BeyondTrust

Embracing Technical & Business Leadership to Bolster Enterprise-Wide Security

BY JEFF LUNDBURG
PRINCIPAL CONSULTANT AT MASADA CYBER SECURITY

Jeff Lundburg is an experienced information security leader focused on Privileged Access Management (PAM), Directory Services, Identity and Access Governance (IAG), and UNIX/Linux security.

Cyber threats are lurking around every corner. Securing your organization's infrastructure can overwhelm you if you don't take the right precautions. But where do you begin? Whether it's criminals infecting your network with ransomware to exact a price, hacktivists making a political statement, careless mistakes by insiders, or ethical hackers raising awareness of best practices by compromising poorly defended infrastructure, you're a target.

But what if you could protect yourself from 90% of these threats with one solution? In my opinion, that's what you get with Privileged Access Management (PAM), a flattened approach to cyber security that strips away layers of complexity by simplifying and centralizing the way you grant permissions to your IT assets.

SAY YES TO PAM

Too many companies take a lax approach to cybersecurity. Some think they'll never be breached. Others worry it's too expensive, and it will slow down their operations workflows or project deliveries. Resistance to change associated with additional security controls and monitoring is common. Various organizations disagree with the need to adopt better controls. Whether it's systems administrators, developers, network engineers, security teams, or budget owners—each can be focused on their immediate priorities while the entire company is at risk.

Another hurdle is integration. You're often dealing with third-party apps, in-house customizations and software, on-site operating systems like UNIX, Linux, Windows, and OSX, and off-prem cloud-based apps that run on AWS and Google Cloud. The pace of change is greater than ever.

There seem to be many reasons to say no to robust cybersecurity, but you need to say yes. There are endless rabbit holes, and you have to look beyond these distractions. You can find a place for asset and vulnerability management and behavioral analytics in your cybersecurity toolbox, but you have to start with the basics. The biggest bang for your buck is PAM.

BeyondTrust

> You can find a place for asset and vulnerability management and behavioral analytics in your cybersecurity toolbox, but you have to start with the basics. The biggest bang for your buck is PAM.

A FORTUNE 100 SUCCESS STORY

I could tell you the benefits of PAM, but instead, I'll show you what happened at my previous role in a Fortune 100 financial services company that adopted this approach to cybersecurity. We're talking a major player with over 90,000 people (employees, contractors), more than 50,000 servers, and over 80,000 end-user workstations.

t started in 2007. I'd worked with the company in various roles since the mid-1990s as a contractor and as an employee. At the time, I was working for a third-party services provider that operated the majority of the company's data center resources.

That year, an audit revealed they weren't adequately logging privileged activities on their critical systems. So, they started looking at the various solutions on the market. IT leadership at the time decided to acquire Symark's PowerBroker as a solution. In 2008, I accepted an employee position in the company's IT security group. Same parking lot, different badge color. That first year, my focus was deploying a host-based access control platform on Windows and Linux servers, and later evaluating enterprise password management solutions in the marketplace.

Over the next two years, PowerBroker was deployed in the enterprise by our third-party services partner with limited results. By 2010, we made the decision to take operational ownership of the PowerBroker platform back in-house. We aggressively expanded the coverage throughout the enterprise, remapped all local "sudo" rules to PowerBroker policy, and implemented an RBAC (role-based access control) policy model that would scale in the enterprise.

In 2011, Symark had acquired BeyondTrust, adopted its name, and added the former competitor's Windows security applications to its portfolio of products. The company acquired the PowerBroker for Windows solution in 2014 and rapidly deployed it throughout the enterprise, dramatically reducing risks associated with administrator entitlements on these systems. We now had available to us a workable mixed-environment PAM solution that fit our needs.

Here's where it got interesting. When we started our journey, some of the products we needed didn't exist, and my team didn't have the budget we'd hoped for. But we did have a vision and a clear idea of where we wanted to go.

It's important to think strategically and you have to think ahead. The solution to the problem you're having now might be three years away, but when it's finally available, you should have already secured management buy-in and set up the building blocks. Only then will you be ready to implement it.

SETTING UP THE LONG GAME

To lay the groundwork for the adoption of a solution like PAM, you need an enterprise-level vision and a capable engineering team that can set aside the old way of doing things when something better comes along. With the right mindset, anything is possible. But your security team needs to focus on three key elements: reducing risk, improving the user experience, and driving operational efficiencies (bang for your buck).

BeyondTrust offers all of the above. As I said earlier, using a PAM platform to manage permissions and passwords eliminates probably 90% of your security risks. It also reduces complexity and eliminates many redundancies, thus lowering costs and streamlining the user experience.

BeyondTrust

> To lay the groundwork for the adoption of a solution like PAM, you need an enterprise-level vision and a capable engineering team that can set aside the old way of doing things when something better comes along. With the right mindset, anything is possible. But your security team needs to focus on three key elements: reducing risk, improving the user experience, and driving operational efficiencies (bang for your buck). BeyondTrust offers all of the above.

When you're managing privilege at the server and application level, you're dealing with too many points of administration. BeyondTrust's Endpoint Privilege Management integrates with Active Directory to create a single touchpoint for managing privilege and access permissions. Instead of having hundreds of administrators dealing with segments of your network, or even with individual machines, you have a few people doing everything consistently across the enterprise.

This approach reflects industry best practices. When you look at a juggernaut like Facebook, it's astounding to realize that their ratio of servers to admins is something like 30,000:1. But when you think about that figure, it makes perfect sense. A single administrator can manage this scale with good enterprise-class tools and practices.

It took about eight years to reach full enterprise coverage, but thanks to my team's vision, this financial services giant greatly improved its cybersecurity posture. We also leveraged BeyondTrust's Active Directory Bridge, which allowed us to integrate our UNIX/Linux PowerBroker policy with our directory and Identity and Access Governance platforms in ways that enhanced innovation and reduced delivery time of new security enhancements.

Effective PAM tools not only provide real-time preventative protection, but they also provide valuable data, including session, keystroke, and activity logs. This information can be leveraged using AI and advanced analytics to enhance security further, improve network performance, optimize applications, and increase overall efficiencies. They are also well-positioned to secure cloud-based and other off-prem systems and applications. Identity and Access Management organizations are heavily audited today and modern enterprise-class PAM tools help ease that burden.

ALL GOOD THINGS

But all good things must come to an end. At the end of 2019, I decided to strike out on my own again. I needed to exercise my entrepreneurial muscles, and I wanted to bring PAM to organizations to not only reduce risk, but also enhance business effectiveness.

I believe there is demand in the marketplace for smaller organizations that don't have the resources to implement traditional PAM solutions. I'm talking small and medium-sized businesses, municipal government agencies, and educational institutions that don't have the staff to properly protect their IT assets.

These organizations struggle to afford the software necessary to fight these threats, not to mention the difficulty in recruiting and retaining the cybersecurity talent required to operate the tools. Yet they are increasingly being attacked. They need cloud-based solutions that are easy to consume, affordable, and very secure.

I am very excited to be integrating BeyondTrust products with this new clientele because the company has been offering a single-vendor cybersecurity suite for over a decade. Conglomerates and multinationals can afford to deploy multi-vendor environments. They have the luxury of integrating solutions from diverse sources and coding bespoke solutions in-house. Growing businesses, not-for-profits, educational institutions, and mom-and-pop shops don't have the resources to deal with such levels of complexity.

I'm hoping to level the playing field, and I'm also exploring the possibility of providing scalable managed services and cloud-based solutions to my new clients with my new firm, Masada Cyber Security.

BeyondTrust

> BeyondTrust's Endpoint Privilege Management integrates with Active Directory to create a single touchpoint for managing privilege and access permissions. Instead of having hundreds of administrators dealing with segments of your network, or even with individual machines, you have a few people doing everything consistently across the enterprise.

THE CAT'S OUT OF THE BAG

I'd like to loop back to the start by repeating that Privileged Access Management can solve 90% of an organization's cybersecurity issues, but relatively few organizations have adopted this approach. Fortunately, the IT landscape is changing. In December 2018, Gartner published its first Magic Quadrant for PAM, and BeyondTrust was named a leader.

The report showed that the use of PAM tools is on the rise. By 2021, the number of organizations that employ formal change management practices and DevOps environments will rise to 40% and 50% respectively. That's a massive increase. It looks like the rest of the IT industry is finally discovering the secret tool some of us have been using for the last ten or twelve years.

I remember seeing someone from Anthem speak at a conference after their breach. He finished his presentation with something that stuck with me. He said, "Whatever you'd do after you're breached—do that before you're breached." I don't think there's much better advice than that. So the question becomes: Why aren't you?

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 70 percent of the Fortune 500, and a global partner network.

beyondtrust.com