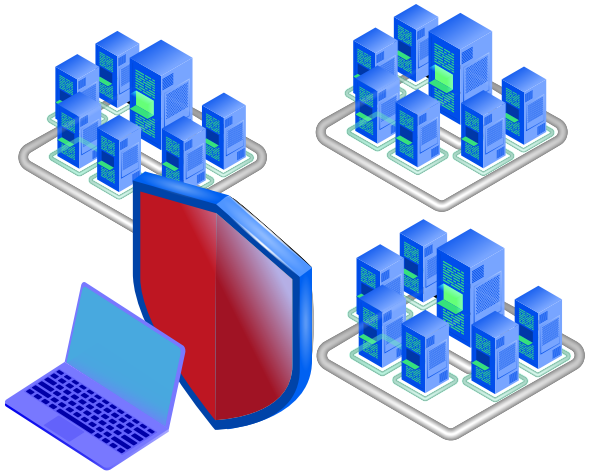
Secure Remote Access

Four Reasons it's Important and Three Places to Apply It

Introduction

As an organization's infrastructure becomes more and more connected and complicated, it becomes more important than ever to have a safe and protected way for employees to access systems remotely. This is not just a challenge for IT environments, but OT environments as well. Nearly half of the Fortune 2000 organizations consider OT networks to be critical components of their business[1]. It's essential to make sure that these are protected—while administrators are able to successfully do the work that needs to be done.



What Is Secure Remote Access?

Secure remote access refers to any security policy, solution, strategy or process that exists to prevent unauthorized access to your network, its resources, or any confidential or sensitive data. Essentially, secure remote access is a mix of security strategies and not necessarily one specific technology like a VPN [virtual private network].

— Bernard Brode,
AT&T Cybersecurity

Why It's Necessary

1. **Provides Decision Makers with Necessary Visibility**
   Decision makers need visibility into what is happening in their environment in order to make the best possible choices. Without the necessary data being delivered in a timely manner, these individuals will not be able to successfully do their job and make the decisions that will ensure the organization and its data is properly safeguarded.

2. **Centralizes Geographically Distributed Systems**
   Many organizations have OT assets in different geographic locations across the country or the world. It's important that the necessary users are able to access data from these assets no matter where they are. Secure remote access allows authenticated users to see a full picture of their environment, and monitor assets from anywhere on the globe.

3. **Work More Easily With Third Parties**
   Many organizations use third party vendors, contractors, and suppliers. By giving these third parties secure remote access, you will be able to deliver the key information that they need directly to them, rather than giving them access to your entire environment.

4. **Ensures Important Updates Are Made**
   Many equipment manufacturers of industrial control systems are responsible for providing remote maintenance. By providing secure remote access to these manufacturers, they will be able to ensure this maintenance is done. Without this, an important update may be missed, or they may be unable to fix a bug or malfunction.

Where To Implement It

1. **The Machine Zone**
   The machine zone consists of the machine control equipment in an organization's industrial environment. A larger organization will often have multiple machine zones so that different areas of their industrial processes are kept separate. When combined together, this is called the plant zone.

   It is best to have a dedicated remote access gateway as opposed to a PC with a remote desktop connection.

   A PC will put you at a higher risk of digital attacks for a few reasons:

   - A malicious attacker could compromise your device through use of the PC's advanced networking capabilities. From there, they'd be able to access certain parts of your environment they could then leverage to launch attacks from.
   - A PC has a full operating system with its own vulnerabilities. Usually, the system integrator or machine builder is responsible for addressing these issues, so it may not be a part of your organization's patch management strategy. This leaves you with vulnerabilities that you may not be aware of or able to address.
   - PCs are not typically equipped with the components to successfully manage industrial control equipment. This means you would need to get another software package in order to do this monitoring.

Where To Implement It

2. **The Enterprise Zone**
   The enterprise zone includes the organization's personal computers, customer databases, and other IT assets. It often contains security solutions to protect these assets.

   Your organization may consider a VPN to protect these resources. However, the shortcoming here is that a remote user may have access to more than they need. If a remote worker's account is compromised, that malicious actor will have a great amount of sensitive data at their fingertips. Additionally, there will need to be a connection created between the enterprise zone and machine zone, creating additional vulnerabilities.

   A remote access gateway is a superior option because this will limit the machine networks to limited visibility. It will also keep the organization's enterprise network separate from the machine zone.

Where To Implement It

3. **The Outside Zone**
   The outside zone consists of all the key assets outside of the enterprise zone, such as remote users' computers and cloud connectivity services.

   Some relatively labor-intensive solutions may involve having remote workers download a software package onto their PC. However, the downside to this is that IT will need to check if updates are available, and that the updated software is installed on the computer. Another worry of this is that an attacker may be able to fool a remote user into downloading something that looks like an update, but is really something malicious.

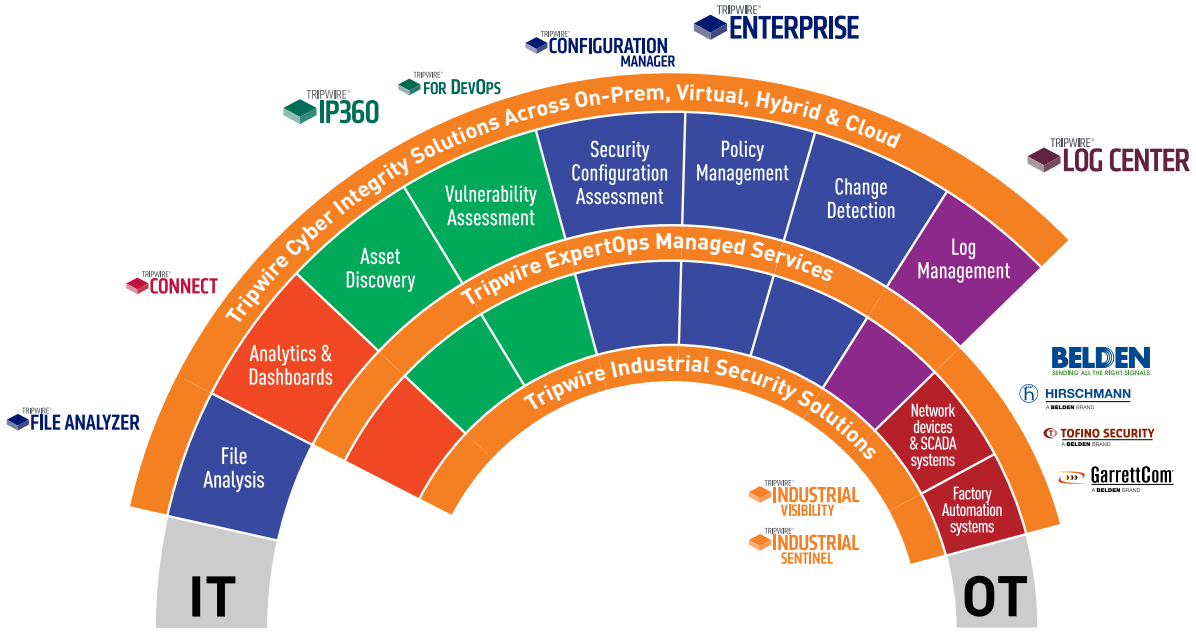
   You may also consider a free VPN tool that can be downloaded with a static public IP address, instead of two-factor authentication. However, this creates more work for your security team—as they will have to constantly check for vulnerabilities and watch for security updates.
   Instead, opt for a remote access gateway. Many of these don't require any user-installed software, saving you time and work. Additionally, they often rely on containers that run only the microservice components needed by the application. This means that a security flaw will not have as large of repercussions on your OT environment.

Next Steps

Secure remote access is a crucial component for keeping your OT environment properly managed and protected. Tripwire can help you build out secure remote access in your environment with its robust solutions specifically designed for ICS environments. Learn about how Tripwire solutions, including Tripwire Industrial Visibility, can improve your security posture.

Schedule Your Demo Today

Let us take you through a demo of Tripwire's security and compliance solutions.
Visit tripwire.com/contact/request-demo



1 Antova, Galina. "How to Address the Surging Need for Secure Remote Access to OT Networks." SecurityWeek, 24 Mar. 2020, www.securityweek.com/how-address-surging-need-secure-remote-access-ot-networks

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

BRSRA1a 2101