TAG

USING REMOTE.IT FOR CLOUD MICROSERVICE ACCESS

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG

remote.it

USING REMOTE.IT FOR CLOUD MICROSERVICE ACCESS

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG

Secure, ubiquitous, and convenient access to cloud microservices has emerged as key management and administrative requirement for modern development organizations. IT cybersecurity vendor Remote.it is shown to provide effective support for practitioners looking to solve secure remote access as part of their CI/CD workflow.

INTRODUCTION

Connectivity is now expected for everything, whether it be access to devices in the field or microservices in the cloud and the implication for information technology (IT) and cybersecurity practitioners is significant. Most aspects of existing methods for remote access, for example, require a fundamental rethinking, because corporate perimeters with virtual private network (VPN) or remote desktop protocol (RDP) support are no longer part of the typical enterprise architecture.

Instead, zero-trust based distributed architectures using multiple public cloud and software-as-a-service (SaaS) capabilities have arisen as the new norm. Remote access, like many other IT and security tasks, now requires a more ubiquitous solution, one that can utilize identity-related information to validate reported identities and that can target granular workloads hosted anywhere with network access.

In this note, we explain a transition to build in secure remote access fundamentally at deployment of compute services, rather than configuring and maintaining network segments to supporting such access for IT and security administrators to cloud microsegments from anywhere (a vestige of the transition to work-from-anywhere post-Pandemic). Specifically, we show how the solution from commercial IT and security vendor Remote.it offers a well-conceived platform for hosting and administering such secure access.

OVERVIEW OF CLOUD MICROSEGMENT ACCESS

Enterprise IT and security professionals now have the responsibility to manage and maintain the integrity and security of multi-cloud environments. Such environments typically include the use of microsegmentation to support isolation and separation of hosted workloads and applications and to enforce user and machine access policies that were previously supported by complex enterprise perimeters, which are now typically dissolved from the architecture.

Since multi-cloud infrastructures are increasingly complex, IT and security professionals now need a flexible and ubiquitous means for securely accessing cloud microservices from work, home, and other locations. Unfortunately, many such teams still rely solely on legacy solutions like the remote desktop protocol (RDP) or virtual private networks (VPNs), which can often leave cloud environments vulnerable to cyberattacks, and require significant on-going support to maintain connectivity.

RDP, for example, has significant security limitations that make it an unacceptable solution for IT and security use, especially for critical microsegmented workloads of applications. One drawback is its susceptibility to brute-force exploits, where bad actors guess login credentials. This type of attack can be disastrous, as successful intrusions to the cloud can compromise resources and perhaps lead to lateral movement within the network.

Traditional forms of remote access also typically lack proper control and monitoring capability to ensure a secure environment. Once an administrator gains access to a workload or application through RDP or a VPN, there is often no granular control over what they can do within the cloud environment. This unrestricted access can result in misconfigurations, accidental deletion of critical files, or sessions being hijacked or intercepted.

To address these concerns, more secure mechanisms are needed to remotely access cloud microsegments. These mechanisms should respect best practices for secure modern remote access including support for strong authentication, granular access control, enforcement of least privilege, use of encryption, and more. Specific functional requirements will depend on local policy and the criticality of the microsegments being accessed.

OVERVIEW OF REMOTE.IT

Cybersecurity startup vendor Remote.it provides a comprehensive solution for secure remote access and management of Internet of Things (IoT) devices, servers, and other network-connected systems. Their innovative IT security platform is designed to enable seamless, encrypted connections while prioritizing security and ease of use and deployment for administrators, managers, developers, and other users.

The Remote.it solution is built on patented technology which enables connectivity with code. The software stack enables any service (TCP or UDP) to be registered and owned by a user and securely connected to, regardless of location or network. The process begins with devices initiating communication through Remote.It's infrastructure, which acts as an intermediary, facilitating the connection without compromising cybersecurity.

A key advantage of the Remote.It technical approach is the elimination of the need for static public Internet protocol (IP) addresses, which can be expensive to maintain, and which can also introduce various cyber risks. Further, unlike a VPN the Remote.It solution does not require that private subnet addresses be unique either, eliminating a common challenge when attempting to connect microservices between container clusters set to use default IP address ranges. Instead, the Remote. It platform allows users to assign a user defined name to access the service directly, and since the

Remote.Its connectivity binds to the localhost address of the network stack, no services are scannable, and thus the attack surface is eliminated, and along with it the potential malicious attackers to locate and target devices directly.

All Remote.it connections are protected via strong encryption algorithms, which ensures that data transmitted between devices remains confidential. Remote.it also employs various authentication methods, including username/password combinations, cryptographic keys, or tight integration with existing Single Sign-On (SSO) solutions, thus adding an extra layer of protection against unauthorized access.

It's important to also note that remote.it offers centralized management through its dashboard. Administrators can configure access permissions, monitor connected devices, and revoke access remotely. Such control enhances the security of the network and simplifies device management, especially in large-scale IoT deployments. It also provides versatile support for a wide range of platforms and operating systems.

USING REMOTE.IT TO ACCESS CLOUD MICROSERVICESS

As one might expect, a key use-case for Remote.it in the context of modern multi-cloud infrastructure use involves establishing secure remote access to microservicess hosted in public or private cloud services. As suggested above, Remote.it offers a platform to address this requirement and enables IT and security professionals to securely access microsegmented workloads from anywhere.

A key consideration when managing cloud microservicess is the typically large number of remotely hosted and geographically dispersed resources that must be securely accessed and administered. Remote.It reduces friction when connecting to these cloud devices and services by giving developers control of connectivity regardless of the network or location.

To best understand how this provides benefit for teams trying to manage cloud deployed microservices, it is critical to recognize the best practices guided through use of the Remote.it platform and tools. These various practices and how they relate to use of the Remote.it platform are listed and discussed below.

PRACTICE 1: API INTEGRATION

Users of Remote.It who need secure access to the cloud will often integrate with the REST or GraphQL API. Using this API with account key credentials from Remote.it, cloud security teams can access data about devices and services to monitor location or uptime. They can also access data about events associated with these devices or services for debugging or security reviews. Furthermore, they can set up on-demand connections for users to segmented workloads.

PRACTICE 2: CLOUD IAM REPLACEMENT

Remote.it customers with workloads in Amazon Web Services (AWS) have been able to replace the identity and access management (IAM) function provided by AWS. This function is used for setting of permissions and policies on access to cloud resources and to create accounts. This can be simplified using Remote.it which includes the ability to control user access at the service level, eliminate IP accessibility, protect the network from the Internet discovery and scanning, and onboard and offboard user access to devices based on email address.

PRACTICE 3: JUMP SERVER CONFIGURATION

A jump box is a bridging device or instance used to access some other device, instance, or service in a separate security zone. A common use of Remote.It involves setting up a bridging service where users are not required to open ports or configure port forwarding rules. All resources in the cloud remain on private IP addresses. By not having a public IP address and port, Remote.It removes significant attack surface areas for hackers to scan your resources and exploit known vulnerabilities. This particular use case is especially useful in container deployments, as secure access is provisioned and deprovisioned automatically as resources are deployed or torn down through the use of user roles and service tags.

PRACTICE 4: MOBILE APP USAGE

It is desirable to include as many useful utilities as possible for users and administrators to manage and use their remote access solution for cloud resource access. Remote.It provides a mobile application that is available on iOS and Android devices, which allows users to communicate with other devices without having to open ports, even when IP addresses are unavailable. This allows easy management of device sharing, device search, and other services.

PRACTICE 5: ORGANIZING SERVICES AND DEVICES

IT and security administrators know that if they have many cloud devices and services in their environment, then it is a requirement to have some means for keeping them organized. Without such organization, it is impossible to search and access cloud resources efficiently. Remote.it supports the grouping of devices and services by categories. The platform helps users sort and group devices while performing various tasks such as execution of scripts. Further as Remote.It's deployment relies solely on its connectivity as code technology, it can easily be retrofitted into existing environments, providing to its users a single dashboard or API for access to an organization's entire network assets.

NEXT STEPS

Any IT or security team currently struggling with secure, flexible, and efficient access to their cloud Microsegmented workloads, would be wise to review the Remote.it solution. The platform offers the right types of support functions that will maintain consistency with security initiatives and tasks related to cloud devices and services, while also offering users and administrators with greater convenience.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.