REMOTE AND VULNERABLE

Securing a Changing Workforce from Cyberattacks

VIRNETX

Remote Workforce Means Rising Threats

For many enterprises, the era of small cubicles and cramped workspaces spread across jammed office buildings is rapidly coming to an end. According to a Gartner study, **31 percent** of all global employees are now working remotely with the United States leading the way at **53 percent.**

The challenge for enterprises to support their growing remote and hybrid workforce is the need to provide secure access, over the Internet, to business applications, services, and infrastructure.

While there are many benefits to working remotely for employees and employers, the big increase in remote workforces has raised the threat of cyberattacks to an all-time high. KuppingerCole, an independent, international analyst firm, reports a **238 percent increase** in worldwide cyberattacks since the start of Covid-19. Not surprisingly, a more remote workforce is being blamed. A Forrester study found that 74 percent of businesses and organizations correlate more cyberattacks to remote workers and technical vulnerabilities.

Because remote and hybrid workers often use personal devices (BYOD) and unsafe Wi-Fi networks, which are outside of the Enterprise's control, these employees are highly susceptible to cyberattacks. To help them get their jobs done efficiently, and without interruptions, remote workers require easy and secure access to applications regardless of device type or network. In addition, IT teams need tools that offer visibility and control over employees they are assigned to protect.

The Cloud and Security Concerns

Cloud computing growth has rapidly expanded as enterprises continue to move applications and services to the cloud. The cloud offers scalability, operations and development efficiency and remote access benefits for their workforce.

However, shifting critical data to the cloud has resulted in security concerns and the need for enterprises to control access and gain visibility into how information is being used, who is accessing it and where it is going.

Supporting Frontline Cybersecurity Soldiers

On the frontlines protecting remote and hybrid workers are busy IT teams and security professionals. Often overworked and under resourced, these cybersecurity foot soldiers are fighting the good fight against relentless cyber-attacks but are frequently losing high-stakes battles. Enterprise security leaders are looking for security solutions and partnerships that can ease the burden on their teams, allowing them to operate more effectively and efficiently.

They need tools that can significantly improve security postures, increase workforce productivity, provide quick responses to security issues, and consolidates security visibility across the enterprise.

Paradigm Shift to Zero Trust

The shift to remote work and expansion of the enterprise network perimeter has driven the growth of Zero Trust Network Access (ZTNA) solutions. The Zero Trust concept treats all networks like the Internet, where all users and devices are untrusted by default.

Device location within the network is not a factor for deciding trust.

Each user and device on the network requires authentication and authorization, based on policy, prior to accessing any applications or resources on the network.

ZTNA facilitates security around remote work, because Zero Trust policies enable granular access control, end-to-end encryption of network communications and remove application visibility from the public Internet.

The Genesis, Genius Behind Matrix

Matrix provides the interface for a growing remote and hybrid workforce to securely access enterprise applications, services, and infrastructure by leveraging the secure environment created by the VirnetX One platform. Matrix protects applications using zero trust network access (ZTNA), allowing employees to work from anywhere with seamless and secure access to corporate applications, regardless of their location, network, or device.

With Matrix, IT administrators and security professionals can easily manage access, enforce policy, and gain visibility into the array of secure connections created between users, devices, and protect self-hosted corporate applications from threats.

Matrix allows enterprises to deliver a modern, secure, and seamless user experience across their remote workforce without the need for legacy VPNs or exposing applications to the public Internet.

Matrix delivers next-generation ZTNA capabilities across applications, services, and infrastructure to:

- **Remove the attack surfaces**
  Applications are invisible on the Internet to both public and unauthorized users, eliminating external threats and attacks.

- **Secure communication links**
  Encrypted secure communication links are established on-demand directly between authorized users and applications (e.g., peer-to-peer) keeping data secure and under your control.

- **Eliminate lateral movement**
  Applications are segmented into isolated virtual networks with users given granular access only to specific applications.

- **Enforce least-privilege access**
  Network access to applications is determined by identity and enforced by strong certificate credentials to enforce access policy.

- **Deliver a modern and secure user experience**
  Seamlessly connect users to private applications regardless of their device, location, or network without impacting the application experience.

- **Secure applications at scale**
  Easily secure self-hosted legacy, on-premise, or cloud-based applications. Control access, gain network visibility and apply dynamic access policies to protect information.

Why Matrix Matters for IT Teams

For IT administrators and security professionals, Matrix offers intuitive threat protection by minimizing application attack surfaces and allowing Enterprises to quickly adapt to the rapidly evolving threat landscape.

Matrix also gives you time to prioritize and address vulnerabilities while providing insights to IT teams so they can quickly remediate threats and vulnerabilities.

In addition, Matrix supports digital transformation initiatives, scales your remote workforce, and is easy to use and deploy.

Better yet, the platform operates in the cloud and works on a wide range of devices.

Easing the Burden for IT Teams

With Matrix, IT administrators can control users and devices that have application visibility.

This means only authorized employees can see the application exists and navigate to the login page. The login page, application interfaces and application infrastructure is not visible to the public or unauthorized users.

Each application is isolated and segmented into a virtual private network that restricts lateral movement between applications. At the user or device level, Matrix provides real-time management, application access control and network visibility.

Stealthily Helping Employees Do Their Jobs

Remote workers receive training and follow security policy and guidelines, but those processes are not foolproof.

Matrix works in the background to secure and protect corporate applications and ensure security policies are followed while making it easy for employees to do their jobs regardless of their device or location.

Their success is measured on meeting deadlines, work quality, and how they impact the business. Matrix is quietly and effectively with them throughout their workday.

A Major Helping Hand for Hybrids

According to an Accenture report, hybrid work models are being used by 63 percent of high-revenue growth companies. Fifty-five percent of respondents from a Stanford study want to spend some time in the office and some at home. This means more employees are switching between corporate laptops and personal (BYOD) devices.

To do their jobs and securely communicate with their teams and colleagues, they need a variety of applications and data sources that are often confidential and proprietary.

Because they are not easy to use and prohibit their ability to complete their work on time, many employees are not satisfied or increasingly frustrated with the current systems their companies have in place to secure information access.

Matrix provides the solution by allowing employees to securely work from anywhere.

Key Differentiators

VirnetX Secure Domains

VirnetX Secure Domains are dynamic, software-based, virtual private networks that can be created on-demand, to allow mutually authenticated systems to securely communicate over public networks, such as the Internet.

Matrix creates a unique Secure Domain for each application, isolating the application and the users that have access to a network microsegment or secure enclave. This eliminates public access and restricts lateral movement across the network.

Each Secure Domain is represented as a private domain name system (DNS) record, such as company.scom, only available for registration and resolution using VirnetX products.

Secure Communication Links

Matrix ensures all data traffic is kept private and encrypted between an employee's device and the enterprise application. This offers better performance, data security, and control of information across the enterprise.

Secure communication links offer direct peer-to-peer connections meaning user traffic is never visible to VirnetX or other third parties.

VirnetX's technology generates secure connections on a "zero-click" or "single-click" basis, significantly simplifying the deployment network security solutions by eliminating the need for end-users to enter any encryption information.

Secure Any Application or Service

Matrix seamlessly secures a variety of different use cases across the enterprise including self-hosted web applications, remote desktop, file sharing and databases. Protection of these key use cases is critical since they are the top targets for threat actors and represent key entry points to access sensitive and confidential information.

Matrix features templates to quickly secure common use cases while allowing IT administrators and security professionals to create custom templates for more advanced application deployments requiring multiple ports and protocols.

VirnetX One Platform

The VirnetX One platform is a cloud-based, software-as-a-service (SaaS) platform that uses VirnetX patented technology to create an environment that virtualizes private networks and brokers secure communication links between trusted peers, regardless of device, network, or location.

This environment can be applied to secure communications across a wide variety of use cases and offers protection from cyber-attacks. VirnetX One implements a modern Zero Trust architecture built on VirnetX Secure Domain Names and patented technology.

The VirnetX One platform allows cybersecurity leadership and professionals to improve the enterprise security posture, increasing workforce productivity, providing the agility to quickly respond to security threats and consolidating security visibility across the enterprise.

The VirnetX One platform is the security foundation for Matrix.

Supported Operating Systems
Windows 10 or later macOS 10.15 or later iOS 14.3 or later Android 9 or later

Modern & Cloud-Native

- Simplifies complex networking concepts and security boundaries.
- Simple and easy to user experience for network management and administration.
- Consolidates insights into a single dashboard view offering administrators control and visibility into the security of their network.
- Cloud native solution without the need for additional hardware.

Dynamic Virtual Private Networks

- Adapts to secure and enable seamless communications regardless of the physical location or network environment.
- Support any type of network communication or application.
- Virtual private networks can be created on-demand for ephemeral, permanent, and ad hoc use cases.

Trusted Technology

- Patented technology originally developed for the U.S. Intelligence community.
- Worldwide network of partners is helping secure legal, financial, healthcare, manufacturing, and government customers.

Powerful Solutions for Protecting a Changing Workforce

Matrix secures private access to Internet applications, services, and critical infrastructure. Matrix also enforces access policy controls and enables real-time network management to protect cloud or on-premises self-hosted applications from threats.

The Future is Now

Clearly, remote workforces have weakened cyber security for many businesses and organizations. Because remote and hybrid work is here to stay, businesses and organizations need to contain and access security risks, better educate remote workers, develop remote work security policies, and invest in stronger and more effective security platforms.

Matrix offers a powerful solution for hybrid workers to securely access enterprise applications and cybersecurity professionals to prevent nefarious attacks and protect their vulnerable workforce.

For more information, visit https://virnetx.com/matrix/.

About VirnetX

VirnetX Holding Corporation (NYSE: VHC) is an Internet security software and technology company with industry-leading, patented technology for Zero Trust Network Access ("ZTNA") based secure network communications. VirnetX's patented Secure Domain Name Registry and GABRIEL Connection Technology™, are the foundation for its VirnetX One™, software-as-a-services (SaaS) platform. VirnetX's technology generates secure connections on a "zero-click" or "single-click" basis, significantly simplifying the deployment of network security solutions by eliminating the need for end-users to enter any encryption information. VirnetX's products, including War Room™, VirnetX Matrix™, and Gabriel Connection Technology™, are designed to be device and location independent, and enable a secure real-time communication environment for all types of applications, services, and critical infrastructures. For more information, please visit: https://virnetx.com/.

MATRIX™

VIRNETX