VIRNETX
EXECUTIVE SUMMARY

THE PROBLEM

As internet usage grew, more organizations increased their dependency on the internet. The open and public design helped access and reach, but opened a path for nefarious activity. As enterprise networks grew; internally bridging connections between IT and OT segments and externally connected to other organization networks (e.g., supply chain), chains of exposed vulnerabilities have reached near pandemic levels while leaving a wake of increasing costs.
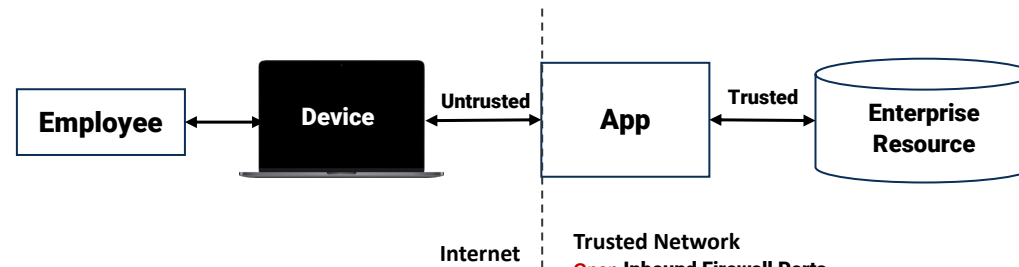
Enterprise networks are based upon the open access architecture of the Internet, but the threat landscape has evolved dramatically since its inception. This requires many tools to protect an organization's network. From threat monitoring to prevent, to intrusion detection to alert, to incident response to act, all these tools are necessary, yet all rely on the public nature of the network. The cost of managing and protecting any organization's network is untenable. The network edge is blurred as the number of devices rise and the boundaries of the workplace exceed the organization's resources. The 'Network' is the problem.

Organizations **need** to proactively architect zero trust security solutions *into* their network.

Public Internet Access

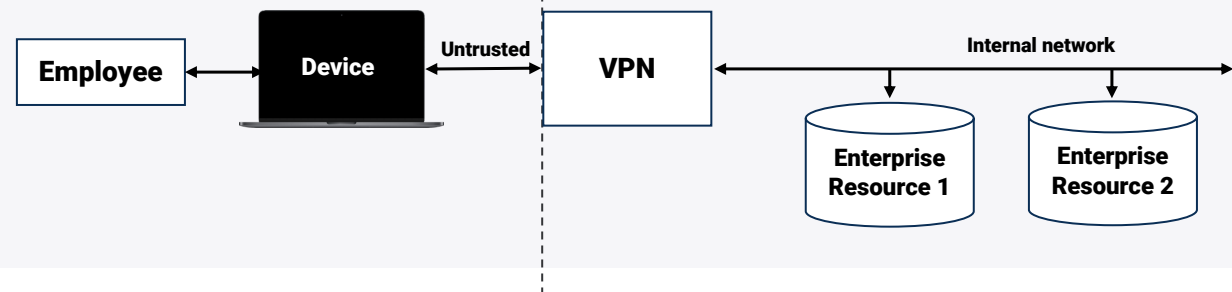**Existence and access to Enterprise resource visible to anyone on the Internet.**

Threat - Potential attack vector for scan-and-exploit attacks, unpatched vulnerabilities, zero-days, misconfigurations, brute force and denial of service (DDoS) attacks.

| Employee | ←→ | Device | Untrusted ←→ | App | Trusted ←→ | Enterprise Resource |

Internet | Trusted Network
Open Inbound Firewall Ports

Enterprise Network Access

Using VPN to gain trusted access to an Enterprise network.

Threat - Phishing attack, malware, credential access or physical access to System allows threat actor to gain access and then move laterally across the network to install malware and steal data.

| Employee | ←→ | Device | Untrusted ←→ | VPN | ←→ Internal network → |

Enterprise Resource 1   Enterprise Resource 2

WAR ROOM   ONE   **MATRIX**

VIRNETX

SOLUTIONS: available worldwide

VirnetX zero trust enabling solutions can be deployed within an existing network regardless of network technology or topology. Enterprise resources as well as user devices both use our patented secure domain names technology with built in authorization and authentication and maintain their own cryptographically signed certificates. While VirnetX brokers initial discovery between enterprise resources and user devices, network connections are mutually authenticated and established peer-to-peer, creating a decentralized network through on demand VPN services. Despite enterprise resources and user devices being on a virtual network each network connection is fully isolated therefore in a worst-case scenario where a user/device goes rogue the threat is contained only to just one network connection. Moreover, on demand VPN services are fully automated and can be triggered without user intervention making it attractive for remote, unmanned devices (IoT).

VIRNETX

Internet

Zero Trust Network Access
Only Authorized Users & Devices

Enterprise Private Networks
with VirnetX Secure Domain Names

- Employees
- Threat actor
- Internet users
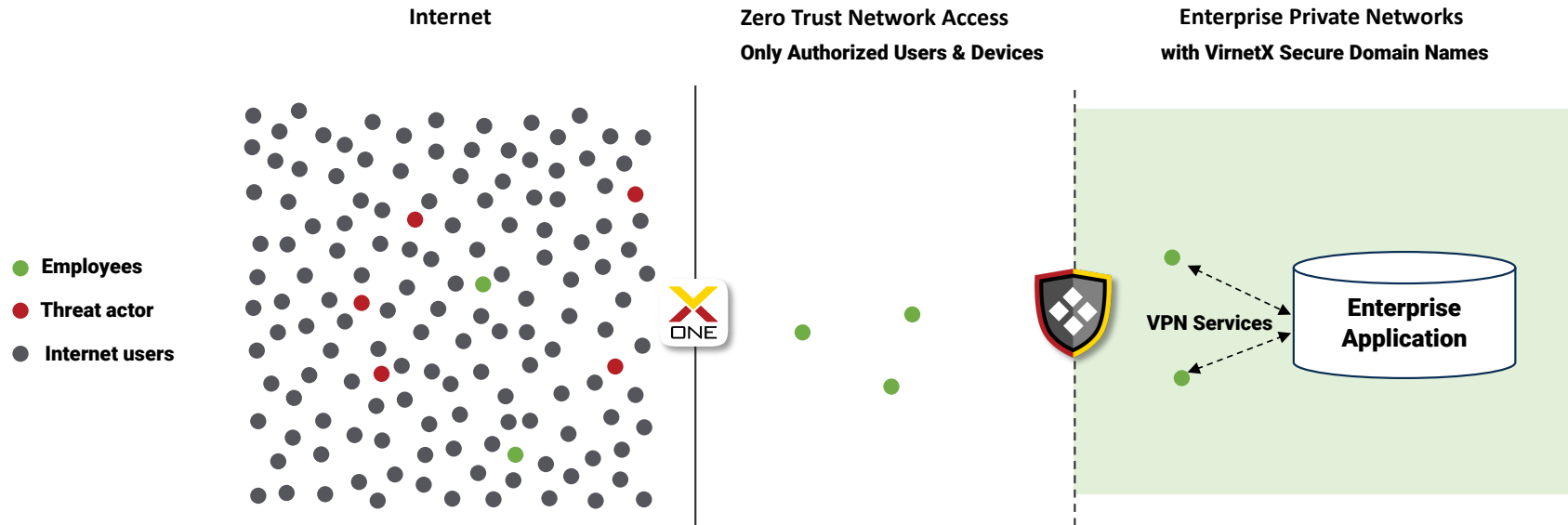
X
ONE

VPN Services

Enterprise
Application

Figure 2. VirnetX offers layered security with Zero Trust Network Access (ZTNA) to filter only authorized users and devices and then segment access between applications, services and critical infrastructure using peer-to-peer virtual private networks.

VIRNETX ONE

VirnetX One™, our flagship SaaS based platform offers organizations outside in and inside in protection with the highest security in the market:

- Seamless activation and provisioning of a zero-trust enabling platform that provisions a dynamic credential-based network
  - using built-in authorization and authentication prior to look up
  - through Secure DNS triggered resolution,
  - while protecting and automatically establishing peer-to-peer VPN connections,
  - leveraging existing VPN services within industry standard operating systems devices
- Providing Full Control and Protection of your organization's sensitive information and intellectual property.
- Gaining visibility and Insight into how information is being used, Who's Accessing It and Where It's Going.
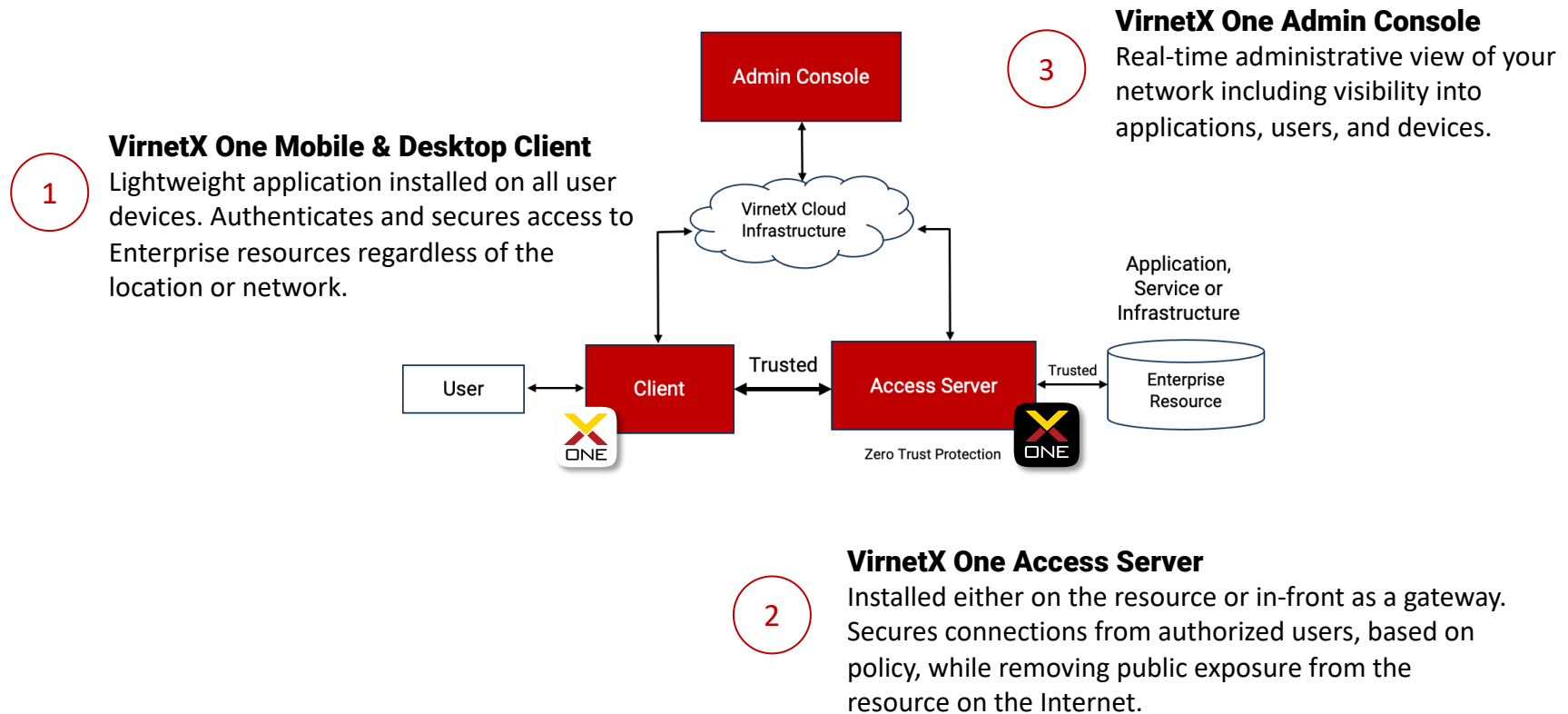- Real time network information, Actionable value, Solid ROI

VIRNETX ONE

VirnetX One Mobile & Desktop Client
Lightweight application installed on all user devices. Authenticates and secures access to Enterprise resources regardless of the location or network.

VirnetX One Admin Console
Real-time administrative view of your network including visibility into applications, users, and devices.

1

3

Admin Console

VirnetX Cloud Infrastructure

Application, Service or Infrastructure

User

Client

Trusted

Access Server

Trusted

Enterprise Resource

ONE

Zero Trust Protection

ONE

VirnetX One Access Server
Installed either on the resource or in-front as a gateway. Secures connections from authorized users, based on policy, while removing public exposure from the resource on the Internet.

2

Figure 3. Foundational components for deploying the VirnetX One platform to secure your network.

VirnetX Matrix™, enterprise application protection against cyber attacks
- Built on a zero-trust philosophy seamless and secure access to all applications for your remote workforce. Implement a modern, cloud-based, zero trust network architecture secured by VirnetX One.
- Threat Protection
  - Zero Trust Network Access
  - Flex network segmentation
  - Protect cloud or on-premise applications
- Secure Connectivity
  - Client-based encrypted application access
  - Certificate-based authentication
  - Automated issuing, renewal, and revocation of device certificates
- Real-Time Access & Control
  - Manage user access per application
- Increase Visibility
  - Individual device posture and insights
  - Health and operational status of application network
  - Visibility into the users and devices with access

VirnetX War Room™ provides an industry leading, safe, and secure video conferencing meeting environment where sensitive communications and data is invisible to those not authorized to view it.

- Validates permissions of all users, and devices requesting access to any secure meeting room prior to granting access.
- No longer be at the mercy of someone 'bombing' your meeting just because they received the link!
- Clients include government organizations as well as all professionals from legal, financial, and healthcare where limiting access to confidential data is an absolute and critical requirement.

CONCLUSION

As long as there has been an internet, there have been people who try to compromise it. The bigger the Internet gets, the higher risk it becomes for intrusions, phishing, viruses, worms, and fraud. As the threats have increased, so has the need for better security solutions and with a business case to support it. The VirnetX One platform and products like Matrix and War Room meet today's requirements. Customers who implement the VirnetX products will have the assurance that their data and information is protected by the most secure technology available in the market today.

ABOUT

VirnetX Holding Corporation 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 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. VirnetX's patent portfolio includes over 200 U.S. and foreign granted patents, and pending applications. For more information, please visit: http://www.virnetx.com.