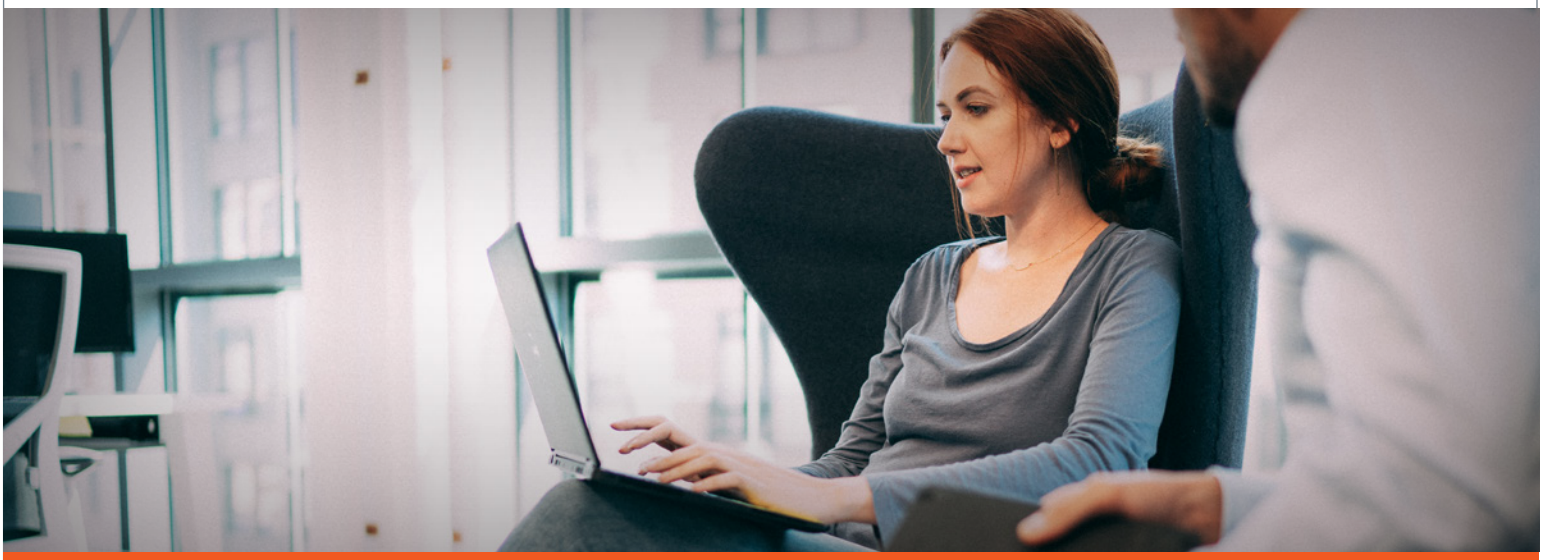
WHITE PAPER



A ZERO TRUST APPROACH TO SECURE REMOTE ACCESS

Protecting Privileged Access for All Remote Sessions

BeyondTrust

TABLE OF CONTENTS

1 Introduction - What Is Zero Trust?

By definition, a zero trust security model advocates for the creation of zones and segmentation to control sensitive IT resources. This also entails the deployment of technology to monitor and manage data between zones, and, more importantly, authentication within a zone(s). This encompasses users, applications, context, attribution, and other resources and parameters.

In addition, the zero trust model redefines the architecture of a trusted network inside a logical and software-defined perimeter. This can be on-premises or in the cloud. Only trusted resources should interact based on an authentication model within that construct.

Zero trust is increasingly relevant today as technologies and processes like the cloud, virtualization, DevOps, edge computing, edge security, personification, and IoT have either blurred or dissolved the idea of a traditional firewall and network-zoned perimeter. The seismic shift to remote working has only accelerated the demise of the traditional perimeter.

Zero trust is increasingly relevant today as technologies have either blurred or dissolved the idea of a traditional firewall and network-zoned perimeter.

While zero trust has become a trendy catchword in IT, it's important to call out that, in practice, this model is very specific about how things should be designed and operate. Zero trust may not work for every environment. In practice, it is best suited for new or refreshed deployments, or to strictly control user access to sensitive resources, especially when they are connecting remotely.

When applying the granularity of privileged access management, which includes secure remote access, zero trust can ensure all access is appropriate, managed, and documented—regardless of how the perimeter has been redefined.

Securing Today's Workforce – At Home, In the Office, or Anywhere In Between

As a security best practice, native remote access protocols should be disabled for corporate-issued computing device(s). Unfortunately, in many environments (especially for users working from home), this security control has not been implemented and remote devices may be accessing corporate resources using remote access pathways that aren't adequately secured.

The rationale behind enabling protocols like RDP, SSH, and VNC has been a source of contention between information technology and information security teams. One argument is the need for low-cost remote access technology natively supported by the operating system. This is generally advocated by IT. Security and compliance teams, on the other hand, are wary of the inherent vulnerabilities, wormable exploits, and the lack of auditing and secure network routing of native protocols.

There needs to be a balance between these approaches. Authorized users need to initiate a secure remote access session to any device, any place, regardless of protocol. In addition, session monitoring, credential injection, and least privilege must be applied to overcome the security and compliance concerns governing an organization. These capabilities must be in place whether the employee is

working from the corporate office or from a remote location. Here, zero trust architecture can play a pivotal role to overcoming native remote access protocol challenges. A zero trust implementation can accommodate almost any environment and allow for remote sessions using proprietary access technologies.

> *Zero trust architecture can play a pivotal role to overcoming native remote access protocol challenges*

Zero Trust and Secure Remote Access in the 'New Normal'

Amidst travel shutdowns, social distancing, and stay-at-home orders, employees find themselves working with new freedoms and new restrictions. Employees working from home are using video conferencing, VPN, and remote access solutions to conduct business. Within this "new normal", there are plenty of operational tasks now being performed from home that require privileged access. This runs the gamut from managing the organization's social media accounts to administering servers, databases, applications, and SaaS solutions.

Our home networks are now serving entertainment, school, work, and providing an active conduit into our business. As a result, we are allowing our insecure home networks to be an extension of our information technology 'perimeters' to perform tasks in our business environments.

We have already seen security weakness related to these trends in the form of ransomware and breaches that only succeed due to threat actors having compromised remote access. With hardening and rearchitecture of remote access, we can minimize this risk.

Remote working introduces new attack vectors and potential regulatory compliance issues that need to be resolved. For most organizations, this represents an unacceptable risk to the business since most of their highly sensitive data and applications reside on mission-critical platforms within their data centers and trusted cloud environments.

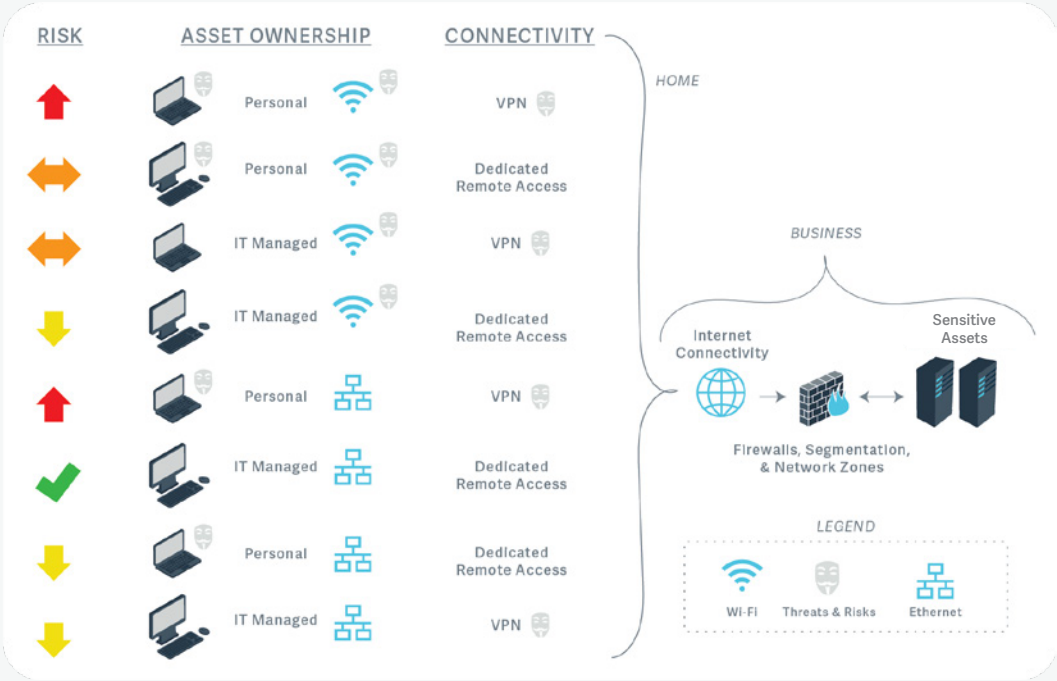
Remote working introduces new attack vectors and potential regulatory compliance issues that need to be resolved.

As the concept of a perimeter has fundamentally changed, and the way we use privileges and access sensitive information has broken our traditional security best practices, we need to rearchitect a solution that can address these underlying issues.

The diagram below illustrates risks based on remote working within a decentralized, perimeterless environment, and reflects the combination of assets, connectivity, remote access technology, and prime locations for a threat actor to infiltrate an environment.

In addition, based on normal connectivity, applications could operate remotely or using a remote session. To secure all activity, connectivity itself must be secured and all access provided only via a remote access technology.

Figure 1:
Risk Assessment Framework.



The risks based on the combination of assets, connectivity, remote access technology, and prime locations for a threat actor to infiltrate an environment based on a privileged remote worker

In Figure 1 above, each "mask" represents a risk:

- **Three Masks:** Unacceptable critical risk
- **Two Masks:** Medium level of acceptable risk
- **One Mask:** Low risk for remote access
- **Zero Masks:** Best case for acceptable remote connectivity

Note that using a personal device with a business-issued VPN client is always a critical risk, regardless of whether the connection is wired or wireless, because the device is unmanaged and the organization has no control over how it is used, updated, or operated.

In this decentralized environment, threats exist when accessing sensitive internal resources from:

1. **Personal or Bring Your Own Device (BYOD) hardware** that is unmanaged, unpatched, multi-user, end of life, or may otherwise be susceptible to phishing or malware. In addition, BYOD users are typically their own local administrators, amplifying the risk.
2. **Insecure home networks** based on WiFi connectivity where the connection is potentially insecure, has a weak password, is wide open, or may allow a man-in-the-middle attack due to a common SSID or poor encryption. Also, other devices could compromise the wireless network or monitor communications. This includes privileged accounts outside of corporate governance used by home networks accessing consumer SaaS solutions.
3. **VPN technology**, which typically uses split tunneling and should never be installed on personal devices that could compromise communications and provide a conduit for lateral movement via the

flaws in the home network. Because VPN technology only operates at the network layer, it is unable to monitor remote sessions. And typically, remote users only need application access (application layer).

Addressing the Risk

To mitigate the threats, a combination of zero trust, IT managed devices, IT Governance, and privileged access management can succeed where traditional technology alone may pose an unacceptable risk.

- **IT Managed** – Managed security controls for risk assessment including core disciplines for vulnerability and patch management.
- **Connectivity** – Minimizing network risk with a wired connection in lieu of unknown wireless connectivity.
- **Privileged Access Management** – Remote Access sessions are initiated at the application layer based on role, including credential obfuscation, eliminating the need for network layer traffic per application per user. Privilege elevation is strictly controlled locally and across the network, also eliminating local administrative credentials and admin rights for end users.
- **Governance** – Documenting all privileged activity for compliance, including remote access user behavior.
- **Zero Trust** – Implementing a cloud-based management architecture for all remote access sessions honors zero trust, and strict application control is enforced. This applies the concept of zero trust to all sessions, regardless of their origination or destination.

VPN Security Challenges

VPN and other traditional endpoint security solutions (especially on-premises) cannot typically perform the above functions. They were never designed or architected to manage remote workers and cannot effectively manage risks outside of a defined perimeter. For zero trust to succeed, the network and environment need to be secured before a zero trust architecture can be implemented.

Remote access technology was designed to manage sessions and, with a few considerations, can be implemented using a zero trust model. However, a combination of zero trust, endpoint security, and IT managed devices with secure connectivity can accomplish the desired goals.

> *VPNs were never designed to manage remote workers and cannot effectively manage risk outside of a defined perimeter.*

Finally, as a potential replacement for VPN, secure remote access with zero trust can provide the following advantages over VPN alone:

Table 1: VPN vs. Privileged Remote Access

Feature	VPN	Privileged Remote Access
Scalable	✓	✓
Secure	✓	✓
Network Layer Access (Protocol Tunneling)	✓	✓
Role-Based Access	✓	✓
Encrypted Traffic	✓	✓
Application Layer Virtualization		✓
Remote Desktop		✓
Virtualized Web Application Access (HTTP/ HTTPS)		✓
Proxied RDP Access		✓
Proxied VNC Access		✓
Proxied SSH Access		✓
Application Session Monitoring		✓
Application Session Recording		✓
Just-in-Time Access		✓
Privileged Access Management Integration		✓
ITSM Integration for Access		✓
Password Management / Credential Storage		✓
Agentless Access		✓
Prevent Lateral Movement		✓

2 Success with a Zero Trust Model

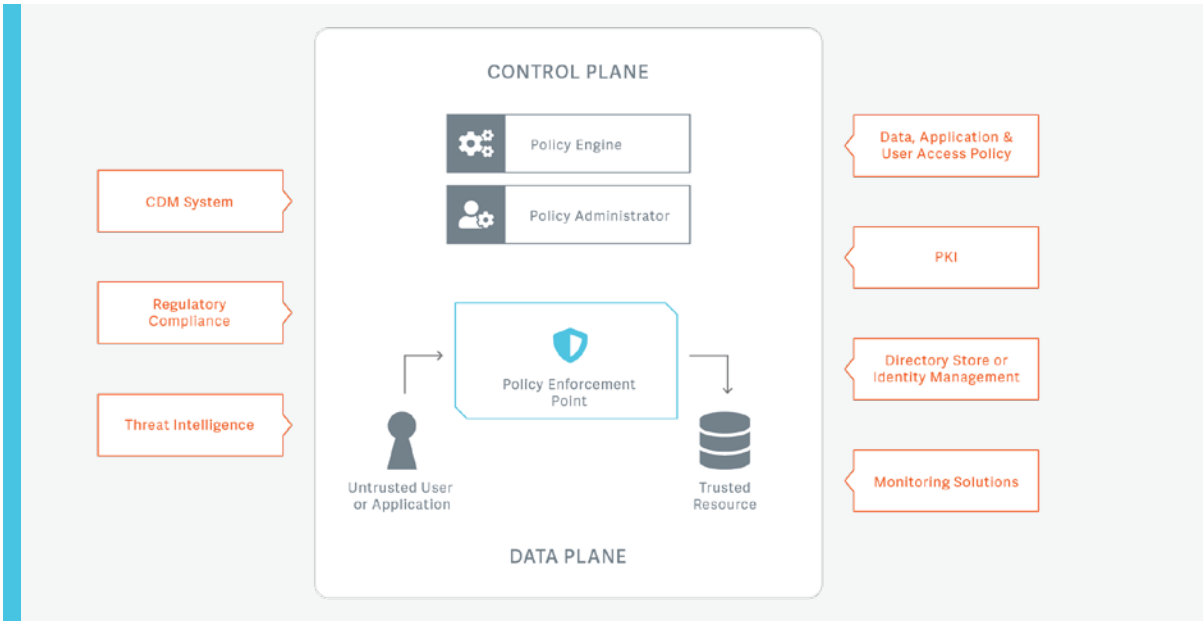
To successfully implement zero trust controls, we must explore what a successful deployment of a zero trust model looks like. We need to then apply the model to remote access sessions, regardless of where they are deployed and operate from or to.

Achieving Zero Trust, as Defined by NIST, with Secure Remote Access

Based on the guidance defined by NIST 800-207, a zero trust architecture clearly states that the goal is to focus security on a small group of resources (zones) in lieu of wide network perimeters or environments with large quantities of resources interacting "freely". It is a strategy where no implicit trust is granted to systems based on their physical or network location (local area network, wide area networks, or the cloud), but rather access is granted by a trusted source for either a user or application.

Consider this diagram of a simplified NIST-based zero trust architecture:

Figure 2: NIST-based Zero Trust Architecture



The key components of the control plane and data plane are typically found in secure remote access solutions as follows:

- The *Policy Engine* is responsible for the decision to grant access to a resource. It uses as much data as it can based on roles, attributes, and threat intelligence to determine if access should be granted.
- The *Policy Administrator* is responsible for establishing the connection between a client and a resource. It provides the negotiation between the resources to "state" that the connection is allowed.
- The *Policy Enforcement Point* is responsible for enabling, monitoring, and terminating the connection between the Untrusted Resource (user or application) and Trust Enterprise Resource.

If we map this to BeyondTrust's Secure Remote Access solution we find:

- The *Policy Engine* can be found in management capabilities governing remote access, and the role

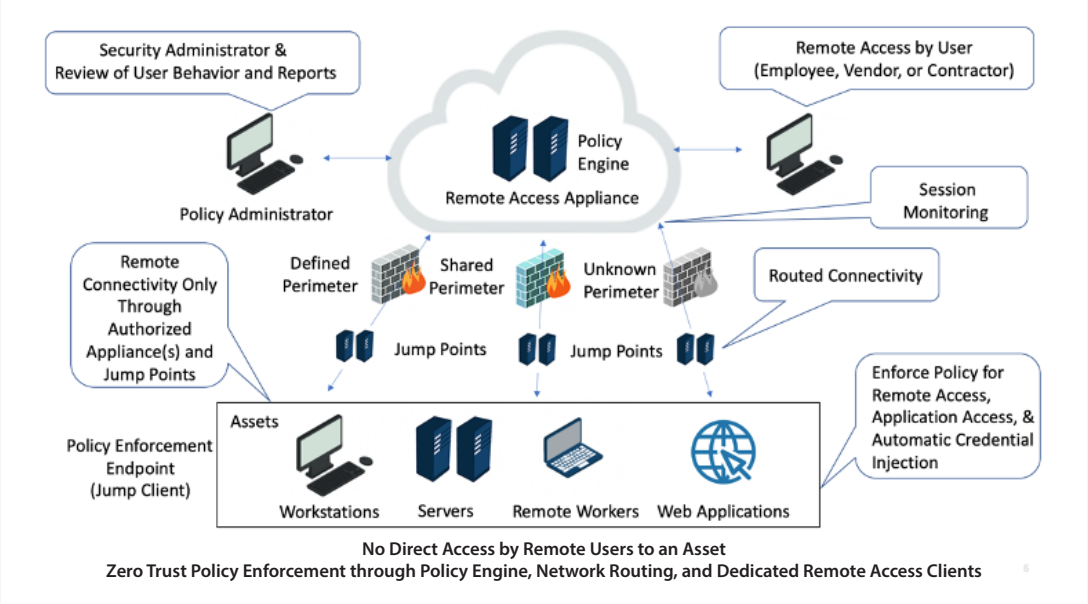
and attribute-based access models defined by the Policy Administrator. BeyondTrust Secure Remote Access can manage assets and users in any network zone regardless of perimeter, as long as there is Internet access available.

- The Web *Policy Administrator* creates, updates, and manages the policy for end users, grants access, and automates application remote access; this is the basis for zero trust. Access to the resource or application is granted to the Policy Administrator and can be managed through the BeyondTrust Secure Remote Access Console.
- The *Policy Enforcement Point* is implemented using a Secure Remote Access Jump Client. It responds to a remote access request for a session or application from a trusted Policy Engine or intermediate proxy, called a Jump Point. This is fundamental to zero trust since a user is never granted direct access to a resource as when using a native operating system protocol. All connectivity is managed and monitored, and only session activity (screen, terminal, or web page) is rendered to the requesting user.

Based on this design, all remote sessions honor the model of least privilege, just-in-time access, integrate with ITSM solutions, and follow a zero trust architecture for policy and administration.

The diagram below illustrates how this occurs as a part of daily operations:

Figure 3: Zero Trust Policy Enforcement



If you are considering rearchitecting, redeploying, or modernizing your remote access solutions, you can achieve zero trust using this paradigm.

Additionally, any partial implementation of this model can be an improvement in secure computing for a software-defined perimeter. This architecture is much more secure than allowing a home computer with VPN access into your environment to perform administrative functions.

3 Zero Trust Design Considerations for Secure Remote Access

Zero Trust has been developed in response to industry trends that include remote users, dissolving network perimeters, and dynamic, cloud-based assets. It focuses on protecting resources, not logical network segments, as network segmentation is no longer seen as the prime component to the security posture of the resource.

Together, zero trust and secure remote access can solve remote worker and remote session challenges and even strengthen your security posture for on-site and traveling workers.

Key considerations as you embrace this model include:

Technical Debt

If your organization develops its own software for consumption, and the applications are more than a few years old, you have technical debt. Redesigning, recoding, and redeploying internal applications can be costly and potentially disruptive. There needs to be a serious business need to undertake these types of initiatives.

Consider using zero trust and secure remote access as the mechanism for remote worker connectivity.

Adding security controls to existing applications to make them zero trust-aware is not always feasible. It is likely that your existing applications have no facilities to accommodate the connection models in the specification and are not coded to operate in a perimeterless model as specified by NIST. Therefore, depending on the architecture of your custom application, consider using zero trust and secure remote access as the mechanism for remote worker connectivity. This will allow it to be a successful add-on to your existing solution without re-engineering established systems.

Legacy Systems

Legacy applications, infrastructure, and operating systems are most certainly not zero trust-aware. They have no concept of a remote worker and rely on direct network connectivity to operate them.

Any zero trust implementation requires a layered or wrapper approach to enable legacy systems. However, a pure zero trust approach entails enveloping all resources – regardless of their location – with these concepts. You can, however, log remote session activity, record interactive screen sessions, and monitor events to look for potentially malicious behavior. This is a partial implementation of zero trust with secure remote access and may be sufficient for some environments to mitigate risks. This is an important consideration when a single remote session may actually interact with multiple systems behind the scenes that are not being managed, but represent a high value to a threat actor.

Peer-to-Peer Technologies

If you think your organization does not use peer-to-peer (P2P) networking technology, you may be unaware of the default settings in Windows 10. Starting in 2015, Windows 10 enabled a peer-to-peer technology to share Windows Updates among peer systems to save Internet bandwidth. While some organizations turn this off, others are not even aware it exists. This represents a risk of privileged lateral movement between systems that is fundamentally uncontrolled. While no vulnerabilities and exploits have materialized for this feature, it does present communications that violate the zero trust model.

If remote access sessions require protocols like ZigBee or other mesh network technology for IoT, you will find that they operate completely counter to zero trust. They require peer-to-peer communications to operate, and the trust model is based strictly on keys or passwords, with no dynamic models for authentication or modifications.

Therefore, if you decide to embrace zero trust and secure remote access, consider hardening your endpoint security model to not allow any inappropriate network communications on the same subnet as the source or destination. While there may be exceptions for devices like local printers, conceptually the perimeter stops at the device itself and remote access only controls the connection point-to-point.

4

Next Steps Toward Zero Trust

Today, we are challenged with securing significantly more remote workers than in years past—many of them working from home. A Secure Remote Access solution using a zero-trust architecture can ensure these resources are managed from potential inappropriate connection abuse and that all applications are executed within a zero trust model. This means no end users are ever trusted for a remote session unless the confidence for execution can be measured. This is true for any location an asset may reside, irrespective of the perimeter.

Additional Resources

- The Top 5 Remote Access Problems
- The Remote Access Challenge
- Give Them Access, Not a VPN
- The True Cost of Free Remote Support Software
- BeyondTrust Secure Remote Access

ABOUT SECURE REMOTE ACCESS

BeyondTrust Secure Remote Access solutions enable organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks. Users can quickly and securely access any remote system, running any platform, located anywhere, and leverage the integrated password vault to discover, onboard, and manage privileged credentials.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 78 of the Fortune 100, and a global partner network.

beyondtrust.com

V2021_03_ENG