Over the past year, high-profile breaches, such as the hacking attempt of a Florida water treatment facility, have highlighted the urgency to secure operational technology (OT) and non-traditional endpoints. Improving endpoint security for IoT, desktops, servers, and other devices was a high priority for Oxford. Their IT team identified the need for a solution that would allow the many vendors that serviced the buildings access to what they required, but without installing any local software or VPNs. These tools can create security gaps, especially with regards to privileged access.

**Company Snapshot**

Oxford Properties Group is a leading global real estate investor, asset manager and business builder. Part of its global portfolio includes over 50 office and residential properties in North America, where Oxford is both the owner and operator.

With the cost of cybercrime expected to exceed $6T USD globally, Oxford continues to re-evaluate and introduce measures to ensure that it can deliver a world-class cyber security platform for its managed assets.

“\nThe majority of the systems within the buildings being accessed are not traditional IT systems. They are building control systems, like smart elevators, surveillance systems and HVAC units where it is not possible to install antivirus software. We recognize that privileged access management is one of the most important tenets of a modern cyber security program and a must have for a zero-trust architecture and robust BYOD security framework.”

CURTIS JACK, MANAGER OF TECHNICAL ENGINEERING, OXFORD PROPERTIES GROUP
Why BeyondTrust

BeyondTrust was chosen for its comprehensive, cloud-based PAM platform that can streamline permissions to any users, endpoints, systems, and other assets on the network. The BeyondTrust solution also allows Oxford to leverage a consumption-based model that aligns costs against usage. The cloud-based PAM solution hardens endpoint security and enhances business agility since it does not require the vendor to install any local applications—they simply request access and can connect to the network with any internet-enabled device.

The BeyondTrust PAM platform consists of three solutions to enable Oxford’s Zero-Trust Architecture:

**Privileged Remote Access**

Enables any internal or external user (including contractors) to securely access the OT network and obtain privileged access to remote systems and endpoints (including building management systems) in a just-in-time manner. This ensures users and vendors can remotely access the network and securely complete any work that requires elevated permissions as long as they have an internet connection.

**Password Safe**

Creates a scalable process to centralize and automate privileged password and session management. Privileged credentials accessed across Oxford Properties’ assets—by employees, vendors, and even machine identities—are automatically synchronized.

**Endpoint Privilege Management**

Ensures that any legacy endpoints—including building management systems—are secure to minimize the risk of cyberattacks, including from traditional malware, ransomware, fileless threats, and other sophisticated attacks. This solution removes any excessive end-user privileges and controls applications on Windows, Mac, Unix, Linux, and network devices.
Robust Centralized Control with BeyondTrust
BeyondTrust’s PAM solutions provide Oxford the advanced digital resilience, scalability, and business agility it needs to proactively adapt and respond to emerging threats and evolving market forces. The Oxford Operational Technology team can now:

- Remove the overhead of managing a VPN for over 500 external, third parties, vendors, and remote privileged users
- Store and manage privileged account credentials in a centralized vault that leverages a policy-based framework to minimize the risk of unauthorized access
- Automate the vendor onboarding process to reduce turnaround time and administrative overhead while ensuring that no system is left unmanaged
- Provide a comprehensive audit trail that can be used for monitoring and to support any forensic investigations
- Implement a Cloud-based management architecture platform to centralize remote access across the Oxford OT network

"With BeyondTrust’s Privileged Remote Access solution, we can make sure that access to any part of our infrastructure is impossible unless we say so because we have centralized control of all the credentials needed to get access," said Jack. "We are able to enforce a policy of least privilege by giving just the right level of access needed for their role plus the ability to schedule when vendors have access to which systems and for how long. Additionally, Privileged Remote Access has enabled us to create an environment where our building managers don't have to be on site 100% of the time. A lot of the work they do can actually be done securely from a remote location, which has been an added bonus during the pandemic."

Jack and his team also appreciate the comprehensive audit trails, session forensics and other reporting features that Privileged Remote Access offers. His team can review and monitor the use of privileged accounts, capture detailed session data for real-time or post-session review and collect all the data required for regulatory compliance when it comes time for audits.

Password Safe helps Oxford reduce the risks associated with privileged credential compromise by safeguarding access to privileged account passwords, secrets, and SSH Keys. "This is the first time we have ever implemented a security product that made the end user's job so much easier. Our building managers previously managed dozens of different credentials for staff and vendors. Password Safe centrally manages every credential, so they now have only one password for them, one password for vendors and one password for their staff," said Jack

Up Next: Implementing Endpoint Privilege Management
Mahmoud Abdelsalam, Cybersecurity Architect at Oxford, is working with BeyondTrust to further mature their PAM implementation by layering on BeyondTrust Endpoint Privilege Management to seamlessly elevate, manage, and control privileged access across all endpoints.

"Our goal is to have a zero trust security approach to ensure all access to our buildings and its systems is fully managed and documented," said Abdelsalam. "Being able to employ Endpoint Privilege Management from the cloud will give us the additional agility, flexibility, and scalability to eliminate unnecessary privilege across a variety of operating systems in a controlled way, while also better managing and securing the privileged access that is needed."