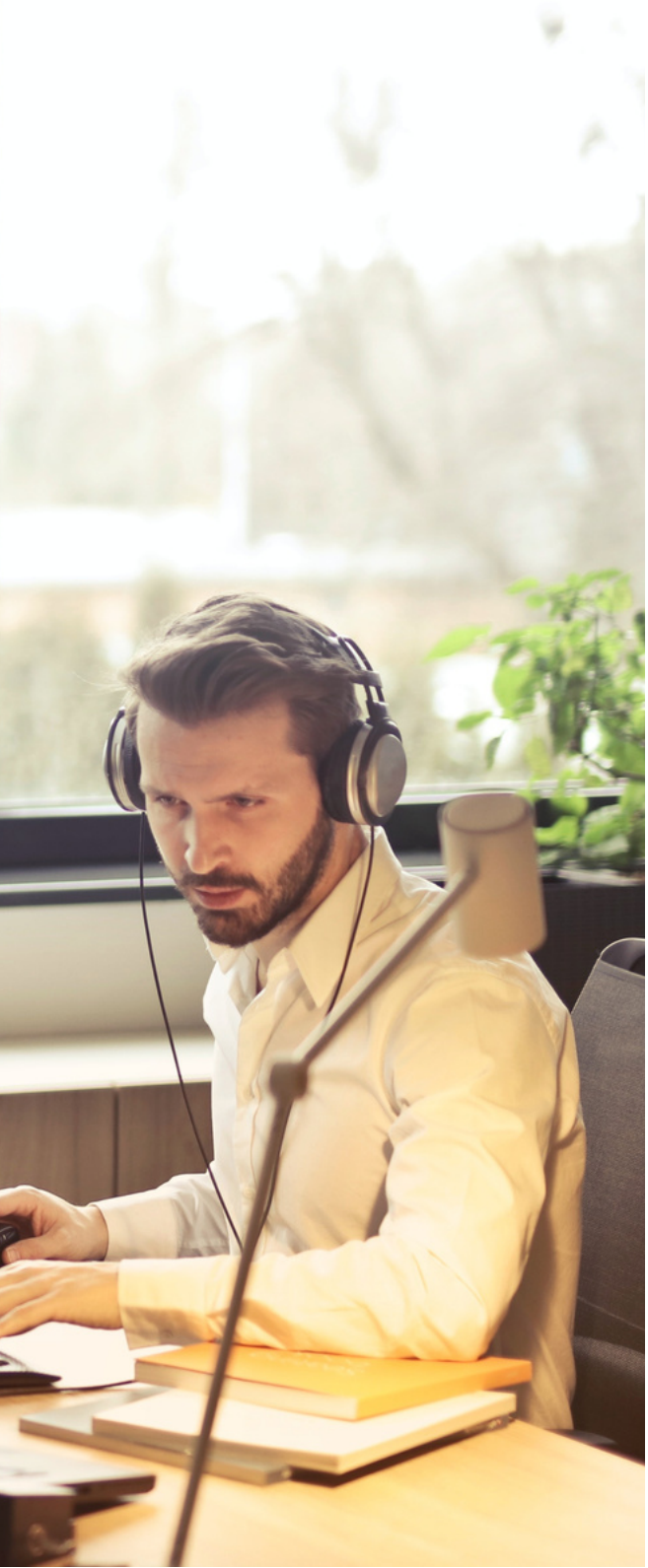
ASSERTION®

# THE ONLY GUIDE YOU NEED FOR VOIP REMOTE WORKER SECURITY

APRIL 2023 // PREPARED BY ASSERTION INC.

# INTRODUCTION

By 2025, cybercrime is expected to make more money than the global illegal drug trade. And given how the VoIP market is slated to grow – at a CAGR of 15% – it's sure to be a hotbed of activity



Today, VoIP networks are an accessible and juicy attack surface but remain grossly under-acknowledged by security organizations. There's another aspect that adds a layer of vulnerability to the existing security challenges – the rise in remote worker VoIP deployments after the Covid-19 pandemic.

A study found that 20% of organizations experienced a breach because of a remote worker.

According to IBM's Cost of a Data Breach report, the cost of the average data breach cost increased by over $1 million whenever remote work was a causal factor. Additionally, it took organizations with a remote workforce 58 days longer to identify and contain the breach than office-based organizations.

It's safe to say this: Remote work can result in more frequent – and more costly and damaging – breaches!

At Assertion, we're committed to making VoIP Security a priority. By driving dialogue and discussion around it, we hope to create a safer and more secure world for Voice Communications… and it all starts with awareness and education.

We created this ebook to simplify the world of VoIP Remote Worker security through a series of 3-minute reads. The chapters in this book discuss the state of today's landscape, common VoIP security threats, and insights to improve your understanding of remote VoIP security and its unique challenges.

We are confident that you will come out with an improved understanding of the need for security in remote worker VoIP deployments.

**More importantly, we hope that the book helps you do your bit to create a more secure world for Voice Communications.**

# Table of Contents

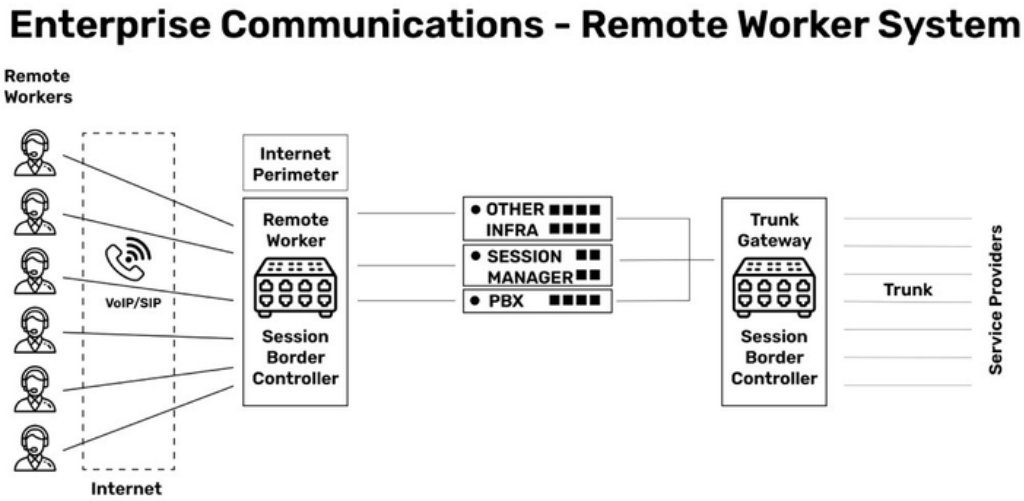


# CHAPTER 1: AN INTRODUCTION TO REMOTE WORKER VOIP SECURITY

In our context, remote workers are folks who use voice and video communication devices from outside the office. When COVID pushed everyone to work from home, companies scrambled to enable all kinds of infrastructure for remote use. This included a remote worker setup to facilitate voice and video communication for remote workers.

**Session Border Controllers (SBCs) have a big role to play here.**

Let's take a minute to look at this diagram just so we are all on the same page about terminology.




SBCs deployed at the edge of enterprises, control and regulate all forms of real-time communications including VoIP, video, and collaboration sessions. The diagram above describes a classical remote worker setup for communication infrastructure.

The normal telephony infrastructure is sandwiched between two SBCs:

- On one side, remote worker clients get connected to remote worker SBCs, which act as firewalls and attempt to block bad actors from coming in over the internet.
- On the other, the trunk is connected to another set of SBCs, which block bad actors from coming in from the trunk side.

**A little history:**

Over the last two decades, companies all over the world have been switching to VoIP (usually SIP) on the trunk side. But because this was a steady and planned move executed over many years, SBC deployments on the trunk side are mature, and therefore, relatively far more secure than the remote side.

Here's why: Many companies, in the urgency of enabling remote working voice and video, set up remote worker SBCs without paying attention to their security and configuration. Several others simply assumed that dumping a firewall in front of the PBX before enabling remote work was sufficient.

Both are huge security risks. We will discuss why further below.

Assertion's State of SBC Security Report, the first-ever study on how secure the voice and video perimeter of most companies is, found that:

- An average SBC gets probed within 5 minutes of going online.
- Over 50% of internet-facing SBCs were at high risk – due to misconfigurations.
- Adherence to basic security practices was worryingly low. For instance, security best practices require that certificates older than 13 months be renewed. But 86% of the SBC certificates we examined exceeded that limit. Of those, 70% were older than 24 months.

And the thing is, the study only reviewed Internet-exposed SBCs. It's a pretty good bet that most of them are for remote workers. You see, for management and security reasons, most companies keep their remote worker and trunk-side SBCs separate.

**THE BIG LESSON**

**There's a pretty good chance that remote worker voice and video systems are insecure and exposed to the internet. This means a remarkable number are being attacked and breached!**

**Now, why is remote worker security such a mess?**

- **Vulnerability assessment falls short** - Standard platform-based vulnerability assessment tools including patch management tools, only look at known platform vulnerabilities such as OS vulnerabilities, databases, web servers, etc. — the SBC, a VoIP system's only internet-exposed application, is left unchecked.
- **Current security-by-design standards fail for SIP** - Firewalls, normally installed in front of SBCs, do little for SIP security. They merely pass them through to the SBC, making its configuration and security a high priority. Current models do not investigate the SIP traffic on a call-by-call basis to detect attack any abnormal activity.
- **Static security reviews offer no real value** - Security hardening, typically carried out once a year operates in isolation without considering what's happening to the SBC this minute. This means that it fails to review the SBC's configurations on an ongoing basis and reconfigure them dynamically based on the traffic passing through the SBC.
- **Zero to low awareness of the types of attacks on SBCs** - SBCs are complicated devices and attacks on them pose unique safety challenges. VoIP teams have no way to track and stay updated on the unique security challenges that SBCs face.

These make the security of SBCs a blind spot with:

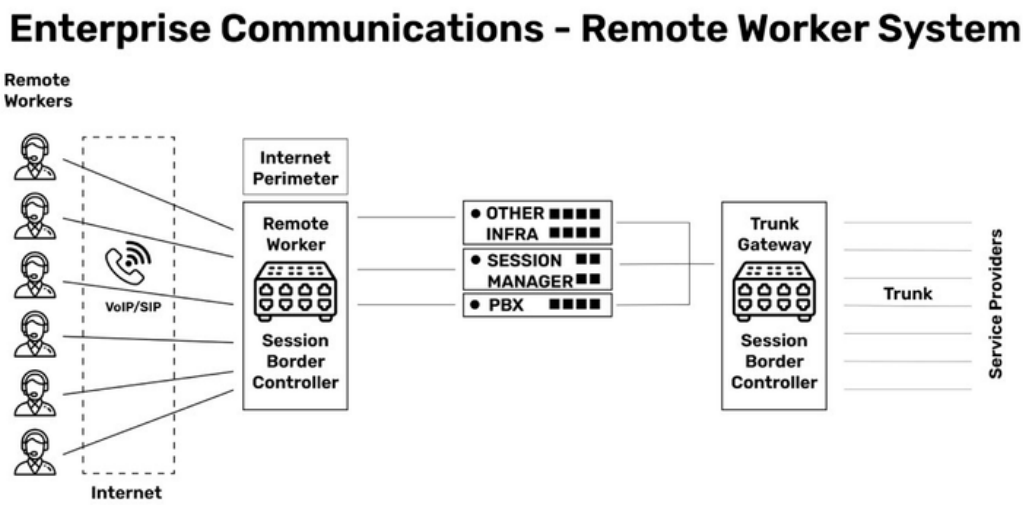
- No attack visibility till they escalate into breaches.
- No reliable threat intelligence for attack prevention.
- No centralized visibility into multi-vendor or geo-distributed SBCs.
- No integration into standard SOC practices.

In summary, remote worker security is a niche that needs to be studied in more detail – threat actors are already beginning to sharpen their attacks on this attack surface – and it's up to us to figure out how to protect our networks here.

The next chapter focuses on the key attack vectors for remote workers, and how to avoid being a victim.

# CHAPTER 2: HOW DO VVOIP REMOTE WORKERS GET ATTACKED?

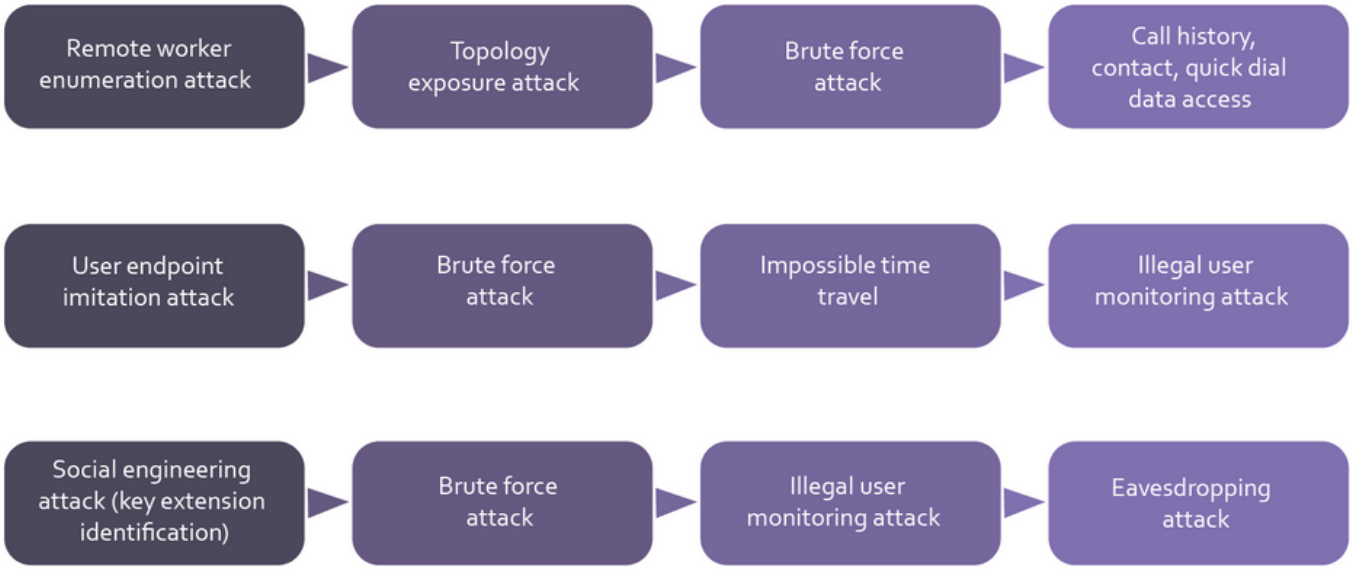
Here's a quick recap of how communication systems work for remote workers.




When we look at the diagram closely, we can almost immediately see some of the challenges of securing this setup. Remote workers connect over the Internet to the company network. The most obvious security challenges are:

1. Is the requested call connection coming in from a bona fide caller?
2. Is the requested call connection coming in from a bona fide endpoint?
3. Has the call been hijacked along the way?
4. If some connection requests come in with 'mangled' protocols, are these real connection requests or attackers?
5. If some connection requests come in from unusual locations, are these real requests or attackers?
6. If duplicate connection requests come in from the same remote worker, are these real or attackers?

While firewalls can check at the IP level, they are helpless at the SIP level because they do not understand the protocol and simply pass it on.
These are not abstract threats. And the outcomes of attacks on remote working infrastructure are serious. Even a single broken-in extension can act as a jumping-off point for a whole series of additional attacks. For example, enterprise toll fraud almost always occurs as an outcome of remote worker security breaches.




# A Remote Worker Use Case for Voice

Here is an example of how remote worker security issues play out in the real world.
A major city transportation authority was an unsuspecting victim of several data exfiltration attacks and a successful takeover of nearly 50 of its remote worker extensions. The organization had been seeing a high percentage of call failures and de-registrations in its voice systems for several months. However, given its large call volumes and distributed workforce, these signs went unnoticed and predictably, raised no alarm. However, they were symptoms of undetected data exfiltration attacks. Let's look at how attackers went about doing this.

## The Groundwork

1. Attackers release crawlers on the internet to constantly look for devices to scan, often using the services of IoT search engines like ZoomEye, Shodan, and so on.
2. When a crawler identifies that a device is an SBC or an exposed PBX, they begin a probe into the device, looking to gather as much information as possible about the device.
3. Attackers then collect specific information like valid extensions, OEM vendors, etc., to plan the next level of attacks: brute forcing a valid extension.

## The Impact

Attackers were found to be monitoring 25 users for nearly two months while tracking all call activity on their lines. This opened the possibility of user impersonation, lateral attacks, privilege escalation, and so much more. Remote workers' compromises are gateways to a series of other attacks and compromises.

Interestingly, attackers had the opportunity for toll fraud but chose not to exercise it, possibly because the value of data exfiltration was high enough that toll fraud was a relatively lower value.

# How could this breach have been prevented?

**The short answer: Defense in Depth.**
Here's the slightly longer version: Attacks on remote worker infrastructure are always going to take place, but instead of looking for a magic bullet that prevents attackers from getting through, we need to instead look at putting multiple obstacles in the way of attackers – to slow them down or stop them in their attempt to break through. In this case, some of the barriers that could've been in place are:

1. **Mutual Certificate Authentication:** where the client and the server both authenticate each other. A non-authenticated client would not have been able to connect at all.
2. **Strong URI/URL requirements:** where the SBC would check the software version details shared by the client and allow only approved versions to log in.
3. **Spoof checks:** where the system could examine
    - The protocol details, to see if there are any red flags there, such as mangled or missing headers
    - The IP address to see if it belongs to a blacklist, which may also require access to a living database of such addresses

In the next chapter, we will approach the remote worker security challenge differently. Instead of looking at a specific use case and trying to figure out how to prevent it, we will discuss how to prevent a vast majority of such attacks.

# CHAPTER 3: PREVENTING REMOTE WORKER VOICE AND VIDEO ATTACKS & HACKS

In this chapter, instead of looking at a specific use case and trying to figure out how to prevent remote worker attacks, we will discuss how to prevent a vast majority of such attacks – VoIP security hygiene.

When attackers hit VoIP remote worker systems, they usually:

- Look for data they can steal, such as customer information, company details, address books, and so on.
- Attempt toll fraud by calling high-cost destinations and premium rate numbers.
- Try to covertly listen in to conversations, so they can use it for other motives (ransom, blackmail, data theft).
- Attack laterally into recording systems, voice mail, and so on, expanding the scope of the breach.

And if your company is the victim, here is an overview of some of the potential impacts, starting with the least obvious:

# Remote Worker Breach Consequences

- **Fines and regulatory hassles:** Since the attackers are an uncontrolled element in your network, it is entirely possible that they may end up causing regulatory violations. For example, the attackers may call OFAC-listed countries such as Iran, Syria, or North Korea, which may invite the attention of regulatory agencies. The agencies may believe you when you tell them it was the action of a threat actor, but do you really want to deal with the hassle?
- **Downtime and attention costs:** Imagine you coming home one day and realizing that someone had walked into your house in your absence and taken food from the refrigerator. Nothing else was stolen. Are you comfortable with that? It's not hard to imagine what you would do – immediately start trying to figure out how the intruder got in, how many times he had gotten in earlier, what else has been touched/taken, and how to ensure that this will never happen again. This takes time, effort, and attention. Now imagine you found out that someone broke into your communication network and made only a few phone calls to premium rate numbers. Are you comfortable with that? You'd have to get a forensic investigation done, look at how the intruder got in, and so on...
- **Impact on brand value:** Data loss is a sticky situation to get out of. Even if you don't have their data, people still see it as a sign that you cannot be fully trusted. Again, not fun. Even employees don't want to be associated with a brand they don't trust or respect.
- **Revenue loss to resource misutilization:** Attackers using up resources, which can be especially difficult if you are dealing with high-demand setups.
- **Added costs:** Through (i) the cost of a forensic investigation, (ii) scams like toll fraud. So, there is a serious upside for attackers and often, the downside is quite low. Vice-versa for you.

# How to Prevent VoIP Remote Worker Attacks from Succeeding

In an earlier chapter, we briefly mentioned defense in depth – the idea of having multiple obstacles in an attacker's path – to make sure that the attacker is slowed down/demotivated in his attempts to break in.

Here are the typical actions that attackers undertake when they attempt to break into your VoIP system, and the obstacles you can put in place:

- **Look for exposed SBCs on the internet:** For 'cold' attacks, attackers are constantly querying the internet to look for exposed devices. One of the simplest things you can do is to stay under the radar – just avoid responding to Nmap and similar network scans.
- **Probe for valid extension ranges and supported endpoint types:** Before they can start querying the network, attackers gather information such as extension ranges and supported endpoint types. For this, they will attempt to register on common extension ranges. If attackers have gathered more information through techniques like social engineering, they will attempt to lock one extension for a brute force attack.

**What can you do? Keep an eye on multiple registration failures on a valid extension range?**

Naturally, when an attacker has figured out an extension (and maybe even a password), they will attempt to log in. You can thwart many attempts by

- **Tracking multiple failed attempts at logins** – This would be a sign that someone is attempting to break in. The solution is to immediately block the IP address being used to attempt the logins.
- **Detecting leaked or compromised certificates** – This, of course, would require access to a list of leaked or compromised certificates. Assuming that you have access to such a list and can, in real time, feed it to your SBC, you can configure the SBC to block clients that present such certificates.
- **Looking for rapid user sign-in attempts from globally distributed locations, also called 'Impossible time travel'**. For example, if the attacker has stolen your username and password, and logs in from Florida just a few minutes after you logged out from California – that's a red flag.
- **Identifying improbable geo-locations** – For example, you've been logging in from California all your life, and now your username and password are being used to log in from Moscow.

If the attackers successfully break into your VoIP system, it's still not the end of the road for you. Detection of attacker activity can take place easily inside the network because you fully control the network. You can detect, flag, and act on:

- Attempts to steal user's personal data (user call history, speed dial, address book)
- Attempts to spy on call activity (illegal user monitoring, wiretapping)
- Attackers covertly listen in on live conversations (eavesdropping)
- The activity of known cyber criminals on your SBC
- Outgoing calls made by intruders (for harassment, extortion calls, etc.)

VoIP remote worker attacks are gateway attacks – opening the door to bigger and more dangerous risks, so it's best to be smart and prevent remote worker systems from being compromised.

All communication infrastructure OEMs have capabilities built into their SBCs that can reduce the risk of remote workers – reach out to your SI or OEM to discuss how you can secure your VoIP system.

ASSERTION®

# CHAPTER 4: THE STATE OF VOIP REMOTE WORKER SECURITY

In the previous chapters, we talked about specific challenges in VoIP remote worker security. In this final chapter, we'll talk about what we have seen about the state of VoIP security and how it maps to the larger domain of IT security in general.

Trust is critical for business. If you believe that trust and reliability go hand-in-hand and that communication is critical for your business, communication security is paramount.

Communication systems are subject to the same level of scrutiny from threat actors as data networks. However, data networks are given far more attention than voice networks. This leaves the door open to serious business disruption and loss.

Voice networks, like websites and databases, are applications on the data network, so there are substantial similarities in securing them.

Despite this, we can see that security principles that are regarded as basic in the data world are ignored in the voice and video world. For example:

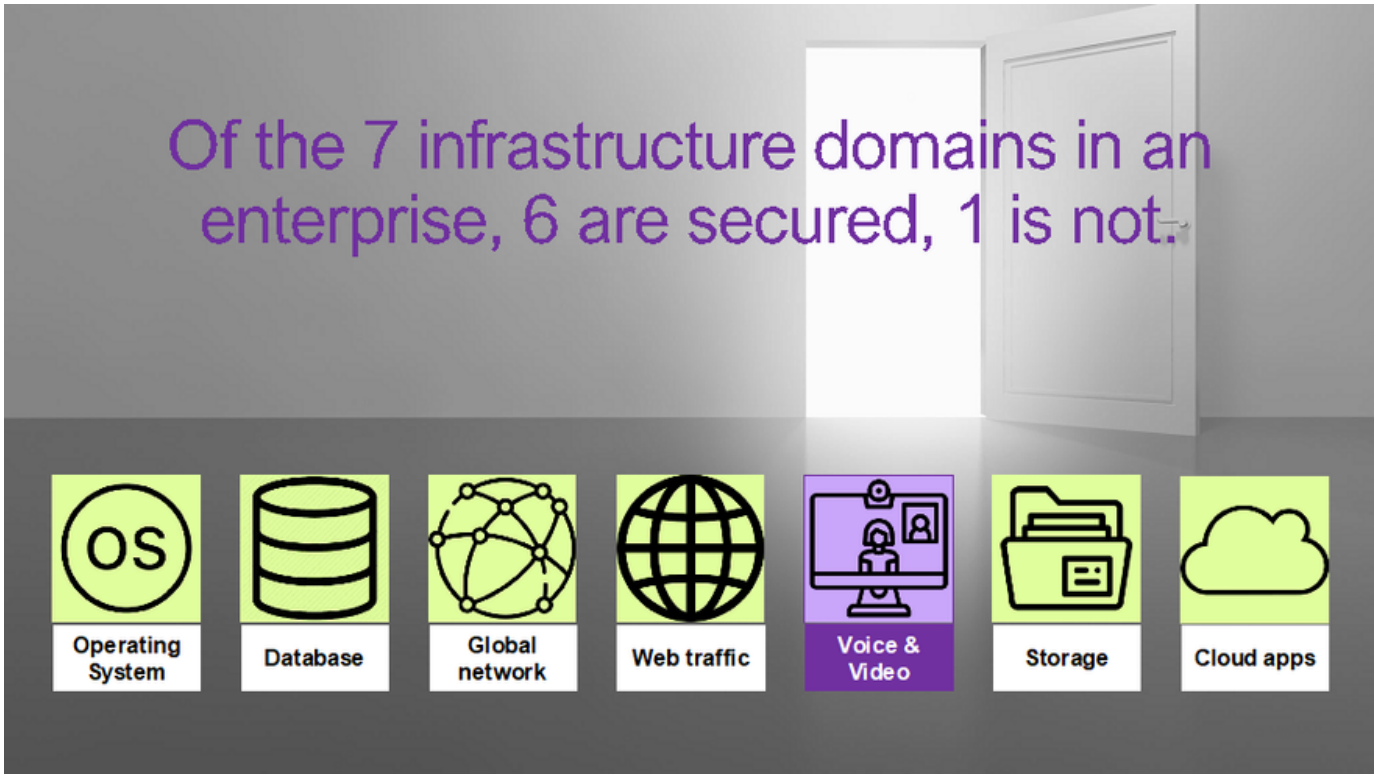
- 28% of the SBCs have one or more administration interfaces directly exposed to the Internet (including ancient, outmoded, terrible-for-security protocols like Telnet and FTP!)
- Almost half (49%) of the SBCs have unsecured interfaces enabled (HTTP, SIP)

(Source: Assertion® 2021 State of SBC Security Report)

Voice networks, even over IP, have significant differences from data networks, enough to need specialized security solutions.

Just as data applications (ranging from WordPress to SAP) need specialized security scans and tests because of the unique interfaces they expose to the Internet, so do voice applications. Vulnerability Analysis (VA) systems and firewalls simply do not have the intelligence needed to guard voice applications against attacks. For example, if a SIP call is coming from a known 'bad' phone number, normal data security systems would not know how to protect against that.

SBCs offer some of these capabilities, but they need access to a constantly updated 'bad list.' At this moment, there are over 20 million numbers from around the world that are known to be linked to fraud and threat actors. Even the best-configured SBCs do not leverage this knowledge.



# CHAPTER 5: HOW ASSERTION® SECUREVOICE™ SECURES VOIP REMOTE WORKER SYSTEMS

Preventing remote worker attacks needs a purpose-built and comprehensive approach to security. At the very least, a robust remote worker security model should enable you to

- Detect multiple remote user registration sessions
- Flag suspicious login attempts
- Detect endpoint breaches
- Catch brute force attacks before they lead to a breach
- Detect abnormal calls or calls from/to non-business locations
- View locations where threats are originating from
- Identify and improve configurations that might be enabling attacks

... and most importantly,

**Give you visibility into – and control over – attacks and breaches, as they happen.**

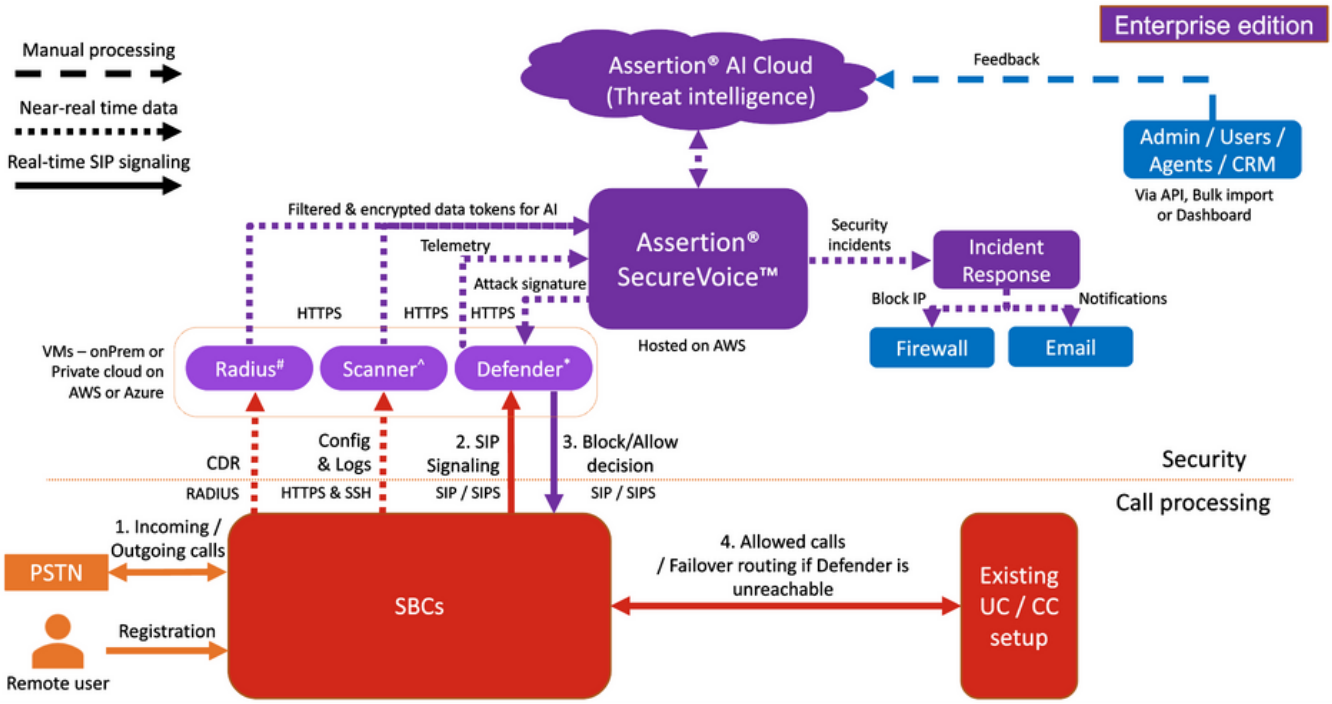
## Assertion's Comprehensive Approach to VoIP Remote Worker Security

The NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and practices. It provides a taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes

# How Assertion® SecureVoice™ Works for Real-Time Threat Prevention

Assertion® SecureVoice™ has two key components:

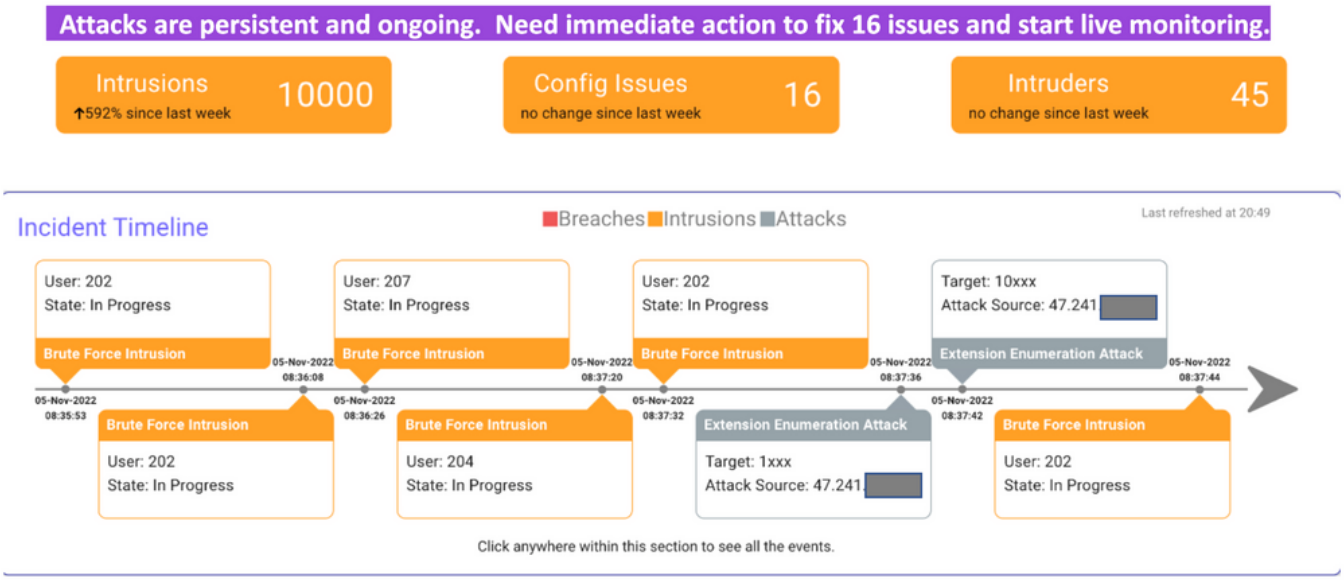
· **A Defender:** This studies every SIP message in real time and analyzes it individually as well as in relation to previous SIP traffic to make Block/Allow decisions.
· **A Scanner:** This collects configuration and SIP trace log data, Syslog, or CDR from the SBC to understand how the SBC appears to a public or private network attacker.




By correlating this information and combining it with the threat intel received from the Assertion AI cloud, the SecureVoice SaaS determines if an attack is underway or not.

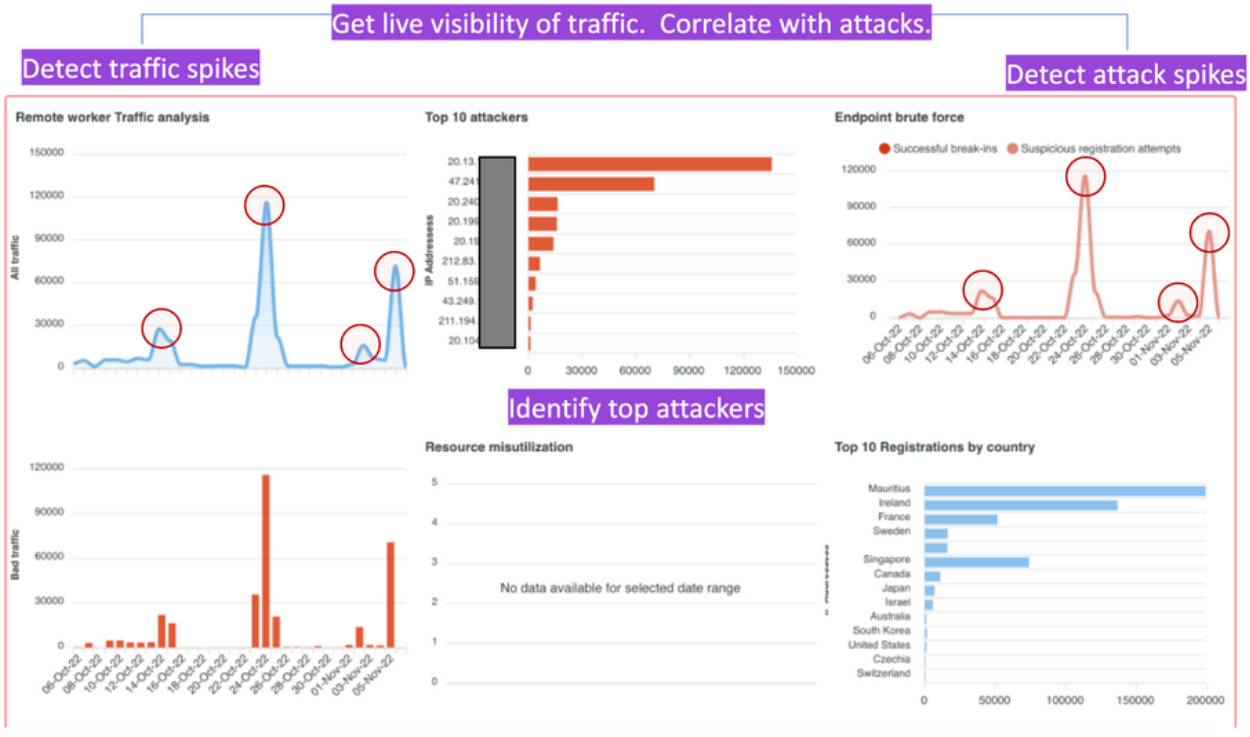
## Assertion® SecureVoice™'s real-time visibility into attacks

# Live Threat view




## All the attack data and evidence you need – at your fingertips

# Last 30 days attack statistics



# What VoIP Remote Worker Security with Assertion® SecureVoice™ Means for You

With Assertion® SecureVoice™, you can

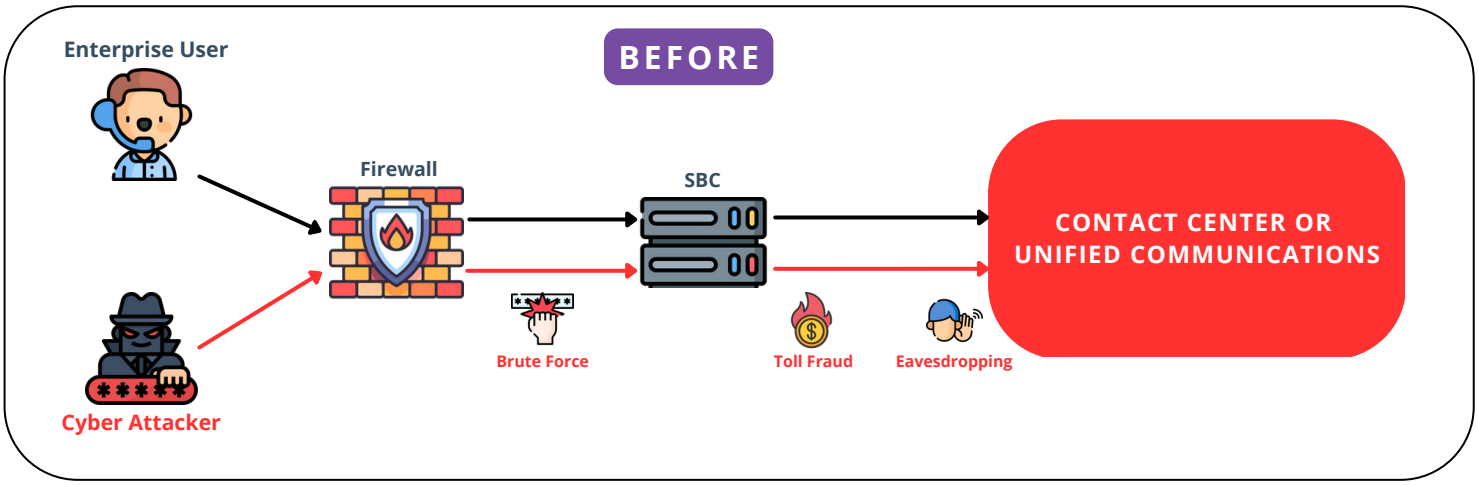
Protect against SBC Break-ins

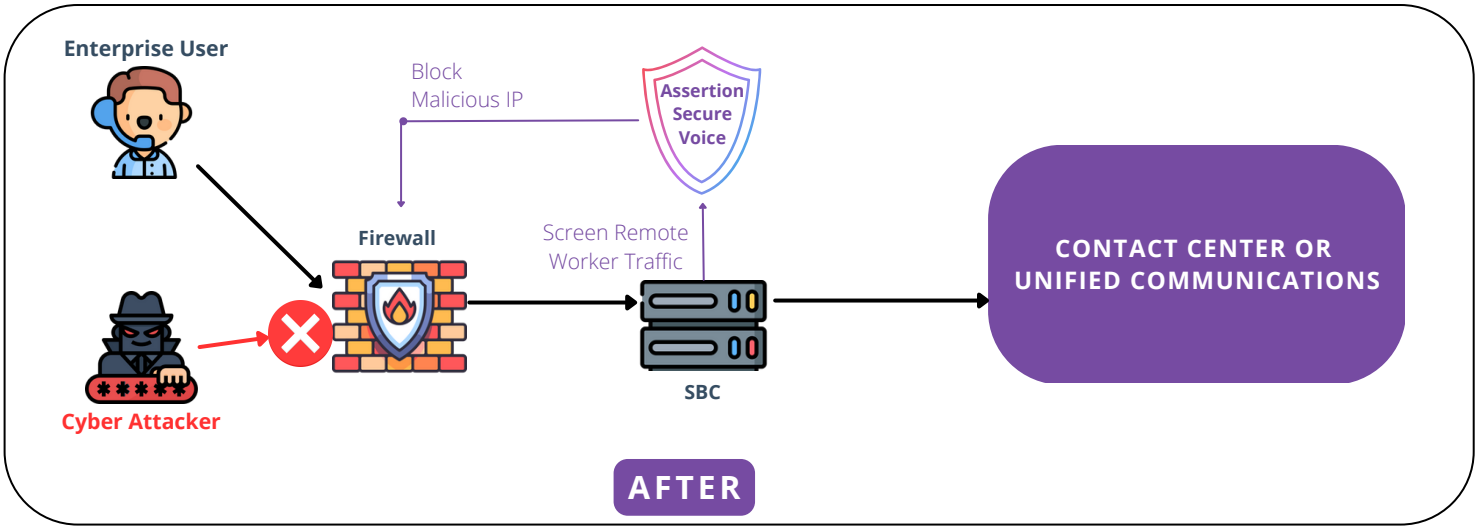
Detect user impersonation

Prevent spying and eavesdropping

Block unauthorized usage

# Experience what True Remote VoIP Security Looks Like



# ASSERTION, COMMITTED TO CREATING A SECURE WORLD FOR VOICE

At Assertion, our ultimate goal is secure every conversation through our advanced security solutions — so companies can Collaborate Confidently.

With over 300 years of cumulative experience in the UC and CC space, our team is backed by industry veterans and trusted experts. Our partners and customers include industry leaders from around the globe.

Our flagship product, Assertion® SecureVoice™ can help you

- Thwart Toll fraud calls and Remote Worker attacks
- Block Scam calls, Robocalls, TDoS attacks,
- Increase outbound call answers,
- Reduce identity theft,

for 360° security for your voice environment.

SEE ALL THIS IN ACTION – IN YOUR SETUP.
SIGN UP FOR A 30-DAY NO-OBLIGATION TRIAL

GET YOUR CUSTOM POC TODAY