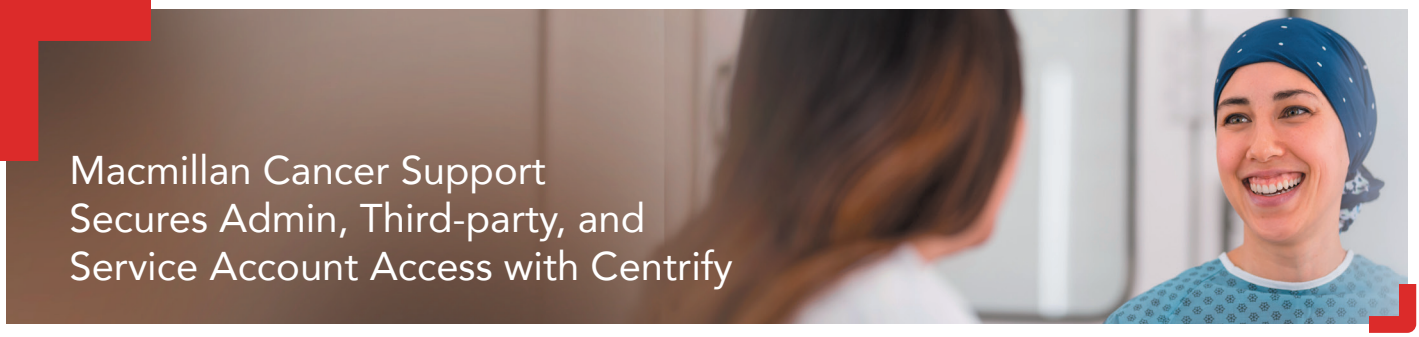

Macmillan Cancer Support Secures Admin, Third-party, and Service Account Access with Centrify

Founded in 1911, London-based Macmillan Cancer Support is one of the largest charities in the UK. The organization hosts several high-profile fundraising events, including World's Biggest Coffee Morning, Brave the Shave, and Go Sober for October. Proceeds are used to provide practical, medical, financial, and emotional support for people affected by cancer.

THE CHALLENGE

Macmillan Cancer Support has been serving the people of the UK for over a hundred years. Recently, the organization launched an initiative focused on protecting itself, its employees, and the public it serves. As part of that initiative, they hired security expert Tim O'Neill, who was tasked with building a team and maturing the security function into a proper department.

O'Neill wasted no time getting started. "The first thing I did was hack the organization to analyze its weaknesses," says the company's head of Information Security. "I found that a lot of work had been done: their policies were up to date, and they had a comprehensive training structure in place. They'd accomplished a lot, but some best practices were lacking."

"There was a domain administrator account called 'administrator,' and people didn't seem to realize the risk associated with that. There were 450 admin accounts and 8,000 Microsoft® Active Directory accounts for just over 2,300 users. Furthermore, the environment had no multi-factor authentication."

> "We needed a solution that could automate the management of our service accounts and also provide secure — but appropriately limited — third-party access to systems."
>
> **TIM O'NEILL**
> ***Head of Information Security, Macmillan Cancer Support***

O'Neill's next step was to prioritize the risks. "We lacked the ability to see when a person logged on, what device they were using, what location they logged on from, who logged on from two devices simultaneously — each of these things added another element of risk," he says. "These red flags made identity management and access rights our top priority."

Because the organization collects no patient data, there was no need to adhere to patient protection regulations, but they had yet to achieve compliance with PCI and ISO 27001 security standards. Also, as a common element of these and many other standards, access to the environment by third parties was not properly secure. Once third-party users were in the system, they were given too much freedom to move around the environment.

Finally, service accounts had become a management headache. "If you manually manage each service account, you'll eventually fail due to the amount of time and resources required," says O'Neill. "We needed a solution that could automate the management of our service accounts and also provide secure — but appropriately limited — third-party access to systems."

THE SOLUTION

As a charity, Macmillan is very aware of the fact that money spent on IT roles is money not being used to help someone dealing with cancer. Every penny counts. But that doesn't mean they went looking for the least expensive solution on the market.

"Our goal is to keep the team small, and we do that by selecting the best products," says O'Neill. "That makes ease of use essential. We look for tools that are easy to navigate, easy on the eyes, and that help you to get in, get the job done quickly, and move onto the next task."

In terms of functionality, the company identified their top three required features. The product would need to:

- Control all critical accounts.
- Provide secure third-party access.
- Help identify and manage high-risk service accounts that often had administrative rights and passwords that never expired.

"I was also looking for complementary features that would help deliver a return on the investment," he says. "We wanted a product that could mitigate as many risks as possible."

The team evaluated a handful of privileged access management (PAM) and identity management products. "Some solutions we evaluated were good at PAM, but didn't address third-party access. Others had so many offshoot features that they felt complex and difficult to manage. Centrify provided both PAM and third-party access, and its complementary features were logical and beneficial," he says.

> "Centrify provided both PAM and third-party access, and its complementary features were logical and beneficial."
>
> TIM O'NEILL
> *Head of Information Security, Macmillan Cancer Support*

The final consideration was the relationship with the organization. "We wanted to work with a highly responsive security vendor that would help us improve our security posture without having to rethink our processes, or to work in a way that wasn't natural to the organization," says O'Neill.

"While I was already somewhat familiar with Centrify, I wasn't sure it had maintained its best-of-breed status," he says. "I also wanted to ensure it was right for this environment."

During the evaluation, Centrify met every key requirement. "A short time after receiving the Centrify POC, I saw how we could provide secure, remote access for third-parties. They could log in and get access to systems they were authorized to use, but they couldn't move laterally, were time limited, and their actions were recorded," he says. "In no time, I had a list of every service account on our domain, and could test service account credential rotation. We found that Centrify delivered the biggest bang for the buck."

> "In no time, I had a list of every service account on our domain, and could test service account credential rotation. We found that Centrify delivered the biggest bang for the buck."
>
> TIM O'NEILL
> *Head of Information Security, Macmillan Cancer Support*

THE RESULTS

O'Neill's team began by addressing the most critical risks. "As soon as Centrify was installed, we started using it as a vault to safely store credentials and automatically rotate passwords. That one step tightened access, improved our security posture and provided immediate value. From there, we could define the parameters of who needed access to what," says O'Neill.

The next step was addressing the risks associated with third-party access. "Third parties often come in to fix issues, so they may need access all over the network," he says. "But you have to be careful because bad actors often use third-party access to mount attacks. With Centrify, third-party users don't even know what their access credentials are, and their actions are monitored."

Before Centrify, setting up and managing third-party accounts was a time-consuming process. Now, they're up and running in minutes, with multi-factor authentication providing an additional layer of protection. Third parties are granted access only to specific machines, for a limited amount of time, and their activities are recorded.

Rather than use a jump host, Centrify places the user surgically on the target system while the workstation remains unattached. That provides no exposure to the broader network and prevents the user from moving around laterally. It further leaves no chance of a virus or malware spreading to the internal systems, and it removes the need for NAC tools to guarantee workstation compliance with company protocols.

"The Centrify approach saves us time, money and resources. By moving from VPN-based third-party access to Centrify, we even eliminated the expense of VPN licenses," says O'Neill.

> "The Centrify approach saves us time, money and resources. By moving from VPN-based third-party access to Centrify, we even eliminated the expense of VPN licenses."
>
> TIM O'NEILL
> *Head of Information Security, Macmillan Cancer Support*

In fact, cost savings over several areas have helped the company achieve an ROI. "As with third-party accounts, managing service accounts manually is labor intensive and costly. By automating, we've reduced those expenses as well," he says. "I anticipate further cost, time and resource savings once we integrate Centrify with our change management and ticketing systems."

But not all benefits have been cost or security oriented. "There are obvious business benefits. There's a disaster recovery benefit. There's even a business continuity benefit for us: Prior to Centrify, users stored passwords in vaults on their laptops. So, if someone was out for a day, and they had credentials nobody else had access to, we were stuck. We eliminated that problem as well," he says.

"Today, we're far more effective at protecting the organization. We're better protecting our patients at possibly the most difficult point in their lives. We're protecting our employees against executing tasks that might have unintended consequences. Now, they can't access servers unless there's a problem case or a project assigned to them."

Overall, the organization has achieved what they set out to do: "We've taken control of our most critical accounts. We've automated password rotation. We've reduced the number of total accounts and we've secured and streamlined the management of third-party and service accounts," says O'Neill. "We've even

implemented a policy that allows only Centrify jump boxes to RDP; even with permissions and account details, you cannot RDP from anywhere else."

According to O'Neill, "Security is often seen as difficult and fraught with danger as it typically requires change across the infrastructure and the business. Centrify was a fast, effective security project that challenged that perspective and helped earn the security team respect across the organization."

LOOKING FORWARD

"Today, we've achieved all the primary objectives of the Centrify project. Our next action will be to come back to the product and brainstorm all of its potential uses — whether intentional functionality from the manufacturer or not. We'll list those uses out and see which ones best address any remaining risks, and that will point us to the next stage of our work."

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +65 9788 25949
Brazil +55 11 3958 4876
Latin America +1 305 900 5354

sales@centrify.com

www.centrify.com