How Cerbos helped Nook build secure and extensible roles and permissions

Case Study

nook

cerbos

HENRY ARNOLD,
CTO & Co-Founder, Nook

"Having the separation of the permissions from the code base just makes the code base more elegant. It makes the permissioning more elegant. It means they're centralized, so they're not tied to specific endpoints. And ultimately it means that different business owners have the ability to actually make updates."

JOE LINES,
CEO & Co-Founder, Nook

"We went from one user - all permissions, to a world where there are many users - many roles. The product relies on Cerbos to bring the detailed roles that we want. All of our customers are using Cerbos."

Highlights

Challenges

- Building a secure and extensible authorization system
- Centralizing access controls
- Ensuring security with regard to visibility of financial information
- Enabling multiple users and roles per client

Solution

- Quick set-up with easy-to-understand code
- Centralized accounting system permissions
- Version control for easy testing and validation
- Technical advice from an expert team

Results

- Secure and extensible access permissions
- Bandwidth to securely service considerably more clients
- Ability to grow the business exponentially
- Confidence to scale product faster

Challenges

Build secure and extensible roles and permissions

When it comes to growing a business, the importance of getting roles and permissions right from the beginning cannot be overstated. It is the foundation on which secure and exponential growth is built. Joe Lines, CEO and Co-Founder, and Henry Arnold, CTO and Co-Founder of Nook, understood this concept and set out to develop centralized access controls that would allow Nook to securely service and bring more value to their customers.

As the Nook team delved deeper into their mission, they quickly recognized that there are multiple different roles that should exist within the process of helping businesses pay their suppliers. However, they also noticed that most accounting software today is primarily focused on the finance team and their accesses and visibility of processes.

> "In an accounts payable flow, you also have an accountant and there's also operations teams who maybe bought the work, or worked with the suppliers, and can validate whether that works at place.", Henry notes.

At the core of the original vision for Nook was the goal of creating an accounts payable product that would provide unmatched value to customers. To achieve this goal, the Nook team knew they needed to bring in all functions that exist within the acquisition of products and ensure they could make the right decisions while also limiting and controlling the visibility of sensitive financial information for these users.

From business owners controlling funds to finance teams executing payments and operations teams needing visibility into specific invoices - there are multiple roles and levels of access that need to be managed.

> "
>
> *"Almost everything we've decided to do, we've done it properly. We haven't tried to cut corners, so we didn't try and do a half-baked approach. ",* Henry says.

The developers of the Nook team had expressed interest in building an authorization system in code or using a Python framework. However, Joe and Henry recognized the complexities of building such an authorization system, as well as the long-term value of separating roles and permissions from their product's code base.

> "
>
> *"There are a number of reasons to do it, but maybe the most important is, as we grow, we don't want the roles and permissions to be tied to the developers. We want business owners to be able to find the roles and the permissions. And if it's in the code base, then a business owner won't even have access to the code.",* Henry notes.

When it came to selecting a company to develop Nook's authorization system, the team spent nine months regularly looking at products and found that Cerbos met all of their requirements and was the perfect fit.

"There's been some degree of thought that's gone into what roles and permission should look like, which is gonna be tens of thousands of hours, more thought than we were ever gonna be able to put into it. So, as the founders, we recognize that and realize that that's why we want to work with partners who have thought this through in much greater detail than we have the capacity to do.", Henry says.

Solution

Simple, secure authorization layer

Starting with Cerbos was a seamless and efficient process for Nook. They were able to define their user groups and roles, configure policies, and found the process to be straightforward.

As Henry notes, *"We had one developer on it for about 6 weeks. And that got 95% of it done. We've obviously been making improvements, a few little lessons since then, but as far as users are concerned it was operational after about 6 weeks of development, with just one full-time developer. Authorizing endpoints was super straightforward."*

While the time-saving aspect of their partnership with Cerbos as an authorization layer was not as crucial as the security and centralization of permissions, to Joe and Henry, they noted that if they were using Django, they would have had to build their own Python library, which would have taken considerably more than six weeks.

After the initial set-up, the Nook team didn't have to do much else, Henry points out. *"The only time we use it is if we add endpoints, change the name of functions in our code. Then we have to update it. It's part of the release cycle, so it all gets updated when it releases."*, Henry adds.

> *"We're pretty happy. It does what we want. It is just running and we don't really have to worry about it.",* highlights Henry.

As a payroll product partnering with Cerbos, Nook is able to restrict access to payroll and limit the visibility of the bank transaction feed. This has allowed Nook to bring different user groups into the product and be part of the accounts payable flow, which was missing from other products in the space.

> *"It really allowed us to bring on these different user groups into the products and be part of that accounts payable flow, which, when we started out, that's one of the things that we thought was really missing from the other products that are in this space.",* Henry highlights.

"So for the business owner, they now can control the amount of responsibility they want to give to external accountants, which is incredibly powerful for us and incredibly powerful for the accountants.", Henry says.

"We're pretty happy. ==It does what we want. It is just running== and we don't really have to worry about it."

Results

Security and bandwidth to service exponentially more clients

Thanks to their collaboration with Cerbos, Nook has centralized rules and permissions and a scalable, secure, and easy-to-use authorization solution that is cleanly separated from Nook's core application code.

The team at Nook confidently navigate the complexities of accounting system permissions, allowing them to focus on what really matters - delivering unmatched value to their customers.

Moreover, Nook's developers can move fast and build features without being bogged down by complex authorization requirements.

Today, Henry, Joe, and their team have over 3 times the number of users per every client, with the top use case at the moment being 12 users.

"We went from one user - all permissions, to a world where there are many users - many roles. The product relies on Cerbos to bring the detailed roles that we want. Really, we had a working prototype before it and it wasn't fit for serving. We couldn't service any customer that we service now.", Joe says.

Henry explains that *"It might, from the outside, look like Cerbos is particularly powerful if you use microservices. If you have microservices, without a centralized authorization layer, you'd have to implement authorization in each of those microservices, which may not, for example, be using the same programming language."*

Yet, Henry highlights that although Nook is a monolith, the company highly benefited from their partnership with Cerbos. *"We think even as a monolith, it's proved really powerful."*

> *"Having the separation of the permissions from the code base just makes the code base more elegant. It makes the permissioning more elegant. It means they're centralized, so they're not tied to specific endpoints. And ultimately it means that different business owners have the ability to actually make updates.",* Henry explains.

The team is confident that Nook's authorization logic is secure, which enables them to continue scaling their business. Choosing Cerbos has empowered Joe, Henry, and their team to move fast.

> *"It was quick to implement. We didn't need much support. And since it's up and running, we haven't had any problems at all. We basically don't touch it. It's doing what we want it to do. It scales.",* Henry says.

The trust that the Nook team has been able to put into Cerbos is empowering, as Joe notes, *"It's clearly a great product and it's bringing us a lot of value, and we're not paying for it, which is amazing."*

When it comes to other companies seeking to centralize their authorization logic, Henry and Joe recommend Cerbos as the solution. *"If it's about whether they need rules and permissions in their products, that's not for us to judge, but if it's Cerbos versus using some roles and permissions framework that becomes part of your backend framework, then I would challenge whether any of those libraries or frameworks offer the value, not necessarily to developers, but to the business, more broadly."*, Henry explains.

Henry and Joe also recommend empowering product owners to manage access controls, rather than tying roles and permissions to a company's engineering team. The team at Nook understands the value of giving product owners visibility over customer issues and the ability to define different roles for customers, which ultimately defines a company's ability to scale a product.

Looking ahead, Nook and Cerbos have exciting plans to continue to exponentially and securely scale Nook by using new features that Cerbos is constantly releasing, features that the Nook team didn't even know they needed.

"

"The product relies on Cerbos to bring the detailed roles that we want. All of our customers are using Cerbos."

The ==open source authorization== layer for your product.

Model your requirements in Cerbos.
Get up and running in no time.

Book a Demo

cerbos