected personal information (PPI) data - without infringing end user privacy.

What is Azure Virtual Desktop and Windows 365

Historically large enterprises utilized on-premise infrastructure to power VDI (Virtual Desktop Infrastructure). This attracted exorbitant costs to power, license, deploy, manage, maintain in order to meet legal and compliance requirements. In 2019 Microsoft (MS) announced the launch of Windows Virtual Desktop, which provided a new platform that allowed companies to utilize the flexibility of Azure to power their VDI infrastructure. MS later rebranded it Azure Virtual Desktop (AVD) and this paved the way for Windows 365, which removed almost all the management overhead of running a VDI environment and provided users with a simple cloud pc. These two products revolutionized the cost model for the larger enterprise from a major CAPEX to a more attractive OPEX model. Microsoft removes the need to support low-level datacenter operations - the power, backup power, air conditioning, replacement of hardware (including servers, networking equipment)- and provides a simple mechanism to instantly scale out services, collapse in or even venture to new regions.

Cyber Defense Strategy

Industry leading enterprise security teams take a multi layered strategy to security, this also known as 'defense in depth' and it ultimately means providing multiple, different layers of security, using multiple vendors. For example, a company may deploy the following layers of security:

- XDR (x Detection and Response)
- Proxy services (monitoring inbound and outbound traffic)
- SOC (Security Operations Center)
- Email scanning and stripping
- CASB (Cloud Access Security Broker) for access control
- CIRT team (Cyber Incident Response Team) to respond to breaches, viruses or anything that has slipped through the net.

Taking this approach removes reliance on one vendor or even one type of strategy to protect the companies' digital assets and within the confines of a company's logical network perimeter, this can be enforced to ensure compliance. However, with the distinct cost savings and potential ROI returns of taking a BYOC strategy, how do you protect and enforce compliance on the unmanaged devices that connect into AVD or W365 and what are the threats you need to protect against?

Threats to Azure Virtual Desktop / W365 – The Unmanaged Desktop

The average cost of a breach totals $4.45 million across all sectors*. With unmanaged personal devices not subject to automated security updates or the rigor of threat detection from an XDR and a SOC team (amongst many other controls), - this opens the door to far more threats.

Thankfully, due to the design of VDI, many threats are mitigated. However, malware or insider threats are all able to penetrate native VDI defenses, for example:

SentryBay Limited

UK Headquarters
20 Little Britain
London EC1A 7DH
United Kingdom

p: +44 (0) 203 478 1300

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

p: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
p: +1 (650) 242 8796

Keylogging

One of the oldest components of malware are keyloggers, despite being one of the earliest forms of malware they remain a top threat in security breaches due to their ability to effectively capture every keystroke from an infected device and evade even the most advanced forms of cyber defense. This poses the following risks:

- Credential theft - usernames, passwords, PIN codes, and other login details can be recorded without the user's knowledge.
- Financial Fraud - Keyloggers can be used to obtain credit card numbers, bank account information, and other financial data that users enter via their keyboards while making online transactions.
- State & Corporate Espionage - In a corporate environment, keyloggers can capture sensitive information such as business plans, intellectual property, and insider information that can be sold or used competitively against the organization.

Screen Capturing and Screen Scraping

Screen capturing is a common tool used by insider and malware threats to screenshot or record the screen resulting in data leakage, VDI sessions on unmanaged devices a vulnerable to these types of attack, some examples below of how screen capture can be used:

- Information Theft - Screenshots can capture sensitive information displayed on a user's screen, including personal data, financial information, passwords, business plans, or proprietary software being used. This information can then be used for fraud, identity theft, or sold on the dark web.
- Credential Harvesting - Sometimes, malware aims to capture login credentials that might not be caught by keyloggers, especially if the usernames are filled in using a password manager's auto-fill functionality.
- State and Economic Espionage - Screenshots can provide a wealth of competitive intelligence or reveal operational details that are valuable to corporate or state sponsored spies.
- Contextual Awareness - By taking screenshots, malware can provide context to captured keystrokes, making it easier for attackers to understand the data they've obtained.
- Extortion and Blackmail - Attackers may capture sensitive or personal images on a user's screen to use as leverage for blackmail or extortion schemes which can be damaging to an individual or company's reputation DLL Injection and Insider Sabotage

An insider with technical knowledge could use DLL injection to disrupt VDI operations or to bypass security controls such as disabling screen capture blocking or disrupting the means to block screen capture. This could be a deliberate act of sabotage or part of a larger scheme facilitated by malware to obtain company secrets.

Malicious injection

Malicious injection is a mechanism that malware or malicious users can use to modify how an application functions on the computer; from an unmanaged device this is quite a powerful simple technique.

- Evasion - Malware can inject into legitimate processes, the purpose of this can be to evade detection by typical AV and EDR products.
- Function Hooking - Malware can 'inject' into application to disrupt how applications work. for example, capturing user inputs such as the keys typed on the keyboard or spoken words into the microphone or preventing screen capture controls from being enabled.
- Process Control - Through DLL injection, malware can manipulate applications to switch off features such as screen capture blocking.

Real world examples

Last Pass

- a keylogger was installed on the computer of a senior dev ops engineer which overtime gathered the employee's master password and access to the engineer's LastPass corporate vault
- The bad actor was able to steal source code and then use technical documentation to exfiltrate 14 of approximately 200 source-code repositories.
- In total, the attacker(s) stole:
    - Decryption keys

- Encrypted secure notes
- Critical cloud backups
- Product source code

Unfortunately, because the breach was completed using valid credentials, it was hard to detect and the threat was persistent, and over the course of 2 months, the bad actor was able to continuously exfiltrate data.

The effects are still felt by the last pass user base today where it was reported that $4.4million worth cryptocurrency has been stolen to date (October 2023) from around 24 victims through suspected brute force attacking vaults where master passwords were weak.

Existing Security Solutions

There is a myriad of approaches to tackling security concerns on BYOPC, however where vendors typically fall short is the level of security, compliance, and end user adoption due to privacy concerns. Enforcing protections in a lightweight manner, and not only respecting user privacy but also having a perception of user privacy are all paramount elements to success.

UEM Solutions

UEM solutions such as Microsoft Intune work by enrolling devices into the platform, the advantage of this is it provides the admin with varying levels of control of the end user devices, Admins can ensure that their AV is enabled with real time scanning, enable the firewall or even deploy software on their device.

From the user perspective, when they enroll their device into UEM's such as Intune, they agree to allowing their company to have a certain level of control of their device. Unfortunately, this becomes a privacy issue. The same can be said for a 3rd party contractors – this could be a single individual or a company having another company exert a level of control upon your device - this can cause conflicts and have the potential to even lower the level of security of a device.

All of these points place friction on the adoption of a BYO strategy, or block contractors from obtaining access.

Endpoint Anti-Virus

Traditional antivirus (AV) is classed as a passive solution meaning that it is looking across the system for threats instead of actively blocking threat vectors. Antivirus has been the household standard since its inception in the late 1980's ,]It has been known for many years that the efficacy of these products is not up to standard nor do they deal with zero day threats adequately. Typically, AV has two mechanisms for detecting a threat:

- Signatures. The signature of the malicious file must be previously known, in recent times people like Microsoft have added 'cloud protection' which is a more powerful way to leverage the cloud to detect threats in real time
- Heuristics. This is the analysis of the code and how it behaves, if code is seen to act suspiciously it will be flagged as a threat and dealt with accordingly.

Both mechanisms are predicated on the assumption that:

A) The antivirus is licensed.
B) The antivirus is up to date.
C) The antivirus is configured correctly.
D) The antivirus has identified all the elements of the threat, including persistence components.

The next issue is how to enforce a user to switch on their AV and configure it to be compliant with company policy or run a certain engine. Products such as 'endpoint analysis' or EPA can provide companies with the ability to determine if AV is enabled and up-to-date on the user's endpoint and only allow connections from devices that match compliance policies. However, the technology is hard to master, with enforceability, maintenance and usability questions, and a high total cost of ownership (TCO)

End Point Detection and Response (EDR) on unmanaged devices

The other option is to force all users deploy an EDR to their home device. This provides the admin with alerts and notifications and the possibility to detect and respond to possible threats.

The problem with this is threefold:

- Every website and every app launched is monitored and logged to a SOC, this infringes on privacy.
- It provides a massive number of alerts for an end user environment that is somewhat unique to that user and therefore makes it difficult to interpret the alerts, generating many false positives.

- It raises the question of how to enforce this security without having to use a UEM

Native VDI protections

Then there are VDI vendors native protections. Microsoft AVD and VMware Horizon have the capability to block screen capture by using a built in API in Microsoft Windows available on all Windows 7, 8, 10 and 11 devices, and can be centrally controlled. This is a highly available API however it is vulnerable to multiple attacks detailed below:

- Virtual machine – a user can simply load the remote desktop into a Virtual machine and record the screen from the host, this bypasses any protections put in place.
- Injection – using a readily available injection tool from the web, a user obtains a simple file that effectively turns the native protections off, just like a light switch.

The Armored Client

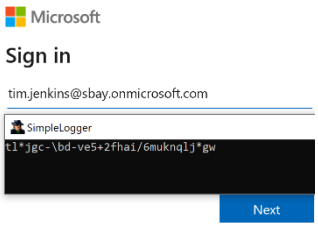
SentryBay's Armored Client is an enterprise grade solution that provides kernel mode anti-keylogging, anti-screen capture and malicious injection protection for Azure Virtual Desktop and Windows 365. This protection nullifies the threats posed by malware and insider threats by assuming that the endpoint is compromised and proactively blocks these threats from harvesting company data. This provides end-to-end zero day threat protection against keylogging, screen capture and injection threats, coupled with an enforcement component that ensures without doubt that every device connecting into the Azure Virtual Desktop or Windows 365 has a critical layer of zero day security running from the kernel mode.

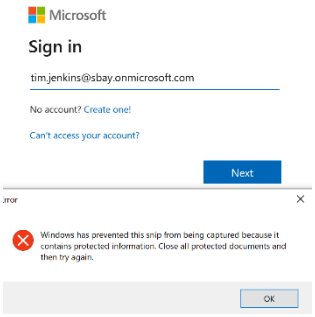
The key features are:

- Advanced Anti Screen Capture – Proprietary advanced screen capture protection
- Anti Keylogging – Kernel mode active protection, built by SentryBay
- Malicious injection Protection – Block malicious injection and manipulation from users or threats
- Virtual Machine Blocking – Block use of virtual machines to prevent security bypass
- Screen Capture Whitelisting – Allow applications to screenshot while protection still in place
- Server-Side Enforcement – Access to AVD/W365 Blocked without SentryBay ACX
- Tamper Protection – Protected application unavailable if security is breached
- RDP Double hop Protection – Block attackers capitalising over an existing RDP session

Anti Keylogging

Armored Client runs at the kernel mode which means that if a keylogger enters the system undetected and begins to harvest keystrokes, the data recorded would be useless, this includes usernames and passwords typed in as well as in session data.





Anti Screen Capture

Advanced anti screen capture protection ensures that all session data is protected whether that is from an insider threat or from malware attempting to steal screen capture data.

Armored Client also provides a simple mechanism in which we can allow optimization tools such as Microsoft teams to share protected and optimized desktops. Similarly, we can allow apps to take screen shots while at the same time blocking all other screen capture threats to be blocked, all at the same time.

Malicious Injection Protection

Armored Client provides zero-day threat from injection attempts on targeted and protected processes ensuring the application integrity is maintained and protections cannot be circumvented.

```
|critical|2023-Nov-03 16:41:07.489426|msrdcw.exe|0x00001e9c|0x00002718|Blocking dll injection!
```


SentryBay Limited

UK Headquarters
20 Little Britain
London EC1A 7DH
United Kingdom

p: +44 (0) 203 478 1300

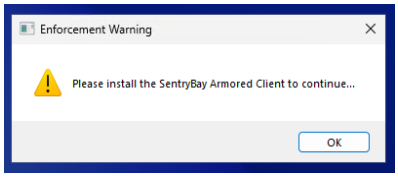
North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

p: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
p: +1 (650) 242 8796

Enforcement and Compliance

All devices accessing protected Azure Virtual Desktops or Windows 365 must have Armored Client installed, without this critical baseline of security users are blocked from logging into the protected asset:



Block Virtual Machine Access.

Armored Client can prevent users circumventing protections by blocking running from a virtual machine, when this is blocked the enforcement capability is invoked ensuring that the unprotected device cannot log into the corporate asset.

```
|service.exe|0x00000bb4|0x000014fc|Checking if running in VM
|service.exe|0x00000bb4|0x000014fc|System firmware RSMB has 'Virtual'
|service.exe|0x00000bb4|0x000014fc|Hypervisor vendor : |VBoxVBoxVBox|86,66,111,120,86,66,111,120,86,66,111,120,0
|service.exe|0x00000bb4|0x000014fc|Notifications turned off : Armored Client is not configured to run on a Virtual Machine
```

Summary

There are natural security gaps in the MS AVD/W365 solution, which are not effectively plugged (particularly on unmanaged devices) by existing security offerings. The Armored Client provides a flexible, application-agnostic and enforceable endpoint access isolation solution. It ensures that all unmanaged and managed devices have a critical layer of security to ensure that zero-day and insider threats are nullified, and pose no threat to the confidentiality or integrity of the company assets – while enabling BYO savings and respecting end user privacy.

*https://securityintelligence.com/posts/healthcare-breach-costs-soar-new-thinking-safeguarding-data/

SentryBay Limited

UK Headquarters
20 Little Britain
London EC1A 7DH
United Kingdom

p: +44 (0) 203 478 1300

North Carolina Office
16900 Ashton Oaks
Charlotte
North Carolina 28278

p: +1 949 394 4902

California Office
1840 Gateway Drive
Suite 200
San Mateo
CA 94404
p: +1 (650) 242 8796