The Balance of Flexibility and Security with BeyondTrust

BY DAN BARTLETT
SENIOR CONSULTANT AT RAMBOLL

Dan is located in the UK and has more than 20 years' experience in information technology, including system administration and IT security.

In today's competitive business environment, mergers and acquisitions are the fastest way to add capacity, expertise, and new products to your company's portfolio. But these ventures are not without their challenges.

Even companies with similar commercial interests may have wildly divergent cultures and IT policies in place, and getting everyone on the same page takes some effort. It's tough enough to do this when you're aligning the processes and procedures of two companies, but the difficulty and complexity increases as mergers occur between dozens of entities around the world.

AN ETHICAL BUSINESS WITH A HUMAN DIMENSION

Ramboll is a Danish engineering, architecture, design, and consultancy firm based in Copenhagen. Engineers Børge Johannes Rambøll and Johan Georg Hannemann founded the company in 1945 on the roof of Danish Technical University, overlooking the ruins of the bombed city at the end of World War II.

The duo felt compelled to help rebuild and develop society with an emphasis on treating their clients and employees fairly. From the start, it was an ethical business with a human element. All these years later, these values of openness and inclusiveness informed the company's international expansion.

A tradition of innovation and mergers fuelled our growth into a truly global organisation. We now employ 16,500 people in 35 countries in Northern Europe, the UK, North America, and the Asia-Pacific region. Our spheres of activity have grown to encompass transportation, urban planning, water, energy, climate and sustainability, the environment, and health.

THE AFTERMATH OF MANY MERGERS

I myself came into the Ramboll fold through a merger. At first, I provided general technical support as I had before the acquisition, but I then moved to our client technology services (CTS) department. I handled client devices and Ramboll's Microsoft Windows deployment, including System Center Configuration Manager. We were piloting app locker and other security measures when the person in charge of the project left the company, and I was asked to take over.

On the whole, IT was not Global and non-standardised. We had a huge applications count including 32 different tools just doing PDF. Every country handled access privileges and admin rights differently, too. Some of our offices prevented users from installing anything at all, while others allowed them to install anything they wanted.

The result was an ongoing problem. Local IT teams were overburdened with basic maintenance tasks and our IT security teams lacked visibility and control at the global level. There was no way to ensure that our people had access to the tools and assets they needed without compromising our infrastructure or our data and ensuring license compliance, along with software standardisation.

We were also the target of cyberattacks over the years. We obviously wanted to find solutions to prevent future incidents, and gaining control of admin rights was a key phase in this.

BOLSTERING COMPANY-WIDE SECURITY

To counter these deficiencies, we decided to bolster and standardise application control and privileged management across our entire organisation. When I arrived, we had already chosen to move forward with BeyondTrust. We purchased our licenses in December 2017, and then embarked on a year-long discovery phase to integrate the platform into our everyday activities and create a full suite of policies and procedures governing its use.

Before we started to implement BeyondTrust, we audited users and administrators worldwide. We wanted to see what apps were used, how they were installed and we needed a consistent set of policies and procedures across all our locations.

That meant some users would lose some access rights while others would gain them. That ruffled a few feathers, but we won over employees who had no permissions in the past by explaining that hundreds of installs could be now done by the user direct - they could update their browser or install a media player without going through IT support. We then showed IT managers who did everything locally how a scattered approach to application control and access management was hurting Ramboll's bottom line. There was too much downtime, hackers were a real threat, and vendors had issues because we had failed to manage software licenses.

A CULTURAL & TECHNOLOGICAL TRANSFORMATION

When we rolled out BeyondTrust, we went region by region, starting with the smaller countries, working with smaller sample sizes, finding any problems and fixing them. We then took what we learned and rolled it out to the next biggest office. This approach meant as each office/region was rolled out we had already addressed some of the problems they may have seen.

“

When we rolled out BeyondTrust, we went region by region, starting with the smaller countries, working with smaller sample sizes, finding any problems and fixing them. We then took what we learned and rolled it out to the next biggest office. This approach meant as each office/region was rolled out we had already addressed some of the problems they may have seen.

“

Later on we introduced BeyondTrust’s Trusted Application Protection capability, which is part of their Endpoint Privilege Management solution. This powerful feature protects us against fileless threats that use approved applications to slip by our defenses.

The smooth rollout was largely due to the time we spent working with an implementation specialist at BeyondTrust to not only help with adoption, but also sort out application permissions. We created four different lists: White, black, grey, and red.

Everyone has access to install applications on the white list, and no one has permission to use blacklisted applications. The grey list consists of applications collected during the audit phase and pending review. When somebody tries to install one of these applications, a pop-up asks them whether they’re sure they want to install it. If they click “yes,” we let them do it, but we reserve the right to block them if our security analysis suggests the application is dangerous and we constantly review the grey list and move those applications to the other permanent lists, it bought us some time and allowed us to begin the rollout.

We also have a theoretical red list for unknown apps. Should a user try to install something that isn’t on any of our lists, a pop-up appears asking for user credentials., and they have to contact IT to approve the app in question.

Using these lists, we have whittled down the number of apps in use. We started with 8,800 items on our grey list. It’s down to 3,000, while our white list is close to 2,000 apps. When you consider that we started seeing 32,000 unique apps (including different versions) worldwide, we’re looking at a substantial reduction in vectors for malware and cyberattacks. We have also consolidated many of our business tools, which has further simplified the work of our IT teams.

Later on we introduced BeyondTrust’s Trusted Application Protection capability, which is part of their Endpoint Privilege Management solution. This powerful feature protects us against fileless threats that use approved applications to slip by our defenses. It inspects processes like JavaScript calls in browsers, phishing scripts in emails, and macros in Microsoft Word and Excel. Instead of blocking these critical applications, it scans for malicious payloads and prevents them from launching. In this way, we can protect our users without curbing their access to everyday tools. We again took a slow and measured approach to this rollout.

All of this required support not just from management, but from all of our IT leads. I spoke with all of our team leads and personally trained our support desk teams. I didn’t send out faceless emails, which often get ignored. Instead, I picked up the phone and spent a lot of time talking to people about BeyondTrust, showing them how it worked, and explaining its benefits. Getting our IT people to buy into the platform required a personal touch.

FLEXIBILITY IS KEY

The platform allows up to 10 user profiles, but we granted all our employees the permissions they need with two profiles. The most restrictive profile applies to 95% of our users and grants them access to the applications they need for their day-to-day work. The second profile has high flexibility for power users (internal developers/programmers outside of direct IT) who require privileges typically reserved for our IT team. They can do 90% of what admins are allowed, but they can’t touch security features like firewall disable and malware protection, bypass security measures etc.

As much as we wanted to shore up our security, we understood that we have to be flexible. To this end, we built a ticketing system that allows IT leads and other managers to request access to features and applications that are prohibited or not on

"

BeyondTrust provides a powerful platform that allows us to streamline and standardise application control and privileged management across our entire organisation. We have successfully deployed a comprehensive and comprehensible solution that protects Ramboll's IT assets and empowers users to make informed decisions about the apps they use. Our people are smarter and better protected, and that's great news for our business.

any of our lists. They have to present a business case and provide a list of users and the access privileges they need. Once they've filed their application, I review their request and we discuss their needs and any risks these might entail.

ENHANCING SAFETY WHILE EMPOWERING USERS

People can be reluctant to relinquish control over their permissions, but BeyondTrust Privileged Access Management is now ingrained in Ramboll's culture. Users understand how it works and what's at stake. They know when to ask for expanded permissions. For example we may have certain apps or control applets which we can allow users to update/edit themselves. We can also create custom scripts for certain tasks which we can ensure run with the right permissions, and it allows users to carry out certain tasks without having IT support taking control to do that.

When COVID hit, everyone flocked to Zoom, but the platform had major security issues, and we blocked it in less than an hour. Unfortunately, it was the only way some of our people could work with certain clients. We needed to grant Zoom access to this tiny subset of our workforce, and BeyondTrust is granular enough that we could permit this specific usage to selected users and then build an approval flow within our ticket system.

BeyondTrust provides a powerful platform that allows us to streamline and standardise application control and privileged management across our entire organisation. We have successfully deployed a comprehensive and comprehensible solution that protects Ramboll's IT assets and empowers users to make informed decisions about the apps they use. Our people are smarter and better protected, and that's great news for our business.

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