



ECORA'S CHECKS AND BALANCES

BRYAN COTE, Senior Product Manager at Ecora, stresses the need for organizations to clearly define roles for those responsible for IAM and compliance, and also talks about how Ecora's configuration and security auditing tools can help.

What exactly is identity and access management (IAM)?

IAM comprises people, processes and products to manage identity and access rights within an enterprise. It also ensures that access is granted or revoked in accordance with company policy and security requirements. IAM components can be classified into four major categories: authentication, authorization, user management and a central user repository such as Microsoft's Active Directory. The ultimate goal is to provide the right people with the right access at the right time.

How can information management managers ensure that proper procedures are being followed to protect valuable information assets?

Ideally, technology would enforce the access rights and privileges from the time an employee is hired through the time he or she is terminated. Since there are very few companies that have achieved this level of automation, we must look first at establishing a strong procedural and policy foundation. When a new employee is hired, a documented request should be made for specific IT resources. With a minimal number of processes in place, tools like those from Ecora can be used to audit the environment, and determine if the processes were followed and if any stray credentials in the network remain that no longer should.

How can organizations clearly define roles for those monitoring compliance to IAM, without using outdated information and impacting the access of others, or without creating a potential threat of improper data manipulation?

The configuration and security auditing tools available today make it possible for people who have not typically been involved in the technical implementation side of IAM procedures to audit the state of those controls within their organizations in real time. For example, if HR controls the ultimate system of record, they can receive reports on a daily basis, listing all active users on the network with the corresponding resources that they have permission to access and audit this report against active and terminated employees. This read-only access can be given to the HR group without requiring them to have administrative access or allowing them to access other sensitive IT information or other security controls.

How long does it usually take to terminate user access in the event of a worker leaving or no longer needing access? How can organizations manage identities and permissions for those employees that may simply be changing roles within the organizations?

There are two parts to this question: 1) How long it takes to think you have terminated access and 2), how long until you know you have terminated access. Most organizations have processes in place to request the termination of an employee's access. However, there are often dozens of other systems that IT is not aware of, to which the user has rights. This often happens with development staff with administrative access to development machines. Also, these machines often have access to other production resources and tend to be administered by the developers themselves, rather than IT. If the developer can find a way to access development machines from the internet, he may be able to access other critical network services from that development box and often his administrative access rights will carry over. A tool that can discover systems in your environment –

whether they are known or unknown – is necessary so that all of the access rights across the machine can be audited to find any unknown points of access. The same issue applies when transferring employees from one role to another – what they had access to should be determined and that access should be reset for their new roles.

How can organizations effectively measure initial adoption and ensure compliance is sustained once it is achieved?

Once the policies and procedures are in place, the authorization of users and the date they should be removed from the network should be tracked. Using configuration and security auditing tools, such as those from Ecora, organizations can set up automated audits of their environments. They can then be compared to human resource information systems or other systems of record to determine if policies are being followed. If some users are slipping through the cracks, it will become apparent immediately and can be addressed before it becomes an issue. Then, improvement can be tracked over time at least until we are responding in real-time to those access requests and removals. Up to that point, there will be solid data to justify the budget for tools in the future.

How can organizations successfully validate IAM controls at various levels of the infrastructure – application, server, network devices, databases, CRM, etc.?

Each layer of the IT infrastructure has different tools for managing identity and access to their unique components. It is important that users have access to this information in a consolidated way. When users are forced to compare access information from dozens of databases, there is a greater risk of error. Having a single, consolidated version of the truth from all the infrastructure components with appropriate presentation corresponding to the types of users is critical to effectively manage IAM across these components. Given the interdependency of these components, any level overlooked or improperly audited provides the proverbial "weakest link" in the security chain.

How are more powerful access rights, such as domain and network administrators, monitored and controlled?

Is there someone within the organization who is responsible for auditing these areas so that there is appropriate segregation of duties?

When the people who hold all of the keys leave an organization, an organization is at its most vulnerable. Organizations typically respond by "changing all the locks," metaphorically. In other words, all root and administrative credentials get new passwords and redefined access. Often, these administrative passwords and accounts are shared by multiple individuals; thus, there is an additional process of communicating these changes securely – not through e-mail – to all the individuals who still need that access. A tool is necessary that allows you to discover and audit systems with administrative root access, ensuring that nothing was missed. Being able to use these tools to discover the environment, discover the systems and audit those systems is very important. Usually senior technology managers, VPs or CIOs bear the responsibility of auditing.

How is Ecora addressing all the things we discussed today, and what do you expect to see in this space for the future?

Ecora is leading the way with providing consolidated, heterogeneous configuration auditing and reporting solutions to the enterprise. Ecora allows configuration and security information to be leveraged by multiple roles throughout the enterprise, giving them a single version of the truth on which to base their auditing and compliance activities and decisions. In a sense, many mandates are being audited by common firms. Having a single version of the truth eliminates the chance of having conflicting evidence that would require reworking the reporting or recollecting the data.

Looking to the future, there will be a much tighter integration among the administrative solutions, the infrastructures that manage the access to the active directories and the lightweight directory access protocols (LDAPs). But given that tight coupling, it will still be very important to have an auditing solution like Ecora's to act as a check and balance and help ensure that the organization maintains a strong IAM posture.