BeyondTrust

CASE STUDY:

GLOBAL SOFTWARE DEVELOPER

CONTROLLED ADMIN PRIVILEGES ACROSS 5,000 USER ENDPOINTS

Company: Global enterprise technology organization

Location: Hoboken, NJ

Size: 6,000+ Employees

Product: Endpoint Privilege Management

Platform: Windows

Company Snapshot

A global software development corporation delivering cloud-based and on-premise software solutions for clients in industries that range from financial services to manufacturing, law enforcement, aviation, and more.

Use Case – Meet Compliance Mandates

As part of the vendor management program of a large customer within the banking sector, an annual onsite audit identified a risk in relation to endpoint privileges. To mitigate the risk and improve the overall security posture, the bank required that the software supplier take action to implement a means of controlling excessive administrative privileges across approximately 5,000 user endpoints. With such a large number of users in varying roles, it would take months, or even years, to identify and audit all the applications running on endpoints and their associated access privilege requirements using existing tools and processes. However, the software developer committed to a timeline of only three months to implement and deploy an effective and secure solution.

"Some of our larger, strategic customers perform onsite audits covering different areas, such as human resources, physical security, access management, and security training. One of the gaps identified was in relation to excessive administrative privileges on our endpoints. It was an area that needed to be addressed."

RICHARD, SECURITY MANAGER

Why Beyondtrust

Although the software development company considered working with native tools within its organization, they ultimately decided to install the BeyondTrust Endpoint Privileged Management (EPM) product. Its speed of implementation was a key factor in the decision, along with the need to find a solution that could control access privilege—without disrupting the day-to-day work of its many users (endpoints).

The company assessed five of the leading EPM offerings, including products from Ivanti, Thycotic, and CyberArk, but opted for BeyondTrust's EPM solution due to its Quick Start policy, rapid deployment capabilities, ease-of-use and the fact that access privileges could be set at low, medium, and high flexibility levels, allowing developers to access and use the programs and applications they need to do their work.

CASE STUDY: GLOBAL SOFTWARE DEVELOPER

Implementing Beyondtrust Endpoint Privilege Management

As a global software developer, the company needed a solution that could be quickly installed and deployed—without disrupting the operations of a broad network of endpoints. Additionally, it was important to allow their sophisticated technical users enough leeway in accessing the programs and applications that they required for their work.

- **RAPID DEPLOYMENT:** Easy deployment allows for a straightforward implementation process with no new hardware required.
- **LOW, MEDIUM & HIGH FLEXIBILITY:** The options available accommodate the varying requirements of sophisticated users at the endpoint. Rather than auditing and assessing individual workstations, skilled users can be a granted high flexibility workstyle.
- **WHITELISTING CAPABILITIES:** The company can designate approval of select, trusted programs and applications without user interaction. Similarly, inappropriate or questionable sources can be blacklisted.
- **AUDITING & REPORTING:** Provide a single audit trail of all user activity, speed forensics and simplify compliance with complete reporting for multiple stakeholders.

Success With Beyondtrust

With the urgency to roll out the EPM solution, the company proceeded in planned phases, implementing the system in an initial pilot to developers in the U.K. Some of the developers were initially reluctant to accept the idea of removing administrative privileges, but their acceptance was quickly won over once BeyondTrust's EPM proved to be frictionless. Additionally, the pilot deployment uncovered several potential issues the company was able to eliminate by tweaking its policies. This served them well as they continued rolling out to other groups around the world, with successful adoption across the board.

Beyond Today

BeyondTrust's EPM auditing capabilities initially revealed some 30,000+ different applications being run on endpoints in the company's global network. In the months since its deployment, Endpoint Privilege Management has identified many of the key programs that are in use regularly and productively at endpoint workstations, making it possible to begin whitelisting approved software and elevating privileges when required. As this auditing process continues, the company is also considering creating a blacklist of applications to identify those that may pose a threat to the broader network so it may immediately block them.

"We did an extensive review of the different offerings in the endpoint privilege management space and BeyondTrust's Endpoint Privileged Management was the clear winner. We didn't have to do any training with the software itself, and we were able to roll it out quickly with minimal impact on our users. BeyondTrust's EPM solution is definitely a strong player in this space."

RICHARD, SECURITY MANAGER

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering companies to secure and manage their entire universe of privileges. 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.

beyondtrust.com

V2020_02_ENG