BeyondTrust

CASE STUDY

Los Angeles Department of Water and Power Boosts Productivity with Endpoint Privilege Management

Roger Boden, Systems Programmer III, and Joseph Cundiff, Systems Programmer II,
with the Los Angeles Department of Water & Power

LA DWP Los Angeles Department of Water & Power

Product: Endpoint Privilege Management
Company Size: 11,500 employees
Company: Los Angeles Department of Water and Power

The Los Angeles Department of Water and Power, the largest municipal water and power utility in the nation, was established more than 100 years ago to deliver reliable, safe water and electricity to 4 million residents and businesses in Los Angeles.

The Los Angeles Department of Water and Power (LADWP) is the nation's largest municipal water and power utility, in charge of delivering safe, reliable services to four million residents and businesses. Behind the scenes, LADWP's IT team knows their work is just as critical as the pipes and wires. A disruption caused by a single gap in security could ripple through millions of customers. At the same time, employees across the department, from engineers in the field to clerical staff in the office, all need systems that enable them to work without interruption.

For the department's system programmers Roger Boden and Joseph Cundiff, finding the right balance between safety and productivity became unsustainable. Local admin rights spread unchecked, configurations varied, and many users held permissions far beyond what their jobs required. To protect the city's lifeline, the team needed a consistent way to reduce risk while keeping everyday operations moving.

“We’re trying to achieve a balance between security, usability, and productivity,” said Systems Programmer III, Roger Boden.

For Boden’s Service Desk Endpoint Management team, finding that balance was a tall order. They support everyone at the utility, from executives and clerical staff to IT engineers and field technicians, and part of their jobs is to keep daily operations running smoothly. But because critical infrastructure is a top target for attackers, the LADWP also knew that it needed to be prepared with strong endpoint security controls.

“It’s not ‘if,’ but ‘when’ the bad actors are going to try something,” said Systems Programmer, Joseph Cundiff.

Addressing the weakest link

The Endpoint Management team first wanted to address the significant risks associated with user behaviors. Limiting a user’s range of permissions to only what they need by implementing the principle of least privilege was the clear way forward.

> “We risk users being the weakest link if we don’t have a way to enforce and manage least privilege. We have to eliminate that risk.”
>
> **Roger Boden | Systems Programmer III, Los Angeles Department of Water and Power**

But as the team started to scale the utility’s least-privilege rules and worked to eliminate local admin rights, inconsistencies emerged and field technicians found they had to jump through hoops just to do their jobs.

“They would have to call in, connect to the network, and have someone install software for them that they had rights to before,” Cundiff said. These roadblocks interrupted workflows and delayed help for LADWP customers.

Meanwhile, the new rules led to 400–500 calls every day for the service desk. This volume made it hard for Cundiff and his colleagues to prioritize their efforts, and they also lacked visibility into which employees were still using outdated software.

LADWP's compliance requirements were another important consideration. The need for an audit trail added a sense of urgency to the task of finding a solution that balanced least privilege with productivity. The team needed a plan to address compliance requirements such as the North American Electric Reliability Corporation's Critical Infrastructure Protection (CIP) standards.

Out-of-the-box functionality with a painless implementation

As the LADWP surveyed the options, they discovered that while most endpoint privilege management solutions offered account-based elevation, which still poses security risks, BeyondTrust's Endpoint Privilege Management (EPM) product leveraged process-based token elevation, which only grants privileges to approved applications or tasks—not the user itself. "It was a more secure, more scalable solution as a result," Boden said.

The token elevation functionality was a key factor in the department's decision to transition away from its legacy solution. With EPM, administrators can create custom tokens within the BeyondTrust policy editor that define specific sets of permissions. This token elevation process offers granular access control by allowing organizations to assign policies to specific applications or users, streamline privilege configuration with customizable "workstyles", and enforce just-in-time access by granting elevated privileges only when needed.

Another deciding factor in EPM's favor was the ease of migration. The Endpoint Management team wanted to maintain a consistent user experience throughout any transition—no small consideration at an organization with more than 10,000 machines. Not only did EPM provide a streamlined migration of existing rules, but it also offered out-of-the-box functionality so the LADWP team could enjoy the product's benefits immediately.

"The forethought was evident in the design of the product," Boden said. "Specifically, the workstyles, flexible tiers, and the range of administrative actions anticipated out of the box."

Additionally, LADWP needed a solution that aligned with Critical Infrastructure Protection (CIP) standards, which are mandatory cybersecurity requirements for electric utilities. BeyondTrust EPM stood out for its ability to support compliance by helping identify critical assets, enforce granular access controls, train personnel, and maintain detailed audit trails to ensure the reliability and security of the power grid.

By integrating EPM with LADWP's existing vulnerability management tools, the team could also reduce risk on two fronts: by controlling what enters the environment, and by continually scanning for new threats.

"We began with the workstation and secured it in a number of ways, using least privilege to minimize the ingress of bad actors. And then we have the perimeter and all other means to protect the environment," said Cundiff.

After reviewing the range of user permissions, LADWP tested BeyondTrust's EPM solution and concluded it was the best fit. The team scheduled the migration to coincide with another update in an effort to minimize the impact on users. Even so, Boden was impressed by how few issues arose and how easy they were to resolve. "There was no headache, no pain of migration," he said.

"The automation really helped us ramp up and start getting more things done," Cundiff added.

Strengthening security, enabling productivity

Since adopting Endpoint Privilege Management, LADWP is substantially more secure and experiences far fewer security incidents.

"BeyondTrust Endpoint Privilege Management has allowed users to continue doing what they need to without IT providing carte blanche admin rights," Boden said.

By standardizing configurations based on user roles, LADWP has eliminated inconsistencies and reduced ad hoc user requests. This role-based approach to least privilege ensures users have the access they need to do their jobs, while also minimizing the attack surface and limiting lateral movement in the event of a breach.

EPM's robust auditing capabilities helped the Endpoint Management team standardize software versions, reducing vulnerabilities and ensuring compliance with a clear audit trail. The tool's challenge-response authorization added another layer of control, giving the team greater oversight and accountability.

As for the service desk, daily interactions have dropped 42%—from 450–500 to 250–300 daily interactions. No longer inundated with requests, the team can now better prioritize their efforts, and overtime hours have been cut in half.

All of this has had a very positive effect on both users and LADWP customers.

"Now the workflow actually flows. There's no break in day-to-day operations to ask for permissions. Our customers are happy, their customers are happy, and it's a good day."

Joseph Cundiff | Systems Programmer II, LADWP

A better experience for users and support teams

In addition to the measurable benefits, BeyondTrust's EPM solution has given the Endpoint Management team real peace of mind, representing a significant shift in LADWP's security culture. "We've empowered users while adopting a culture of least privilege," Boden said. "Hand-in-hand with cybersecurity awareness, it contributes to a security-by-design mindset."

"We've empowered users while adopting a culture of least privilege. Hand-in-hand with cybersecurity awareness, it contributes to a security-by-design mindset."

Roger Boden | Systems Programmer III, LADWP

Ongoing product education is key, with the BeyondTrust team keeping LADWP up-to-date with the latest security information. "The product is intuitive, granular, and reliable, but I've been most impressed with BeyondTrust's employees," Boden said.

Best practices shared via monthly meetings with BeyondTrust's Customer Success team, as well as self-service tips provided by BeeKeepers, BeyondTrust's online customer & partner community, keep the LADWP team on the ball.

With BeyondTrust EPM in place, security at LADWP is no longer seen as a barrier but rather a strategic enabler. The department has transformed privilege management from a point of friction into a force multiplier, protecting critical infrastructure while empowering users to work efficiently and securely. By minimizing risk and limiting the blast radius of potential attacks, LADWP has redefined what modern cyber defense looks like: proactive, precise, and built for the future.

Learn more about BeyondTrust's public sector solutions at beyondtrust.com/public-sector.
