SONET.IO

Secure Remote Development With Sonet.io

The easiest and most secure way to access development environments, keep your source code and data safe, and improve productivity.

sonet.io

www.sonet.io

info@sonet.io

Introduction

One of the main challenges, when it comes to securing access to development environments and the data they contain is to strike the right balance between security and productivity. Intellectual property residing in development applications and tools such as Jira and Github has to be secure and well protected from unwanted access and exfiltration. Companies need to secure their development applications, source code and design documents for all their remote engineering teams, including third party outsourced development resources. Outsourcing is very beneficial to get access to the right engineering resources and reduce development costs. According to the study in Statista global software outsourcing data; and Computer Economics IT Outsourcing Statistics 2020-2021, 60% of companies were outsourcing some software development in 2021. At the same time, the Verizon 2022 Data Breach Investigations Report shows that 94% of lost and stolen assets are by external threat actors.

The challenge becomes bigger with everything becoming remote: the workforce is everywhere, applications reside in the cloud, data is distributed across many locations and applications, and your network is the internet. With the COVID pandemic, the workforce is increasingly remote and engineering teams, spread across the world, likely have source code residing in their devices. Whether the devices are managed or unmanaged, they are vulnerable to attacks and the data on those devices becomes at risk of leaking. It is always more secure to have development related data securely stored in a cloud SaaS application or on premise web application. Also, engineering teams access servers spread across the cloud and on premises, from geographically distributed locations, increasing the risk on those servers and the intellectual property they contain.

Current approaches rely on VPN-based segmentation, combined with very complex impractical application-level controls to attempt to achieve a secure development environment. In addition, these solutions become easily unmanageable when trying to add data protection in the mix, and they rarely achieve the needed level of security. They result in engineers' frustration, a lack of productivity, and security holes that may be exploited.

At Sonet.io, we've built a solution to bring trust back to secure your development environments so that you can hire anywhere and improve engineers' productivity. A solution that not only controls access to applications and data and protects them from harmful attacks and breaches, but also continuously monitors users' activity and records user-application interactions. The solution does not require agents, application connectors or changes in applications, and can be ready in minutes.

Leverage remote work, improve productivity and protect your IP

Any organization can hugely benefit from the availability of cloud services and SaaS applications to improve productivity and leverage the capabilities that these applications provide without the extra overhead of having to deploy, operate and manage these applications. This is especially true for modern development environments that are based in the cloud, such as Jira and Github. At the same time, being able to leverage a remote workforce, whether internal engineering teams or contractors, brings a big benefit to businesses, large and small.

The main challenge is to ensure that access to development environments and applications is governed properly, and that all the source code and intellectual property they contain is protected. This is where the Sonet.io solution comes into play: provide a frictionless secure access to development environments without the need to interfere with end user privacy, install any agents on end user devices or any application side connectors, or make changes to applications. All users need is their favorite browser to access the applications and servers that they have been granted access to, and the Sonet.io service takes care of the rest:

- Continuously control access
- Protect the applications, servers and intellectual property
- Provide administrators with great visibility through a rich set of logs and monitoring data
- Ensure engineers privacy and improve their productivity.

The Sonet.io solution sits between a user, the applications and servers, and provides a layer of security between them. Engineers access development apps and servers through a single URL simplifying access from anywhere in the world.

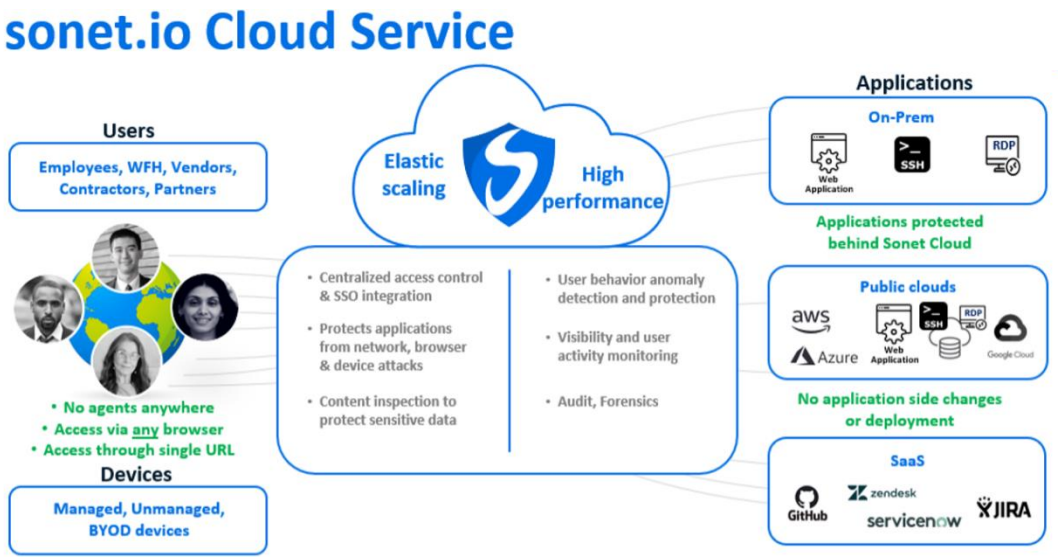

Figure 1. The sonet.io SaaS service

Least privilege access enforcement

The Sonet.io solution enables you to control access to development applications and servers centrally and in a granular manner. This control applies to SaaS apps, Webapps as well as servers. The Sonet.io solution supports https, SSH, RDP and VNC protocols. Many current deployments use VPN segmentation as a way to isolate engineering applications and servers from other enterprise applications. This method has several disadvantages. First, users are forced to have different VPN profiles and use each profile to access the right resources: this is a very inefficient method that reduces productivity and creates frustration for the engineers. Second, any sharing of information between the applications in a VPN segment with another segment requires hopping between VPNs creating frustration and reducing productivity. Third, VPNs provide network level access, which is a very well known issue for security, given that the attack surface becomes the whole network and once users are inside the network, they will have access to all resources in the network, even if segmented, and there is no visibility about their specific application access.

The Sonet.io solution solves this problem by applying the main principle in Zero Trust: provide explicit access to specific applications and servers for specific users and user groups without requiring complex setup and deployments. Access privileges to applications and servers can be very easily assigned and managed for users based on several criteria such as their role, location and risk. For example, Development engineers get access to Jira and Github and other development environments, while QA engineers get access to Jira and ServiceNow only, and system administrators have access to SSH servers.

Access can also be controlled based on user groups, such as contractors, or to specific locations and/or at certain times of day, or from specific IP addresses. This flexibility provides a very easy way to have fine grained control over development resources access without impacting users' productivity.

Inspect and protect your content

Content moving in and out of development applications is fully controlled by the Sonet.io service. For strict control, you can set your policies to deny any downloads and prevent sensitive content from leaving your organization. You can also protect your development environment from any PII information being uploaded into your organization, particularly from technical support engineers.

The Sonet.io solution allows you to control downloads and uploads based on the type of data such as source code and/or content matching of patterns such as email addresses, social security numbers or any other PII data. For example, all users can be prevented from downloading source code to protect from any leaks. Content inspection policies allow the control of how data moves in and out of the applications and servers and can be created per application, for a group of applications, or for all applications without making any changes to any application. These policies can be used to control downloads and uploads, copy/paste of data and viewing of certain data. Data obfuscation can also be used to hide certain confidential data from being seen by users.

Incident response and user activity monitoring

The Sonet.io service provides detailed logs showing all the activities related to the Sonet.io portal access and application access. Logs can be searched and filtered for an easy way to find the required log information.
Rich logs are generated to allow you to track all ongoing activities from users connecting to the Sonet.io portal, to application access, policy violations, configuration changes, etc. Logs generated by the Sonet.io service can be downloaded locally
or ingested in a SIEM solution.

In addition to the rich logging features, Sonet.io offers unique session recording capabilities that include a full recording of user sessions when accessing the applications, servers and desktops without interfering with user privacy. For example, an engineer can use the same browser to access the development applications through Sonet.io, while browsing their personal bank accounts in a different tab in the same browser. Only the development applications access is controlled and recorded by the Sonet.io service and nothing is captured on other private browsing sessions. Policy violations are highlighted in the session recordings allowing administrators to assess risks and take corrective actions, such as policy adjustments. In addition, the session recording capability allows for deep forensics to investigate potential breach attempts.

A dashboard provides an 'at a glance' view of all users access to applications: active users, active applications, policy violations, logs by severity, etc. providing administrators with an overall visibility to engineers access to development environments.

Behavioral analytics

The Sonet.io solution allows you to monitor the behavior of users connecting to your development environments and control their access accordingly. This helps prevent intruders or bots from causing damage to your applications or stealing your data. With Sonet.io, you are able to detect abnormal behavior and act accordingly. For example, if a user does not usually download large amounts of data, and suddenly large downloads for this user occur, the behavior is flagged, the administrator can be notified in real time or block the downloads if the data has a sensitive nature. Other behaviors such as users connecting from unusual locations, or having several connections at the same time from different locations will be detected and users can be denied access and administrators can be notified immediately.

How does it work?

The Sonet.io service is very simple to setup and use. Users can use their favorite browser without requiring any installation on their devices or make any configuration changes to these devices. Users just need a URL that directs them to a portal where they can access any application or server with a single click.

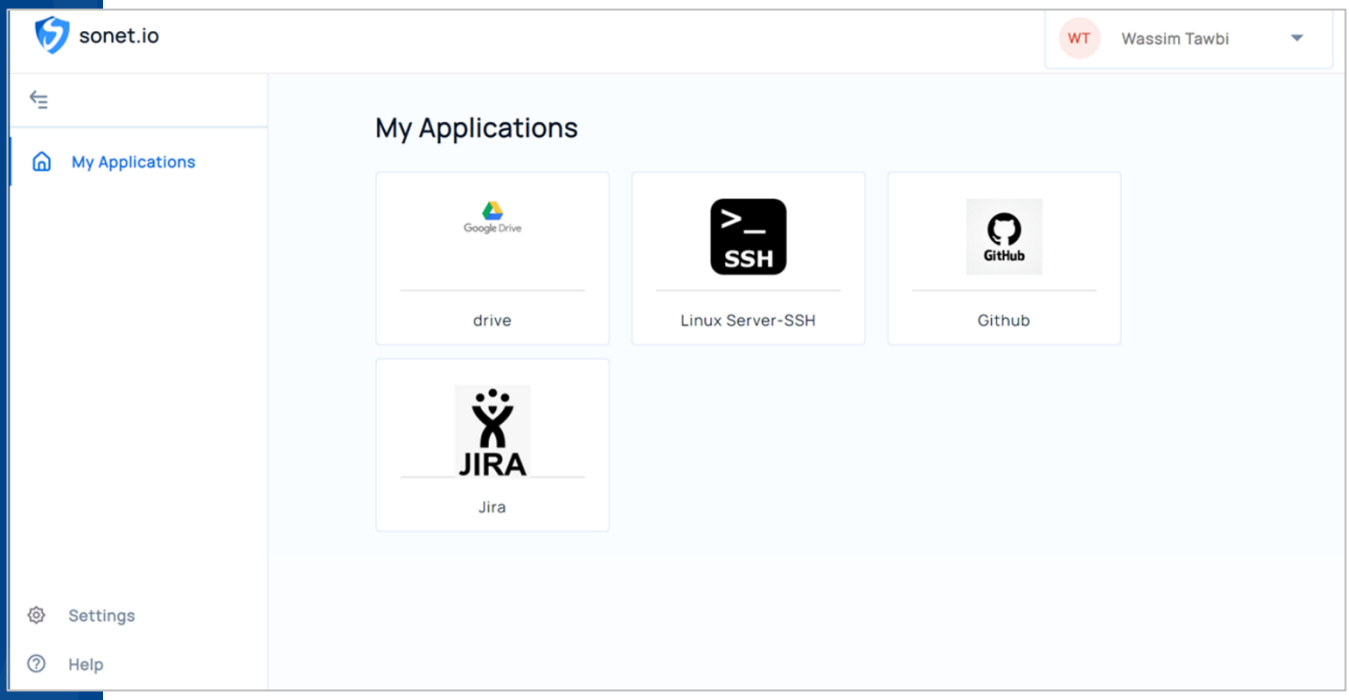

Figure 2. sonet.io end user dashboard

You can integrate with your iDP in a few clicks and import your users and user groups into your Sonet.io service instance, then configure
the applications (URLs) and servers (hostname and/or IP address). The Sonet.io provides an SSO capability for all applications and servers and removes the risk of having
users manage SSH keys in their device, to prevent making servers highly vulnerable to attacks.
The Sonet.io solution has the ability to securely manage access credentials within the service itself.

Development applications and tools can be SaaS applications, cloud hosted web applications, on premise web applications, or servers on the premises or in the cloud. There is nothing to change on the application or server side, and no application connectors or server configurations are needed.

You can assign these configured applications and servers to users to access them securely. Only assigned applications and servers can be accessed by users.

Policies can be created to further control access to applications, servers and content and is done through very simple policies written like natural language.

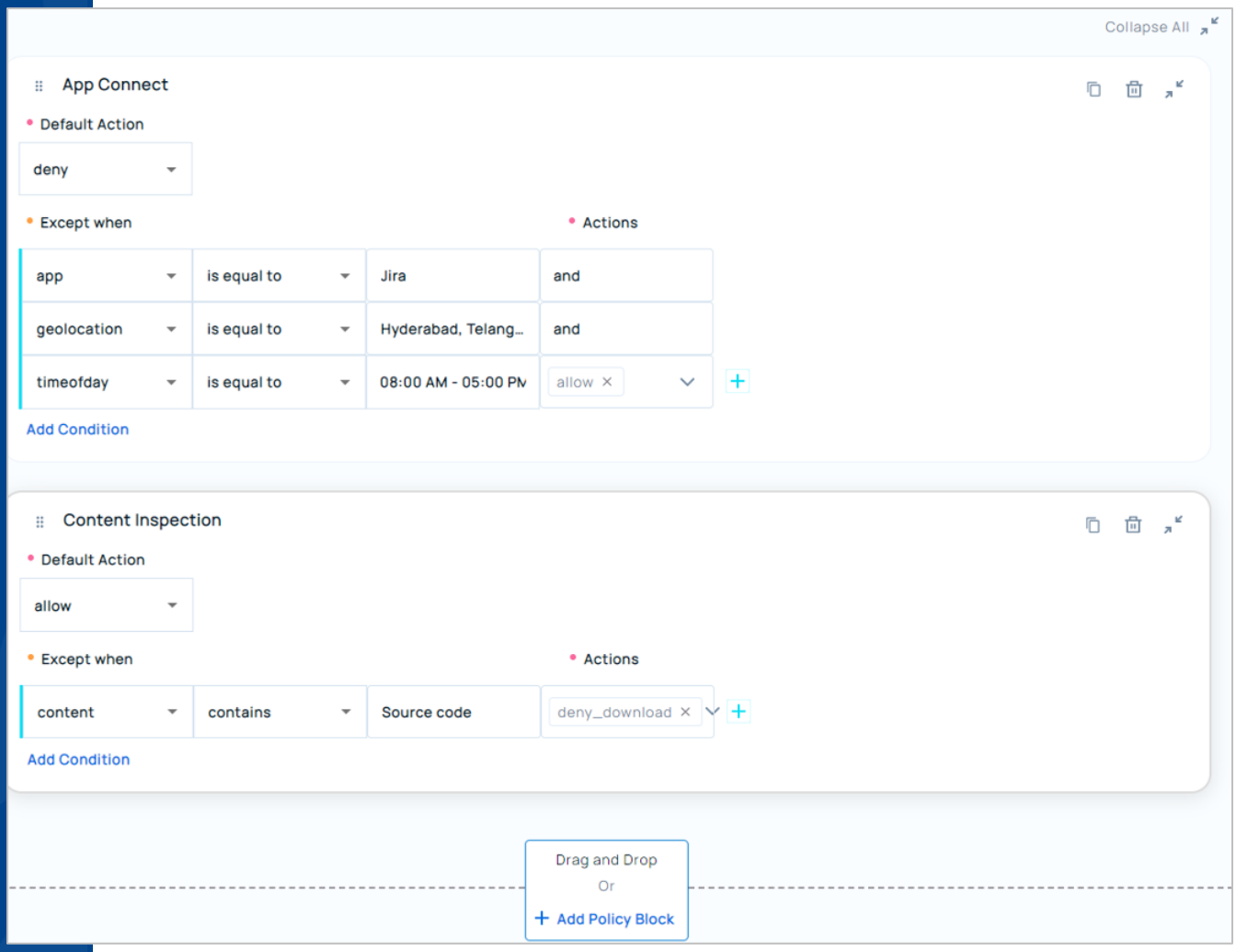

Figure 3. Policy example to limit access to Jira from a specific location and time and prevent source code download

Summary

Whether you are a startup, a small business or a large fortune 1000 company, securing your development assets should be a priority for your business. The Sonet.io solution was built from the ground up for the remote workforce to simplify security so work gets done. The Sonet.io solution allows you to control access, to continually assess risk, and to protect source code and servers, with zero deployment, so you can build products faster. The solution empowers your distributed workforce with security that simply works. Make the Sonet.io solution an integral part of your SDLC and DevSecOps strategy in order to leverage the right development resources anywhere, while staying secure and protecting your valuable assets.

Next Steps

To learn more about the Sonet.io solution,
please contact us at info@sonnet.io.