SONET.IO

SECURING ACCESS TO APPLICATIONS AND DATA FOR YOUR REMOTE WORKFORCE

Frictionless trusted access solution that continually assess risk to protect data and applications with zero agents so your business moves faster

sonet.io

www.sonet.io
info@sonet.io

CHALLENGE

Enterprises of all sizes need to secure access to their applications, servers and data for their remote workforce for managed and unmanaged devices

SOLUTION

A trusted access SaaS service that continually assess risk to protect data and applications with zero agents and zero deployment, so your business moves faster

BENEFITS

- Secure access for all your remote workforce to all SaaS and web applications and servers from managed and unmanaged devices
- Centrally control access with granular advanced policies that includes behavioral analytics to detect and block any abnormal user behavior
- Prevent sensitive data exfiltration through comprehensive data protection and inspection
- Protect your applications from vulnerabilities and cyberattacks without requiring a VPN or endpoint agents
- Improve productivity and reduce operational cost without compromising users privacy with a solution that is ready in minutes
- Meet your compliance requirements with all applications' access and activity records instantly available

With the increase in remote work and the need to collaborate with third party vendors, partners and contractors, customers face several challenges securing access to their enterprise applications and servers, in order to protect their data and intellectual property. The average cost of a data breach in the US in 2021 was over $9M according to a report by the Ponemon institute. In addition, these data breaches result in credibility and reputation harm. With the exponential increase in cybersecurity threats and attacks such as ransomware, it is more important than ever to have easy to implement solutions that provide a strong security with the right visibility, while improving productivity rather than hindering it. Only sonet.io offers such a comprehensive solution.

TODAY'S CHALLENGES

Today's enterprises face major challenges when it comes to securing access to applications, servers and data for their remote workforce:

- They have no control over vendors', partners' and contractors' devices accessing their applications and data
- They have no control over their employee devices when they use BYOD
- 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 very little to no visibility into user activity when accessing applications and data
- Today's zero trust and private access solutions are complex, take months to deploy and leave security gaps

The sonet.io 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 between users and applications, elastic scaling and high performance.

The sonet.io Trusted Access™ Solution

A holistic approach to applications and data security

To address customer challenges, sonet.io built a highly scalable architecture that simplifies the way applications, servers and data are secured. The sonet.io SaaS solution is constructed from the ground up to make it easy to adopt and put in place with no requirements on endpoints or applications.

The solution augments its 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 ZTNA (Zero Trust Network Access) where users access to applications and data is continually 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 and intellectual property information.

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

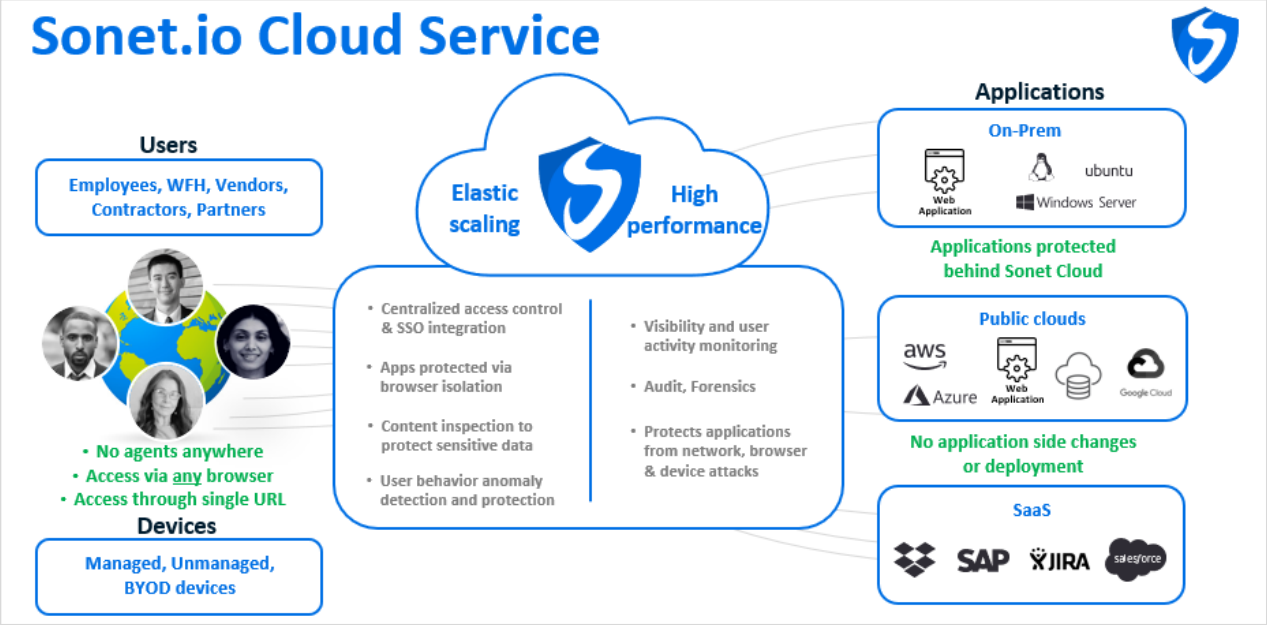


Figure 1. sonet.io Trusted Access™ architecture

Secure Access for All and Ease of Adoption

The sonet.io solution is built for easy adoption by users whether they are employees with managed or unmanaged BYOD devices, vendors, partners, or contractors with unmanaged and uncontrolled devices. Users only need a browser to securely access enterprise applications and servers, and can still enjoy their privacy when accessing any other applications. This removes the barrier of adoption from users and improves productivity and reduces cost by enabling the access to applications without any agent deployment and management.

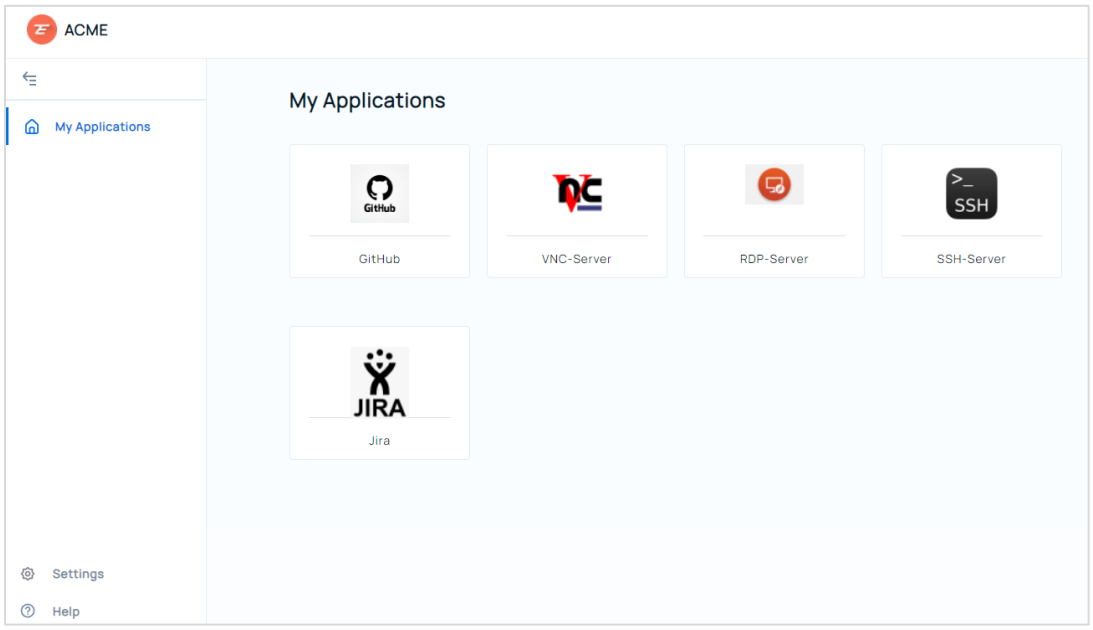


Figure 2. One-click dashboard and full privacy for users' private applications

Any browser can be used to access the sonet.io portal, which presents the user with a dashboard of enterprise applications to which they have been granted access. In a single click, users can access any authorized application from the sonet.io portal through a single sign on mechanism. Users can access their private applications or web sites in the same browser without interference or monitoring from sonet.io. The sonet.io service only monitors activities between the users and enterprise applications. This ensures users' privacy while maintaining strict security to the enterprise assets.

The sonet.io solution provides secure access to all SaaS applications, web applications as well as servers with ssh, rdp and vnc support. Applications can be running in the private or public clouds or on-premise. There is no need for any deployment in front of the applications, such as application connectors, or any changes to application configurations.

Centralized Access Control

Sonet.io access policies to applications allow for a fine grain control over what users can perform on applications. Administrators are able to put in place sophisticated allow/deny policies and advanced behavioral-based policies.

Access policies can be built for a strong authentication and authorization where users are required to use MFA (Multi-Factor Authentication) to ensure proper identification at login. Also, additional MFA can be used during users' sessions to ensure it is always the right user accessing the applications. Access policies to allow or deny access to applications can be based on several criteria, such as time-based or location-based policies.

Advanced behavioral analytics tools using Artificial Intelligence (AI) and Machine Learning (ML) techniques allow customers to apply policy rules on any abnormal behavior. For example, if a user who does not usually download files, starts downloading a large number of files, an abnormal behavior is triggered. The administrator can use policies that send a notification about the abnormal behavior and optionally forces the user to re-authenticate or block the user from accessing the application and data.

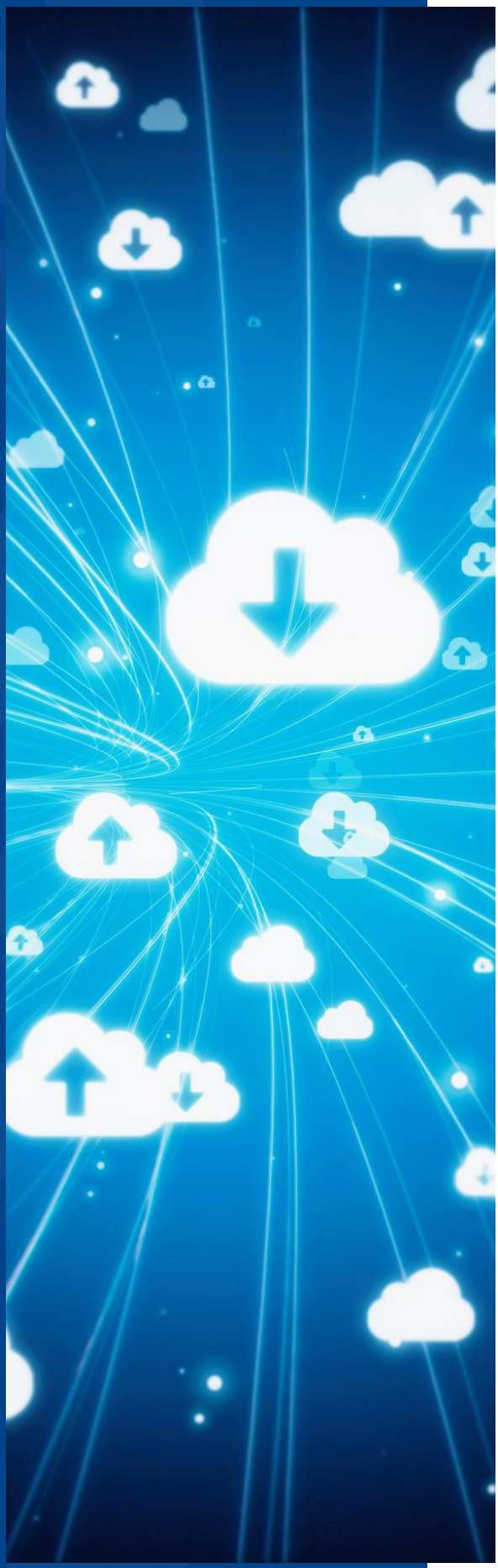
Protect Data and Apps

With sonet.io customers can rest assured that their data is safe from potential leaks. The data protection technology in the sonet.io solution offers the ability to block any download of sensitive data. Administrators can define policies to trigger alerts on downloads that contain confidential data, such as bank account information or social security numbers. These policies do not require specific integrations and apply to all applications without the need to adapt them to every application like other solutions in the market.

In addition to pattern matching, the sonet.io service provides advanced OCR (Optical Character Recognition) techniques that analyzes images or hand-written notes to prevent data leaks.

Data obfuscation is another capability that is offered by the solution. Sensitive data can be redacted on downloads so that it is hidden. Also, data redaction can be used with copy and paste functions where confidential information is obfuscated.

The sonet.io service protects from any types of browser and network attacks that can result from malicious intent or from compromised devices. The sonet.io solution provides a complete isolation that keeps the applications and data safe from any potential threats from the users and their devices. As all the communication between users and applications flows through the sonet.io service, downloads, uploads, URLs and user behavior are inspected for potential threats.



Ease of Deployment

The sonet.io solution does not require any agent installation on endpoints. There is no need to manage endpoint software and deal with continuous updates of software and security certificates, removing the barriers to deployment and adoption. This reduces operational costs and eliminates downtimes resulting from expiring certificates or updates needed on the endpoints. It also helps employees, vendors and partners to be productive in minutes versus days or weeks.

The same ease of deployment applies to the applications side, where no connectors or software deployment is required. Administrators can configure the applications directly in the sonet.io portal for access control. Data access policies apply seamlessly to all applications or a subset of applications and their data and do not depend on the nature of the applications, making it very easy to use the same policy and apply it to any application.

The sonet.io solution seamlessly integrates with your identity management and IdP and Single Sign On (SSO) solutions such as Okta and Azure AD. You can leverage your existing deployment for multi-factor authentication and single sign on within minutes.

Enables Compliance

Compliance requirements can be very stringent and difficult to meet if a solution does not provide the right tools and audit capabilities. With sonet.io, customers have full logging capabilities of all events between users and applications: access events, policy violation events, behavioral anomalies, etc.

Sonet.io logs can be imported into existing SIEM solution such as Splunk to enrich the data collected by those platforms and help with the broad analysis of networking and security events.

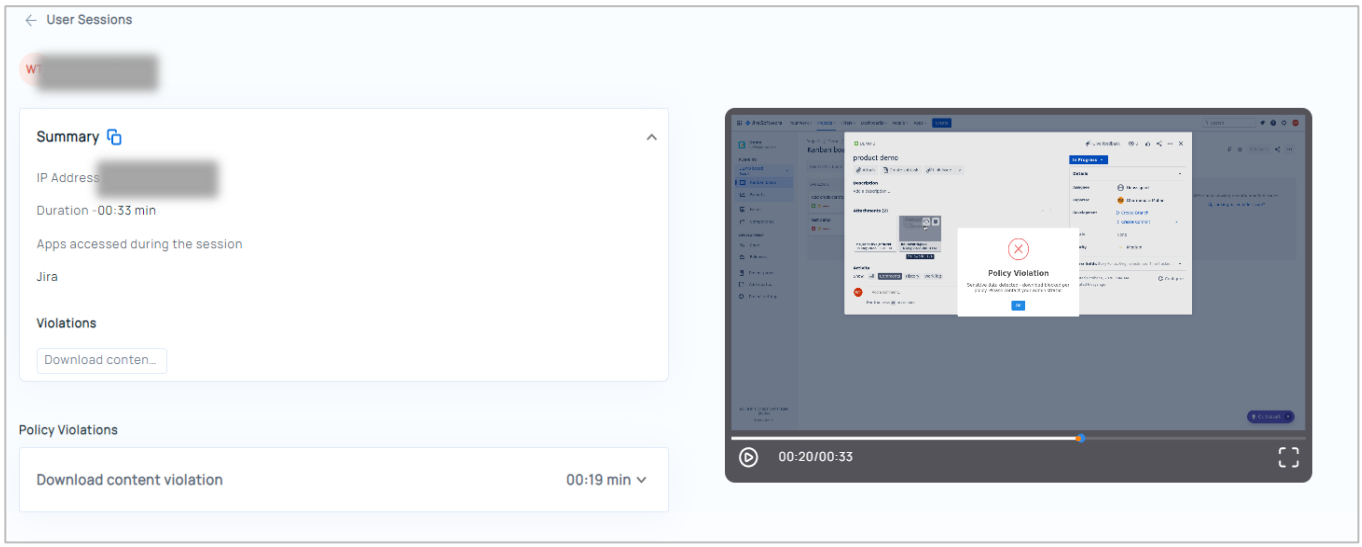


Figure 3. sonet.io session recording and playback capability

A powerful capability of sonet.io is the full session recordings of any users' sessions highlighting policy violations. The sonet.io solution enables administrators to selectively determine which application sessions need to be recorded. This is very important for critical applications that may contain sensitive data. A full preview of sessions with times of policy violations are recorded and can be played back for deep forensics analysis and audits.

Summary – sonet.io Trusted Access™ for application and data protection

The trend of enterprise transformation to become fully distributed with applications, data and users becoming all remote, makes it very challenging for CISOs and IT personnel to secure applications and their data. The problem becomes even more complex for unmanaged devices, such as BYOD devices, partner and contractor devices. There is a need for a different approach than what the market is offering today.

Sonet.io provides a comprehensive solution to this challenge and offers a simple to adopt and deploy solution that removes the burden of managing endpoints and application connectors without compromising security. It is the next generation of the Zero Trust solutions for the remote enterprise.

NEXT STEPS

To learn more about sonet.io solution, please contact us at info@sonet.io.