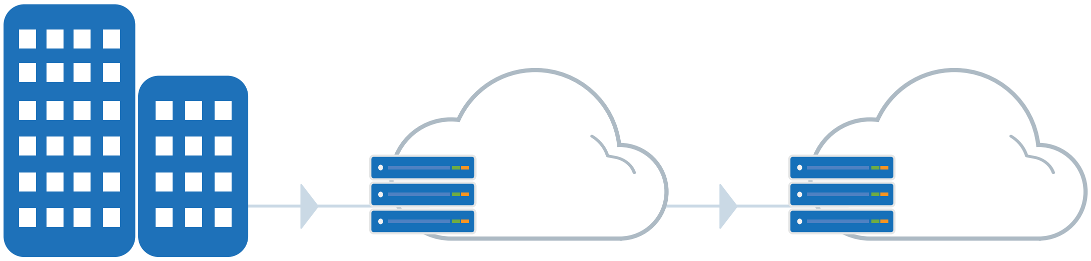
DxConnect & DxOdyssey

Zero Trust Integrated Secure Connectivity Software for Privileged Users, Containers and Hybrid/Multi-Clouds

Introduction

Contemporary connectivity is rapidly changing—as are the security demands for protecting it. Today's connectivity considerations are increasingly impacted by the following developments:

- **Remote privileged user access** (7 percent CAGR) is growing seven times faster than the world's population is (1 percent CAGR) (Cisco, 2019).
- **The Internet of Things (IoT)** is estimated to involve 28.5 billion devices by 2022 (Cisco, 2019).
- **Cloud native microservice connections** will be the quickest growing IP connection type by 2022 (Cisco, 2019).
- **Hybrid and multi-cloud deployments** are surging, contributing to projections of global costs of $6 trillion for cyber crimes by 2021 (Morgan, 2019).



» *The vulnerabilities of traditional network security are amplified by the complex hybrid and multi-cloud deployments of today*

These distributed computing settings require a security methodology to fortify protection in each of these areas. DH2i's DxConnect, along with DxOdyssey, provide zero trust integrated connectivity security in a single solution for remote user access, cloud native microservice connections, and hybrid and multi-cloud deployments. It consistently delivers cost-effective cyber security protection flexible enough for all connectivity needs for the next decade…and beyond.

» *Cyber security protection flexible enough for all connectivity needs*

The Challenge: Overcoming the Conflicting Connectivity Demands of Distributed Computing

The expedient growth of privileged users, containers for cloud native applications, and hybrid/multi-clouds has decentralized the connectivity landscape to support distributed computing. Consequently, enterprise security requirements are expanding in scope and degree, necessitating less latency, and becoming more fragmented by traditional security approaches. That fragmentation is so acute that the respective security needs of each of these common use cases frequently conflicts, forcing organizations to adopt different security measures for them.

- **Hybrid and Multi-Clouds:** When deploying perimeter security methods like legacy Virtual Private Networks (VPNs) for hybrid and multi-cloud use cases, users encounter gateway limitations devaluing the effectiveness and efficiency of the ensuing security. Since organizations don't own the infrastructure of the major cloud providers commonly used, implementation of these perimeter methods is exacting, time-consuming, and largely inflexible. These problems are especially disadvantageous because the chief value proposition of hybrid/multi-cloud deployments is the purported flexibility and celerity they provide.

- **Privileged User Access:** Unfortunately, privileged user access scenarios involve an entirely different, software-based security approach almost impossible to implement with VPNs. Organizations must double the cost and administration efoort to support these respective use cases, then often seek a third security method for cloud native access security for containers.

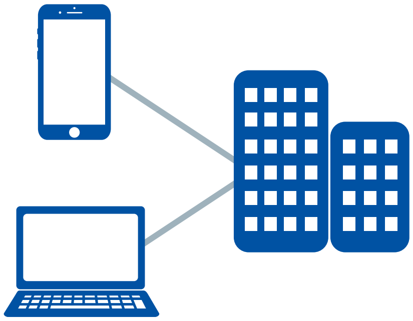
- **Cloud Native Microservice Connections:** The primary consideration for this scenario is the immense scale involved, which often exceeds that of the other two security approaches. Containers work best when they're swiftly deployed on demand and removed just as rapidly to accommodate spiking ecommerce traffic or other types of surges—whether planned or otherwise.

It's not uncommon for companies to triple their security investments for these three use cases, a practice that's particularly pricey and resource-intensive.

Perimeter Security Obsolescence

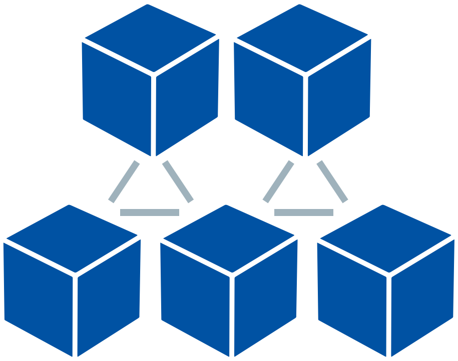
Typical perimeter security methods like VPNs, firewalls, and Access Control Lists (ACLs) are lapsing into obsolescence due to the sheer heterogeneity of the current computing climate. VPN insufficiency is the principal driver of the conflicting needs of the security mechanisms of the aforementioned three use cases; were perimeter security sufficient, organizations wouldn't have to triple their security investments. Historically, VPNs were designed to connect remote offices (such as different retail locations) with a paradigm analogous to castle moats in which they would open their networks to anyone or anything with the requisite password. Although this basic functionality is augmented today with complicated ACLs for evolving business requirements and users, the general castle moat functionality of VPNs hasn't changed and is unsuited for:

- **Hybrid and Multi-Cloud:** Although VPNs work well when users own the IT infrastructure of remote offices, for example, they become highly difficult to secure when one of their endpoints is a public cloud provider's infrastructure.
- **Remote User Access:** Theft is the principal pain point of deploying VPNs for third-party remote privileged users, which can either take the form of stolen credentials or compromised devices. Yet because every third party generally has different networking gear, companies are stuck managing multiple types of VPN connections. The biggest problem with this is that it creates a massive attack surface, as well as a nightmare for administrators to manage. As an alternative, a company may try to force vendors to use a single VPN, which is an expensive proposition.



» *Traditional perimeter security methods like a VPN create a massive attack surface*

- **Cloud Native Container Applications:** In addition to the foregoing issues of scale that VPNs struggle with, there's also a considerable amount of complexity setting up isolated networks for this purpose. Subsequently, there's a vast programming overhead deterring the deployment of VPNs for this use case and a high proclivity for unreliable connections when they are used—emphasizing the fact they were not created for the fine-grained flexibility of microservices. This fact becomes evident when dealing with isolated networks in which developers need to dynamically spin up on-prem containers in large public clouds, yet are stumped at figuring out secure connections to do so.



» *Excessive programming overhead and unreliable connections are primary deterrents from deploying VPNs for the microservices and containers use case*

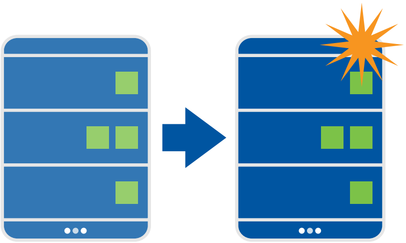
The failure of VPNs to satisfy these three frequently occurring use cases in distributed computing settings results in a void for connectivity security solutions. Based on that void, it's clear an alternative approach must be:

- **Superior to VPNs:** The castle moat perimeter security paradigm is innately broken in the 21st century, as the inexorable rash of security breaches (and cost of cyber security crimes) demonstrates.
- **Diversified:** Contemporary cyber security methods should be able to address all three of the recurring use cases so foundational to the decentralization of the current IT landscape.
- **Inclusive of Open Application Programming Interfaces (APIs):** Open APIs provide an opportunity for additional security mechanisms to buttress enterprise wide protection with solutions accessed via the cloud. For example, organizations may want to access alternative analytics solutions to monitor security concerns, or deploy other measures reinforcing regulatory compliance.

DxConnect and DxOdyssey

The combination of DxConnect (DxC) and DxOdyssey (DxO) typifies each of these traits for comprehensive cyber security in the distributed computing era. It enables organizations to leverage one investment for all three recurring use cases (hybrid/multi-clouds, remote privileged users and cloud native apps) without outdated VPNs. In addition to reducing overall security costs, DxC with DxO also decreases the amount of resources allocated to cyber security. It effectively consolidates the resource management necessary for protecting connectivity for relevant network administrators and developers. The cardinal features of DxC & DxO include:

- **Segmented Micro-Tunnels:** The dynamic micro-tunnels are segmented at the application level to isolate individual applications from the rest of an organization's network. Lateral movement attacks, in which intruders systematically take over networks after initial breaches, are eliminated. Moreover, the tunnels are underpinned by application level Datagram Transport Layer Security (DTLS) encryption and Public Key Authentication. They're also highly available with automatic, self-healing fault detection and failovers, culminating in always on, always secure connections.



» *Micro-tunnels created with DxO are accompanied by automatic self-healing fault detection and failovers*

- **Discreet Invisibility:** The app-level micro-tunnels connect to one another over non-standard User Datagram Protocol (UDP) specifically augmented with packet correction capabilities. Port selection between applications is randomly generated via a matchmaker service for enhanced security. Moreover, ports are closed once connections are completed, rendering tunnels all but invisible while minimizing, rather than expanding, network attack surface.
- **Multi-Cloud Ready:** The concealed micro-tunnels scale across hybrid and multi-cloud settings while delivering consistent policy and auditing capabilities, regardless of setting. The solution utilizes cloud platform native capabilities ideal for running containers in the cloud, and is vendor agnostic to eliminate vendor lock-in.

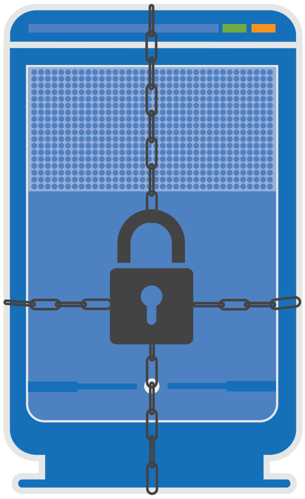
The open API aspect of the software enables secure connections ingrained within the DevOps tool chain

- **Open APIs:** The open API aspect of the software supports building and scaling cloud native applications with common container frameworks such as Docker, Kubernetes, Puppet and Chef. This feature also enables secure connections to be ingrained within DevOps tool chains. Most of all, open APIs harden existing network security infrastructure and data pathways for a holistic, layered security approach leveraging the best cloud services available.

Use Cases

Privileged User Access

DxO & DxC are readily installed with a minimal number of clicks. The configuration—traditionally one of the most difficult steps—is handled by IT, which emails users a configuration file for remote access. Once the gateways are established at both ends and the tunnels are being formed into a group, the latter are routed to the matchmaking service in the cloud for authentication and port selection. At this point, the solution can use its open APIs to add, for example, a multi-factor authentication to the process to reinforce security. Therefore, once the tunnels are authenticated by the matchmaker, they can run through a third-party cloud service to verify the nature of the device, if need be, by sending a text message with a code to which users must respond, or deploying any other form of authentication. Even though users may be authenticated by the matchmaking service, they still have to respond to this device level interrogation for even more fortified security for privileged user access.



» DxO and DxC can use its open APIs to add things like multi-factor authentication to the process to lock down security even further

Edge Computing and the IoT

» *Open APIs and the other verification tools tunnels can access are critical for the IoT use case*

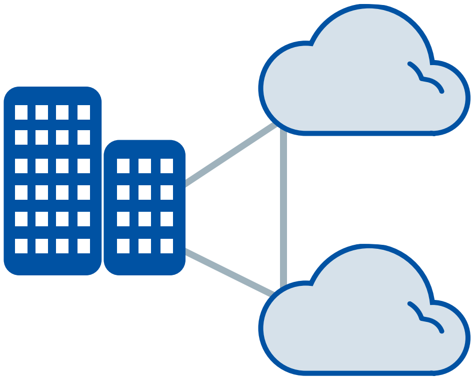
DxO & DxC are applicable to both edge computing and connected devices in the IoT. In the case of a smart refrigerator, for example, DxO & DxC are embedded within the device's operating system. From there, the smart refrigerator is able to authenticate itself and connect to a gateway. Then, a tunnel is formed via the matchmaker service so it can communicate with the refrigerator's manufacturer in the cloud. The open APIs and additional verification tools tunnels can access are critical for IoT use cases in which it's imperative to ensure devices are what they claim to be to prevent Distributed Denial of Service attacks. The lack of hardware or device security on smaller, less computationally accomplished endpoint devices in the IoT makes it necessary to verify devices haven't been infiltrated by hackers attempting to access organization's networks.

Zero Trust Service Mesh

The container versions of DxO & DxC are applicable for creating and developing applications in the cloud via containers. It effectively functions as a service mesh deploying microservices for these cloud native applications. DxO & DxC enable DevOps users to securely access various nodes in the cloud with popular providers such as Amazon Web Services, Azure, or Google Cloud. Each of the resources, the various cloud networks involved and those of the DevOps team on premises, send metadata to the cloud matchmaking service, which facilitates the cloaked tunnels between them. Thus, data securely travels over public WAN networks in the cloud via UDP with DTLS encryption for developers to access microservices. DxOdyssey, which enables users to access hybrid and multi-clouds and which DxO & DxC architecturally sit atop, facilitates the sidecars in the service mesh for the efficient use of microservices with this zero trust, secure connectivity approach.

Fully Integrated Zero Trust Connectivity Security

The realities of distributed computing have indelibly altered the connectivity landscape. The predominance of cloud deployments, applications created and ran in the cloud via containers, on-premise and cloud hybrid clouds, and edge computing has shifted connectivity security from static to dynamic locations. Conventional perimeter security no longer suffices, forcing organizations to adopt a new approach to simplify their security architecture and investments.



» *The predominance of hybrid and multi-cloud deployments has necessitated a new approach to perimiter security—one that simplifies security architecture and investments*

DxO & DxC fluidly adapts to each of the defining scenarios of the decentralized IT landscape, bolstering secure connections for remote privileged users, microservices for cloud native applications, and hybrid and multi-cloud settings. Its capital advantage is the successful integration of zero trust security among each of these use cases, offering a single solution to a multiplicity of settings and needs. Moreover, installation is quick and easy, configuration is largely handled remotely by IT experts, and connectivity is secured at the safest level between applications. Combining DxO & DxC is a modern approach for tomorrow's security needs, yet readily available today.

Try DxOdyssey and DxConnect for free:

dh2i.com/trial

References

Cisco. (2019). Cisco visual networking index: forecast and trends, 2017-2022. www.cisco.com Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

Morgan, S. (2019). 2019 official annual cybercrime report. https://cybersecurityventures.com Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/