SONET.IO

Frictionless, Trusted Access For Contractors And Partners With Sonet.io

Empower your 3rd party contractors and partners with security that simply works, in minutes. Control access, continually assess risk to protect your data and applications with zero agents while improving productivity.

sonet.io

🌐 www.sonet.io

✉ info@sonet.io

Challenge

Enterprises need to leverage 3rd party vendors, contractors and partners without compromising their applications, servers and data security, and integrity.

Solution

A comprehensive, frictionless, trusted access to enterprise applications and servers for all 3rd party users, from any type of device and any location, without the need for endpoint agents or connectors deployment in front of applications and servers.

Benefits

- Eliminate shipping devices to 3rd party users reducing cost and operational overhead
- Improve productivity by allowing 3rd party users near instant access to applications by eliminating logistics and maintenance downtime
- Protect your intellectual property using comprehensive data protection through content inspection preventing infiltration and exfiltration
- Protect applications from potential 3rd party devices and network attacks without requiring a VPN or endpoint agents
- Achieve compliance with full logging and selective session recording capabilities highlighting user activities, policy violations and behavioral anomalies

Enterprises of all sizes depend on partners, vendors and contractors to conduct their business. These partners, contractors and vendors need access to the enterprise applications and other resources, such as servers, in order to perform their duties. In most cases, these applications contain confidential and sensitive data that needs protection from theft and exfiltration.

Enterprises have often to choose between security and productivity: allow an open access to applications with little security controls, which poses serious security risks on the enterprise and their confidential data and intellectual property, or install specific software managed by the Enterprise's IT team on the partners and contractors devices. The latter is seldom possible and hence the enterprise is forced to send a "locked in" device to the contractors resulting in a very high cost in Capex and Opex, and decreasing productivity due to wait times, shipping delays and continuous maintenance. Even with this approach, several solutions have to be put in place (endpoint software, CASB, DLP, etc.) and properly integrated, making the complexity very high and costly, and leaving security gaps.

Sonet.io Trusted Access™ is the only solution that solves this complex problem by providing a comprehensive, frictionless, secure access to enterprise applications and servers from any type of device and any location without the need for any endpoint or application side deployment. The solution is suitable for internal and external users and is particularly appealing for the 3rd party access use case that we cover in this paper. The solution's main attributes are simplicity and ease of adoption, with no overhead to IT teams or partners and contractors. It is highly secure with fully integrated security components, and unequal visibility into users access to enterprise applications and servers.

3rd Party Access Challenges

Today's enterprises rely heavily on 3rd parties to conduct their business but face major challenges when it comes to securing access to applications, servers and data for these 3rd parties:

- They have no control over vendors', partners' and contractors' devices accessing their applications and data
- They have to assume that any device accessing their applications can be compromised and that credentials may be stolen (Zero Trust!)
- Their applications and data are being accessed over untrusted networks and reside mostly in the cloud
- They have little to no visibility into user activity when accessing applications and data
- Today's approaches to solve these challenges are disjointed and insufficient, with little integrations resulting in security gaps

Our Sonet.io Trusted Access™ solution was built from the ground up to address these challenges and provide a solution that is easy to adopt by users and simple to put in place by the security and IT teams. The solution is a true SaaS service not requiring any installations, and built on a modern cloud native architecture to provide the highest levels of security along with elastic scaling and high performance.

The Sonet.io Trusted Access ™ for 3rd Party

Time to value and frictionless adoption

To respond to customer challenges, Sonet.io built a highly scalable architecture that simplifies the way applications, servers and data are accessed and secured. The Sonet.io SaaS solution is built from the ground up to make it easy to adopt and put in place with no requirements on endpoints or applications. It is particularly powerful when 3rd party access needs to be secured and data and IP needs to be protected.

The solution augments strong network security with behavioral analytics powered by AI and ML techniques to provide real time protection against potential threats from hackers and ransomware actors.

Sonet.io offers the next generation of Zero Trust solutions where 3rd party users access to applications and data is constantly checked and monitored and assumes that any device and/or credentials may be compromised.

Data flows between users and applications are fully controlled to prevent infiltration and exfiltration of confidential data and intellectual property information.

Administrators have full visibility into user/application activities with audit and forensics tools available in the Sonet.io solution.

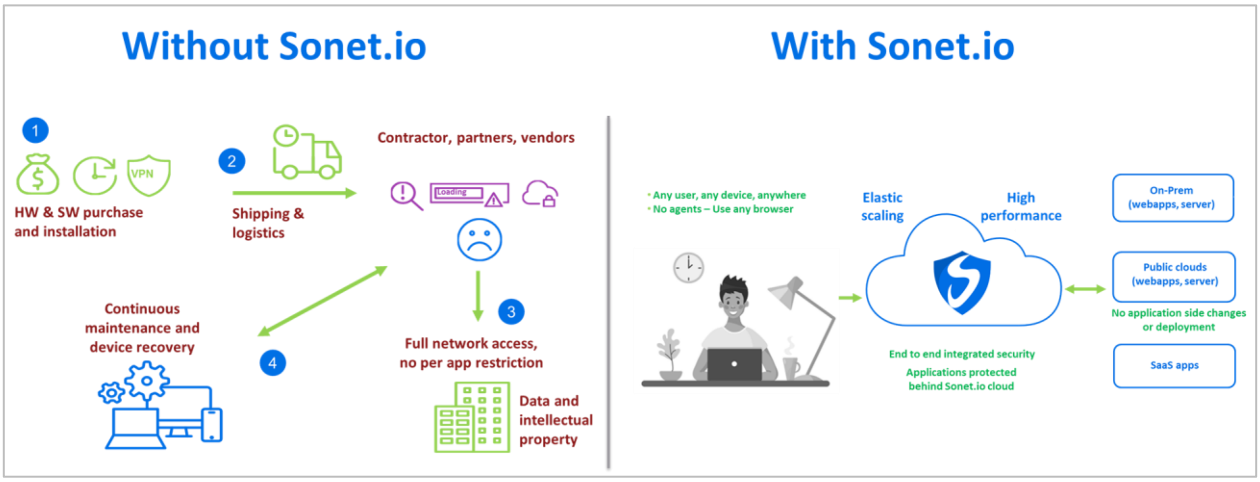

Without Sonet.io
With Sonet.io
1
VPN
HW & SW purchase and installation
2
Shipping & logistics
Contractor, partners, vendors
Loading
3
Full network access, no per app restriction
Data and intellectual property
Continuous maintenance and device recovery
4
• Any user, any device, anywhere
• No agents – Use any browser
Elastic scaling
High performance
End to end integrated security
Applications protected behind Sonet.io cloud
On-Prem (webapps, server)
Public clouds (webapps, server)
No application side changes or deployment
SaaS apps

Figure 1. Sonet.io Trusted Access for 3rd party access vs. current approaches

Seamless User Experience

One of the main challenges in securing application and server access for partners, contractors and vendors is the friction that is caused by deciding to install endpoint software on their devices, or having to provide them with company managed devices that result in high cost, lower productivity and frustrating management overhead. The Sonet.io solution offers unparalleled simplicity and no friction to enable access to enterprise applications. All that a 3rd party user needs is their preferred browser and a URL to the enterprise's Sonet.io portal, which will give them access to the authorized applications.

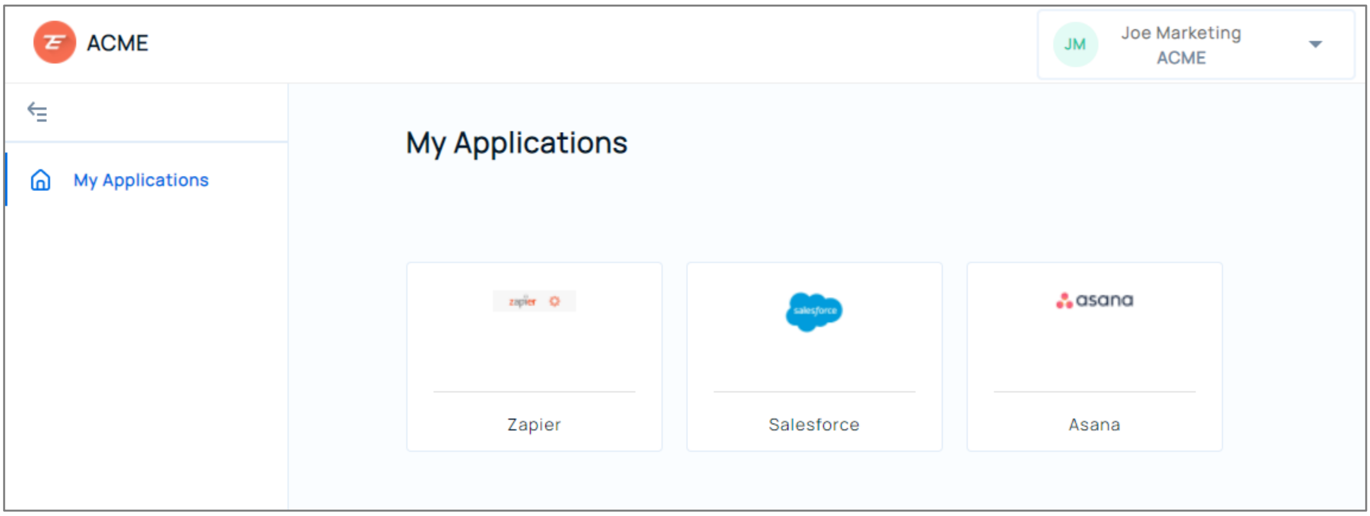


Figure 2. Instant access, one-click dashboard for 3rd party access

The solution can be used on managed and unmanaged devices and does not require the installation of any agent or software on endpoints, nor any specific endpoint configuration, and eliminates the need for VPNs. User experience is not altered and privacy is fully maintained because the solution only inspects and controls access to enterprise applications and does not interfere with users' private communications such as their banking, social media or health applications.

At the same time, the solution is highly secure by providing all the security controls and checks on the communication with applications, protecting content and applications from any potential network, device or browser attacks.

No Administrative Overhead

In addition to not requiring any agent, the Sonet.io solution eliminates the need for any connectors installation on the applications side, making it very simple to deploy by IT teams and eliminating operational costs that other solutions incur.

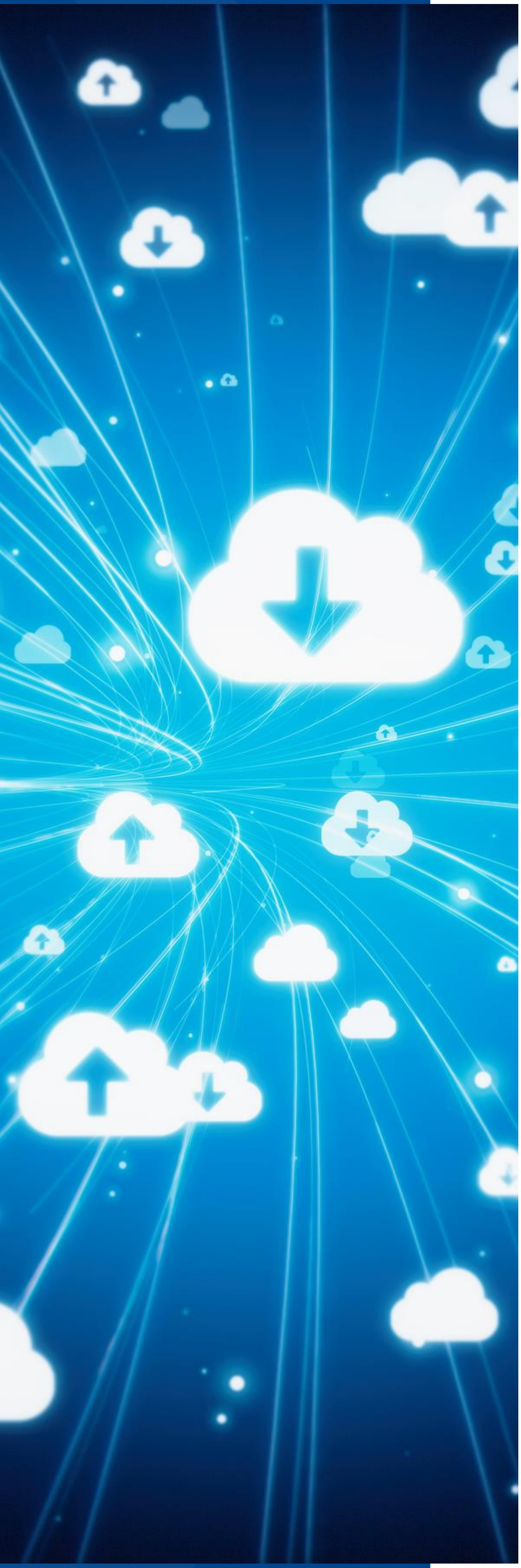
All that is required by the administrator is to configure access policies in the Sonet.io portal to allow or deny access to applications and servers (SSH, RDP, VNC) based on users, user groups or other attributes. For example, contractors can be given access to a limited set of applications at specific times of day and from designated geographies and policies can be setup to control what they can download and/or upload to and from these applications.

The Sonet.io solution is the only solution in the market to offer those capabilities while being 100% cloud-based with no requirements for any deployment by customers. Contrast that with current approaches relying on VPN or agent/connector deployments, which increases the attack surface by providing full network access and all its resources, instead of limiting access to specific applications and servers or keeping the complexity of having to deploy agents and connectors everywhere.

Integration with Existing IdP and SSO

The Sonet.io solution offers strong authentication and single sign-on for users to access authorized applications. IT personnel can very easily integrate Sonet.io with enterprise's existing identity management and SSO solutions such as Okta, ForgeRock and Google Auth making the deployment very simple and allowing a very quick provisioning of the contractors/partners and associated access policy.

Access policies can then be created for those users and groups directly in the Sonet.io portal without requiring any changes to the applications and servers. Policies can be easily configured and applied to 3rd party user groups that are part of an existing IdP.



Protection from Cyberthreats

The Sonet.io solution performs a set of security controls on all traffic between 3rd party users and enterprise applications. It protects applications from any cybersecurity threats that may come from users and their devices by isolating the applications and servers from users. The Sonet.io service inspects all the information flowing to and from applications ensuring that no harmful content is exchanged.

The solution assumes that users' devices and browsers may be compromised and provides the necessary controls to eliminate potential threats to applications and data.

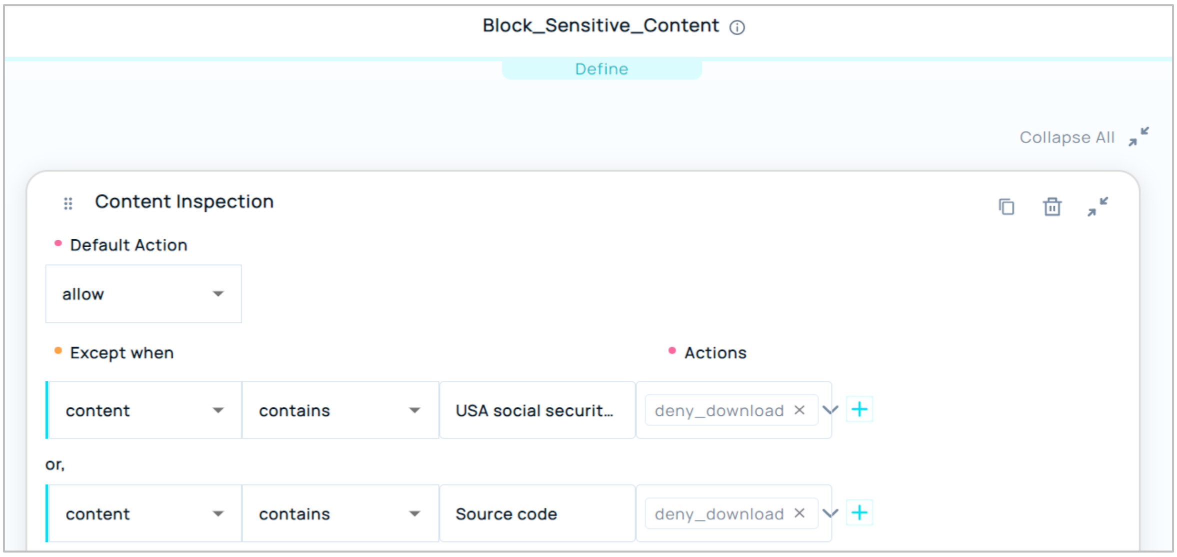
In addition to controls over who can access what applications, from where and when, behavioral-based policies can be setup for an advanced control of users access to eliminate threats resulting from potential credentials theft or other harmful user activities.

Content Inspection and Protection

A full set of content inspection and controls is available to administrators. This is especially important when partners and contractors have access to sensitive data and there is a need to protect that data from being compromised.

Sonet.io gives the ability to control downloads and the type of data that can be downloaded and uploaded. Controlling downloads enables customers to protect their intellectual property and confidential data from leaking to their partners, contractors or vendors. Customers can apply content inspection policies to ensure that uploads, are not only safe from any harmful content, but also clean from any PII or other data that they should not have access to and that can cause regulatory compliance issues. For example, a contractor may be uploading customer prospects information to an ERP system that may contain social security numbers of the prospects; the content inspection policies can prevent that by obfuscating the SSN or by preventing the upload until the unwanted data is removed to eliminate privacy concerns.

Administrators can set policies to prevent contractors from performing operations, such as file content viewing and copy/paste operations. Confidential or sensitive content can be obfuscated at display or in a copy/paste operation.



Block_Sensitive_Content

Content Inspection

Default Action: allow

Except when:

			Actions
content	contains	USA social securit...	deny_download
or,			
content	contains	Source code	deny_download

Figure 3. Sonet.io content inspection policy example

All content, including predefined patterns and custom content matches can be inspected and protected by the Sonet.io Trusted Access^{TM} solution.

Behavioral Analytics

Sonet.io uses advanced AI and ML techniques to ensure that any abnormal user behavior is detected and reported, and actions are taken to prevent potential data leaks or security breaches into the enterprise.

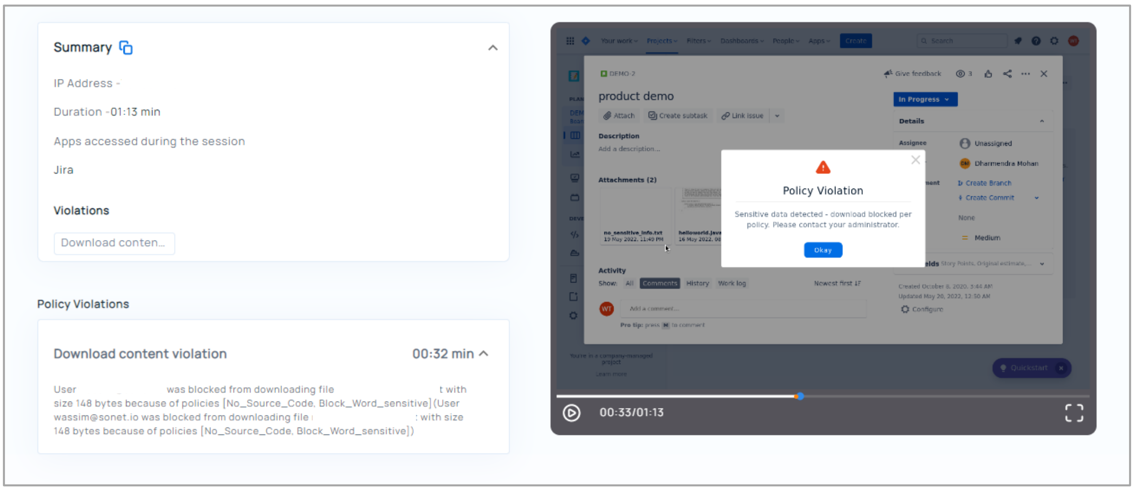
The solution learns regular user behavior, and any deviations from this behavior, which can be an indication of a security threat, are immediately detected. For example, a contractor starts downloading or uploading a large number of files, contrary to their normal behavior, will generate an immediate alert and access can be blocked or an MFA can be enforced in real time. Another example is a partner that is accessing applications from two different locations at the same time, which indicates a potential credentials theft, results in forcing an authentication or blocking that user in real time.

Visibility and Forensics

Full visibility and the ability to perform forensics are critical to ensure compliance and detect any potential attacks or data leaks for any 3rd party access.

User activities and access to applications are logged, all policy violations are reported in the log management tool, and administrators can be notified in real time about the most important events. In addition, full user session recordings are available, allowing the security teams to perform deep forensics.

These capabilities are critical for any customer, particularly when compliance with regulations requiring detailed audits and reporting is needed.



Summary

IP Address -

Duration -01:13 min

Apps accessed during the session

Jira

Violations

Download conten...

Policy Violations

Download content violation 00:32 min

User was blocked from downloading file t with size 148 bytes because of policies [No_Source_Code, Block_Word_sensitive] (User wassim@sonet.io was blocked from downloading file : with size 148 bytes because of policies [No_Source_Code, Block_Word_sensitive])

Policy Violation

Sensitive data detected - download blocked per policy. Please contact your administrator.

Figure 4. Sonet.io user session recording example

Summary – Sonet.io application and data access and protection

As 3rd party users are becoming an integral part of any organization’s workforce, it is crucial that enterprise applications and data they are accessing are protected from any potential threats and confidential and sensitive information leaks. Sonet.io Trusted Access™ was created to solve the challenges of today's “workforce anywhere”.

Built from the ground up, Sonet.io enables workforce access at enterprise scale with a 15 minutes time to productivity onboarding capability coupled with beyond industry standard security controls. Sonet.io enable workforces to work, quickly and securely from anywhere and any device.

Next Steps

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