WHITE PAPER

A ZERO TRUST APPROACH TO WINDOWS & MAC ENDPOINT SECURITY

Achieving a Zero Trust Architecture with Endpoint Privilege Management

BeyondTrust

TABLE OF CONTENTS

1

Introduction - What Is Zero Trust?

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

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 work/work-from-home has only accelerated the demise of the traditional perimeter.

Increasingly, resources that require authentication, privileges, and access may reside outside of corporate governance. This can include other untrusted resources or identities, accounts, and processes. These realities have given rise to the concept of the Data Plane, which is important to manage, and will be discussed in greater detail later in this paper.

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, 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

For the average corporate employee, elimination of local administrative rights on their corporate-issued computing device(s) is a security best practice. Unfortunately, this important security control has either not been implemented, or has been relaxed across many organizations, as remote working skyrocketed in response to the global pandemic.

The rationale behind either not removing local administrative rights or regranting these privileges has long been a source contention between information technology and information security teams. One argument for broadly provisioning these rights is the need for user flexibility, such as having the simple ability to add drivers for a local printer. The counterargument is that 56% of all critical Microsoft vulnerabilities can be mitigated simply by removing administrative privileges.

The truth is, there must be a balance. The following two goals need to operate in harmony:

- **Productivity:** End users need privileged access to operate sanctioned applications and execute system tasks.
- **Security:** The organization needs to exercise control over installation of software and execution of specific applications and tasks to reduce their threat surface.

These two goals apply whether the employee is working from a company office or any remote location and underscore the importance of a zero trust architecture for endpoint privilege management. This model can accommodate corporate office-based and work-from-home environments, while consistently achieving strict governance over authentication.

Zero Trust and Privilege Management 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 we are now performing from home that require privileged access. This runs the gamut from managing the organization's social media accounts to administrating 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.

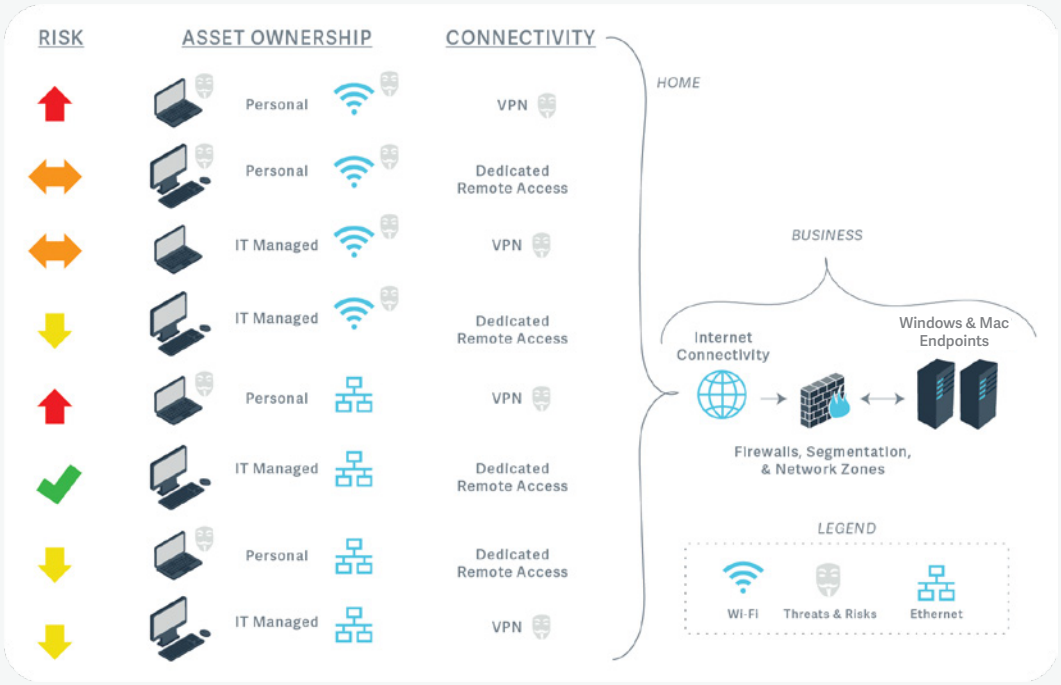
Work-from-home introduces new attack vectors and potential regulatory compliance issues that need to be resolved. For most organizations, this represents an unacceptable risk to the business, since most of their highly sensitive data and applications reside on mission-critical platforms within their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

> *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, a gap exists in managing privileges and applications when a zero trust model for least privilege and application control has not been implemented.

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. This is 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. In addition, other devices could compromise the wireless network or monitor communications. This includes privileged accounts outside of corporate governance used by home networks to interoperate and call 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 monitor privileged activity or mitigate threats at the application layer.

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** – Managing 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** – Strictly controlling privilege elevation locally and across the network and eliminating local administrative credentials and admin rights for end users.
- **Governance** – Documenting all privileged activity for compliance, including privileged user behavioral analysis.
- **Zero Trust** – Implementing a cloud-based management architecture where all privileged activity honors zero trust and strict application control is enforced. This applies the concept of zero trust with least privilege and ensures the risks can be fully mitigated by never exposing root or administrative privileges outside of the extended perimeter, nor to the end user.

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. However, a combination of zero trust, endpoint security, and IT managed devices with secure connectivity can accomplish the desired goals.

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 Windows and macOS endpoints, regardless of where they are deployed and operate from or to.

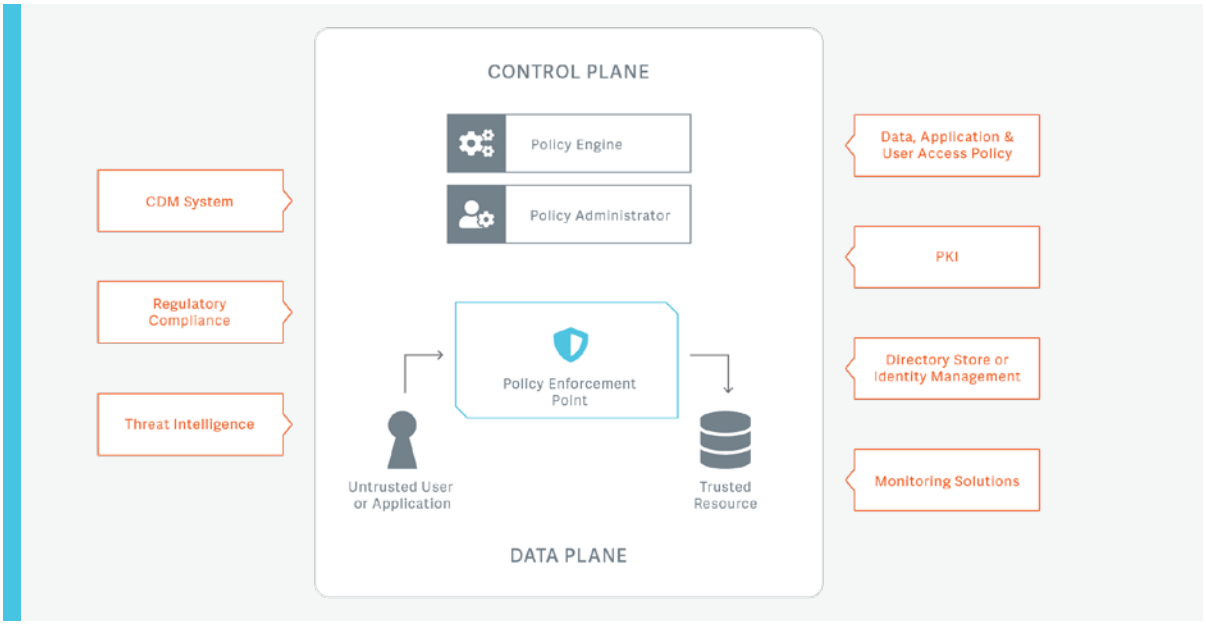
BeyondTrust Privilege Management for Windows & Mac is part of BeyondTrust's Endpoint Privilege Management solution (which also includes Privilege Management for Unix & Linux), and can help secure Windows and macOS endpoints according to zero trust. Privilege Management for Windows & Mac is a preventative endpoint security solution that removes excessive admin rights, applies modern application control, enables passwordless administration, and gives users just enough privileges to do their jobs and be productive. The solution blocks the majority of malware and ransomware and protects against both external and internal threats. Utilizing QuickStart policies, organizations receive rapid time-to-value whether deploying the solution on-premises or via Cloud.

Achieving Zero Trust, as Defined by NIST, with Endpoint Privilege Management

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 there is no implicit trust 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 endpoint privilege management solutions as follows:

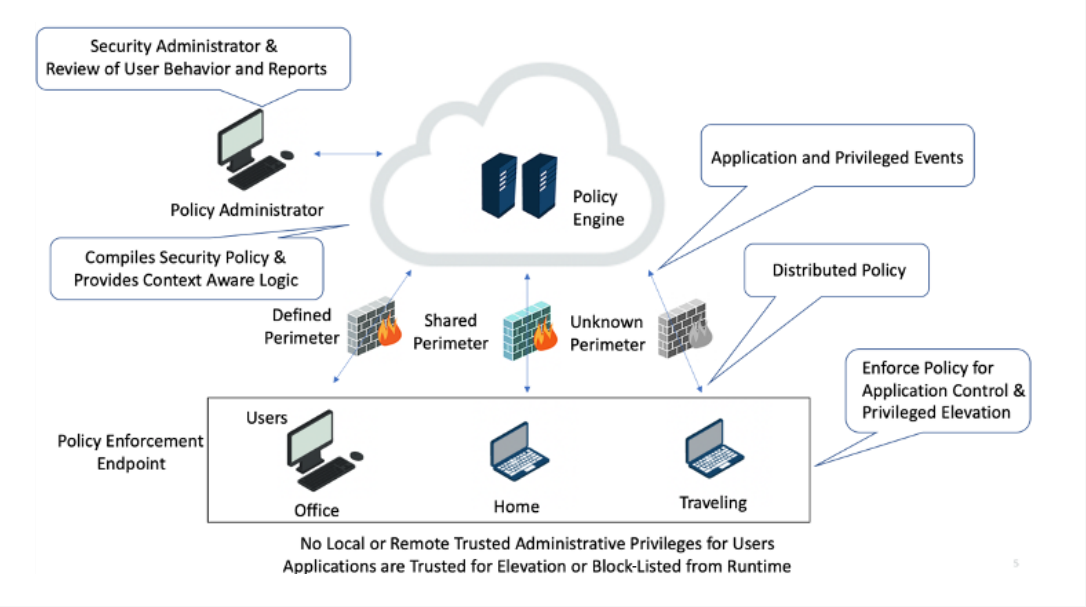
- The endpoint privilege management *Policy Engine* is responsible for the decision to grant access to a resource. Using as much data as it can based on roles, attributes, and threat intelligence to determine if access should be granted.
- The *Policy Administrator* is responsible for establishing the connection between a client and a resource. Providing 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 the trusted enterprise resource.

Here is how the above components map to BeyondTrust's Privilege Management for Windows and Mac product:

- The *Policy Engine* can be found in management capabilities of the rules, policies, and log engine governing least-privilege endpoint access, and in the role and attribute-based access models defined by the Policy Administrator. To manage assets and users, regardless of perimeter, this function can be implemented using BeyondTrust's Privilege Management for Windows & Mac.
- The Web *Policy Administrator* creates, updates, and manages the policy for end users, grants access, and automates application 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 Privilege Management Windows & Mac Interface (when deployed via the Cloud). The *Policy Enforcement Point* is the least-privilege client installed on Windows and macOs endpoints. It initiates privileged applications and performs application control on the endpoints on behalf of the user or application.

- The *Policy Enforcement Point* capability compares the application execution request to the defined policy and launches (or denies) the application with the appropriate privileges, without actually using privileged credentials. This capability is fundamental to zero trust since the application or user is never granted administrative credentials but can execute an application with privileges.

Figure 3: BeyondTrust Privilege Management for Windows & Mac Cloud Deployment.



Application privilege runtime honors the model of least privilege, just-in-time access, and follows a zero trust architecture for administration—regardless of the perimeter.

If you are considering rearchitecting, redeploying, or modernizing your endpoint security model, you can achieve zero trust for privilege elevation, least privilege, and application control using this paradigm. This model satisfies all the requirements for zero trust and allows endpoint privilege management to extend the implementation to additional security models, such as just-in-time access. 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 Windows & macOS

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 endpoint privilege management can solve privileged remote worker challenges and even strengthen your security posture for on premise 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.

Adding security controls to existing applications to make them zero trust-aware is not always feasible. Odds are, your existing applications have no facilities to accommodate the connection models in the specification, nor are 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 endpoint privilege management as the mechanism for remote worker privilege elevation, least privilege, and application control. 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 least privilege, balk at application control, and they do not possess privilege escalation models that dynamically allow for modifications based on contextual usage.

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 privileged activity, capture process launches, and monitor events to look for potentially malicious behavior. This is a partial implementation of zero trust with privileged access management and may be sufficient for some environments to mitigate remote application access risks.

Peer-to-Peer Technologies

If you think your organization does not use peer-to-peer (P2P) networking technology, you are probably 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.

There should be no unauthorized lateral movement—even within a specified microperimeter. In addition, if remote workers have 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 modifications.

Organizations seeking to embrace zero trust and privileged access management must consider hardening the endpoint security model to disallow network communications on the same subnet. While there may be exceptions for devices like local printers, conceptually, the perimeter stops at the device itself and, when modeled with privileged access management, is defined through applications and privileges.

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. By applying cloud-based privileged access management with a zero trust architecture, you can ensure your organization's resources are appropriately managed and protected from potential privilege abuse.

All executing applications can be forced to abide to a zero trust model. That is, no end users are ever trusted with privileges, and applications have no trust for execution unless the confidence for execution can be measured. This should hold true for any location where an asset may reside, irrespective of the perimeter.

To learn more about how BeyondTrust solutions can help with your zero trust projects, contact us today.

Additional Resources

- Guide to Endpoint Privilege Management
- Microsoft Vulnerabilities Report
- The 5 Critical Steps in your Endpoint Security Strategy
- How to Achieve the NIST Zero Trust Approach with Unix & Linux Remote Access
- Case Study: How The University Of Derby Secures Their Endpoints With Beyondtrust
- Demo: Privilege Management for Windows & Mac

ABOUT PRIVILEGE MANAGEMENT FOR FOR WINDOWS & MAC

BeyondTrust Privilege Management for Windows & Mac pairs powerful least privilege management and application control capabilities, delivering fast, unmatched risk-reduction potential. Grant the right privilege to the right user or application, only when needed, and create a single audit trail. Operationalize quickly with QuickStart feature and simplified deployment models for fast time-to-value and streamlined compliance.

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. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 78 of the Fortune 100, and a global partner network.

beyondtrust.com

V2021_02_ENG