ClearSkye

Solve Third-Party Access Challenges While Maintaining Security with Clear Skye and ServiceNow

Many organizations utilize contractors, vendors, and consultants to augment staffing, manage special projects, or maintain business operations. But securing access for these types of roles can be a challenge, especially across multiple locations, divisions, or subsidiaries. And for specific industries, such as healthcare, manufacturing, and technology, the compliance burden that accompanies managing this third-party access presents mounting challenges.

So, what happens when you have third parties that need specific access to data, applications, and services within your organization? How do you best manage this from a people, process, and technology perspective?

People

Your organization needs to utilize third parties for a variety of reasons and those reasons usually translate into a specific set of access needs. For example, if you have shift nurses at a hospital, they need access to their assigned floors as well as to the patient records for those under their care.

Processes

Onboarding and offboarding processes are usually quite well defined for full-time and part-time employees. Policies and processes must be defined for third-party access too. Many IT organizations struggle with simple visibility into who, what, and when third parties will be used, so managing them is a challenge.

What's the risk?

You can't manage what you can't see

"66% of companies surveyed had no idea how many third-party relationships they had or how they were managed, even though 61% of the surveyed companies reported having a breach attributable to a third party."

Data Risk in the Third-Party Ecosystem: Third Annual Study, Ponemon Institute

Breaches are costly and take months to uncover

In 2022, it took an average of 277 days—about 9 months—to identify and contain a breach. Shortening the time it takes to identify and contain a data breach to 200 days or less can save money.

$1.12M

Average savings of containing a data breach in 200 days or less

IBM Data Breach Report 2022

Technology

Many organizations are challenged with shadow IT providing access to data, applications, physical locations, and services for third parties. Rather than using existing access management and governance solutions, managers can and do provide access directly to third parties. This not only means that policy can't be followed but tracking and cutting that access can be nearly impossible without visibility into what access exists.

All of these challenges can translate into lost productivity, a widening attack surface, and an untraceable dent in your organization's security.

The Importance of Identity Governance for Third Parties

Identity governance is a critical part of any organization's security posture that ensures access is managed, logged, and verified on regular intervals. Many organizations struggle with managing third parties because they don't have the same authoritative source for the identity data as standard employees do. And they also fall outside the standard identity lifecycle processes that IT uses to manage access due to the nature of the work they do. Projects can have shifting start dates and end dates, routine maintenance occurs on a schedule that doesn't require constant access but can't be done without it, and staff augmentation can occur at varying level with some people coming back to an organization multiple times.

Identity governance solutions provide critical visibility into who has what access, who approved that access, and whether it's been used in a normal or anomalous fashion. This data allows security and risk teams to monitor usage and flag anything out of the ordinary to help maintain organizational security and manage their broad attack surface.

Identity governance solutions can also ensure that access meets internal policy and external regulatory requirements for compliance and reporting.

Clear Skye Secures Third-Party Access, the Same Way We Do Employee Access

For Clear Skye, access is access regardless of whether that access is for an employee, contractor, vendor, partner, or robot. Clear Skye IGA provides the infrastructure to be able to build processes to manage all organizational access, including third-party access.

Clear Skye offers managers the ability to onboard consultants, contractors, and vendors as they need to, to support their departmental or divisional needs. Because they're not employees, Clear Skye provides flexible approval processes to make sure that the users are vetted before they are onboarded. Clear Skye approval processes ensure that only the right users are getting onboarded and we can automatically provision based on the system information. For example, a department or their location or a specific firm that they work for can dictate some of their access.

Clear Skye also integrates that third-party identity data into the overall lifecycle management process. So should temporary staff convert to employees, Clear Skye detects that from the authoritative source without requiring a bunch of code to extend the typical IGA onboarding process. We can also track backwards conversions of employees and trigger automatic access reviews for those scenarios to ensure they have the right access based on their current relationship to the organization. Clear Skye can also trigger relationship reviews that verify that a third party reports to a specific manager in a specific department.

While it can be a challenge, managing third parties within your organization is not insurmountable if you can put the right people, processes, and technology in place to manage their access. Clear Skye IGA is here to help you manage third-party access in the same way you manage your employee access and on the business platform that your IT and end users are already familiar with: ServiceNow.

The Benefits of IGA Built on ServiceNow

Clear Skye IGA is built on the Now Platform and its identity data lives within the platform data warehouse. This provides some benefits across other solutions on the Now Platform.

Some third-party access might be for a partner organization and their employees or a vendor. And in those cases, if an organization leverages ServiceNow for managing the actual vendor itself, or the risk around the vendor ServiceNow has an established Vendor Risk management module. Clear Skye's identity processes can map directly into those vendor risk processes to minimize the impact of a breach and automatically flag a risk.

The identity data can be utilized to trigger access reviews, create a ticket for someone to look at a flagged account, automatically disable access, or gather intelligence around this specific access so it can be monitored.

It's critical that identity processes are integrated into the organization's overall security ecosystem. And because Clear Skye does this in ServiceNow, we make that connection in a very elegant way that doesn't require tons of code or customization.

Benefits of Third-Party Access Management

- Maintain productivity of third parties
- Ensure accurate and swift provisioning and de-provisioning of access for third parties
- Track access for third parties
- Tighten the overall attack surface and improve security
- Make identity data available on the platform for use with other solutions (Vendor Risk Management, SecOps, Governance, Risk & Compliance or GRC)

About Clear Skye

Clear Skye IGA is an identity security solution built on ServiceNow. It provides identity governance through access request, access certification, employee lifecycle automation, and workflow management. With identity data on the Now Platform, Clear Skye plugs directly into your business processes, provides deep identity control and insights, and builds the bridge between the business and IT.

Learn more at clearskye.com