Wildix

www.wildix.com
info@wildix.com

SECURE BY DESIGN: WHAT DOES IT REALLY MEAN?

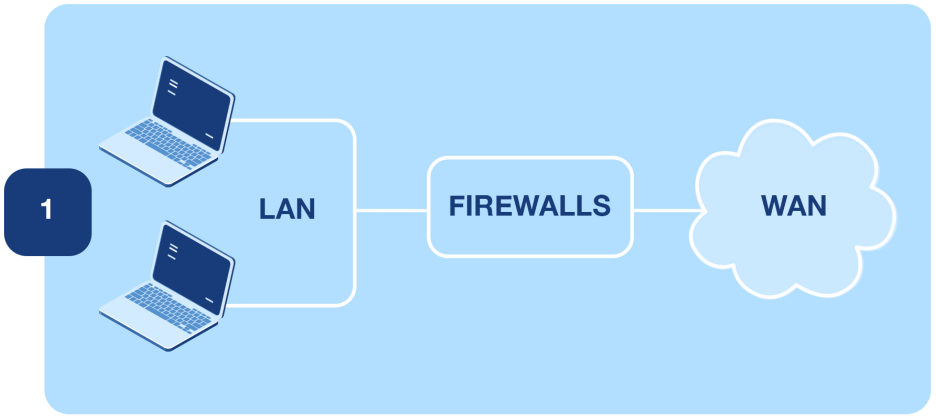
More than a buzzword:
Secure by design means a complete overhaul of conventional security.

With collaboration and business as a whole now primarily taking place online, cybersecurity is paramount to businesses. But too many businesses rely on vulnerable “secured” systems that require extensive upkeep and compatibility checks rather than opting for secure-by-design options. So what’s the difference? Is the distinction insignificant, or is one truly more secure than the other?

The reality is that while a secure system can in theory be protected from malicious actors, vendors often fail to ensure *all* parts of their comms are secure, leading to critical vulnerabilities. Here’s what ends up happening.

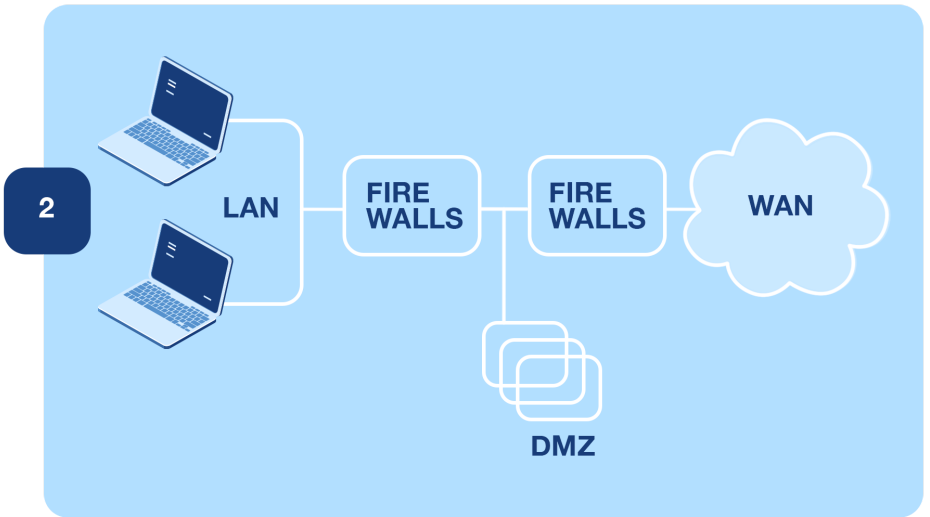
SECURED SYSTEMS

This is the framework for many secured systems:



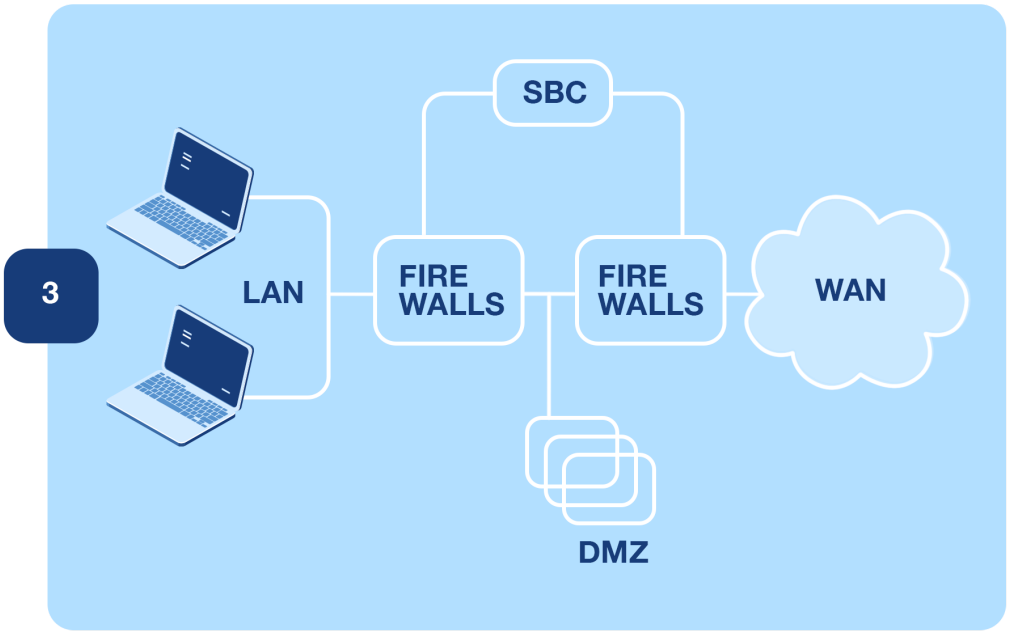
From this, we can see that the system has security added on, in the form of a firewall. In this case, the security is only as good as the configuration of the firewall.

Let's make the system a little more complex by adding in a DMZ, an area that the public can access without accessing the main WAN.



In this case, the two firewalls have to be configured perfectly to allow traffic through. And if you follow the industry standard of having firewalls from different providers, it doubles the chance for a misconfiguration to occur, making access difficult for legitimate users.

In both of these cases, the firewalls are added on top of existing architecture, an example of a secured system. You might also add in an SBC, which allows VoIP traffic through. Again, this must be configured to act in harmony with the two firewalls and the rest of the systems.



Each point represents a critical junction, a point of failure. And it's these points of failure that allow people in who aren't supposed to be there.

HOW DO SYSTEMS FAIL?

One of the most common points of entry for a hacker is through a username and password. These can be obtained through two main means: phishing and through the use of default passwords.

The US CISA notes that "poor security configurations, weak controls and other poor cyber hygiene practices" allow cyberhackers to exploit systems.

These rely on the human element, often someone taking shortcuts in setup or perhaps being a little naïve when it comes to answering emails. As any administrator knows, human error is highly prevalent, no matter how often they warn users and conduct training sessions on basic security.

And a user with incorrectly applied privileges and permissions, especially a C-level executive who doesn't really need them or know how to use them, can be especially problematic. If their account becomes compromised, they are especially vulnerable. Imagine a hacker being able to get control of your email or communications systems and pose as you?

DDoS attacks are almost as bad: They prevent users from accessing systems by flooding points of failure with data. According to Kaspersky, there were 91,052 DDoS (distributed denial of service attacks) in Q1 2022 alone, and 44% were aimed at targets in the US with 5% at those in Germany and 4% at those in the UK.

A common point of attack focuses on older versions of software and firmware. Many devices need to be manually updated, which means they're rarely running on the latest software. As a result, there may be publicly available vulnerabilities that create an opportunity for a hacker to seize control.

Remote services, such as VPNs, are also often vulnerable to attack, especially at the end-points. A compromised endpoint means malicious actors have access to the entire system, resulting in massive security vulnerabilities. Most available systems lack the security needed to prevent cyberattacks on their own, which means you need to layer in other forms of cybersecurity. All this layering can create further incompatibilities, especially when you have to make everyone remote suddenly. VPNs can also require partners to have direct access to the LAN for configuration purposes.

Worse, when you set up VPNs, you need to do it on a per-user basis. What happens when you have 200 people to migrate to a new VPN?

All of these issues can potentially be mitigated through sufficient time, money and effort.

But there's a faster, easier and all-round better way.

Wildix

ELIMINATING POINTS OF FAILURE THROUGH A SECURE BY DESIGN APPROACH

The UK government advocates for strong security to be built into internet-connected products from the start. These products should be "secure by design".

Secure by design fundamentally means ensuring that security is considered from the start of the design process. You limit the points of failure, whether it's by reducing human input (and therefore human mistakes) or ensuring the design is efficient and doesn't require extra pieces of security hardware to remain secure. And you make it easy to use and install.

Authentication

At the start of any secure-by-design product lie 2FA and SSO.

SSO: Secure sign-on. This is built on a trust relationship between a service provider and an identity provider (e.g., Google or Facebook). The SSO identity provider authenticates the person's identity, and then they can sign in.

2FA: Two-factor authentication. This uses two factors, often a username/password combo plus another factor, such as a code delivered to a pre-registered device. Typically, SSO identity providers will use 2FA to authenticate users before they use SSO (e.g., how Google sends a message to your Android phone before you can use Google on a new device or browser).

These help prevent unauthorized use. In addition, they help remove the need for extensive password libraries, ensuring people only have to remember a couple of essential passwords.

Overall, 2FA and SSO reduce the first point of failure: Passwords.

Wildix

Encryption

Only 17% of companies have encrypted more than half the data they store in the cloud, despite 40% reporting a breach in the 12 months to October 2021.

But there's little point in being secure at the beginning if you're not secure the whole way through. That's where encryption comes in. A typical set of security protocols might include the following:

TLS

Transport Layer Security encrypts data as it moves between applications and servers

SHA512

Secure Hash Algorithm 512 converts text into strings to secure it, including digital records.

AES128

Protects data as it's at rest, ensuring security throughout the system.

Taken together, these encryption methods render exchanged data unusable to hackers, as if messages are intercepted, they will be in an unintelligible state. Using multiple up-to-date encryption procedures increases the complexity of the messages and thus makes them more difficult for unauthorized parties to decipher and use.

This question is vital:

Does your communication solution protect data from cradle to grave for data, video, audio and text? If not, why not?

The problem is that unsecured data can be intercepted relatively easily as it passes through various systems. Encryption throughout the process reduces another point of failure.

Wildix

The cloud computing market is expected to grow to nearly $1 trillion by 2026, from $445 billion in 2021

At some point, the vast majority of telecom solutions will end up traveling through the cloud, and it's here where more vulnerabilities manifest. And that's simply because not all cloud solutions are the same. These are the big three:

Broadly, the biggest names offer similar services under slightly different banners. For example, all offer app deployment: Amazon Elastic Beanstalk, Azure Cloud Services and Google App Engine. You also have essentials such as continuous monitoring and interception of malicious traffic, which helps ensure security.

But small cloud solutions and providers offer nothing like this level of security. And that creates issues. What happens if they're compromised? Do they really have the resources to prevent and monitor malware? Do they automate security as effectively as the big three? Even more critically, are they HIPAA and GDPR compliant out of the box?

And if you're interested in government-level security, what about compatibility with AWS GovCloud?

If your comms system uses small cloud providers, the result is a flawed solution. No matter how well they implement their system, the use of an insecure cloud network will result in data loss, breaches and client trust broken.

That's why a secure-by-design approach must consider how data is transported and stored in the cloud, and why major global providers such as AWS are the only way to go.

Wildix

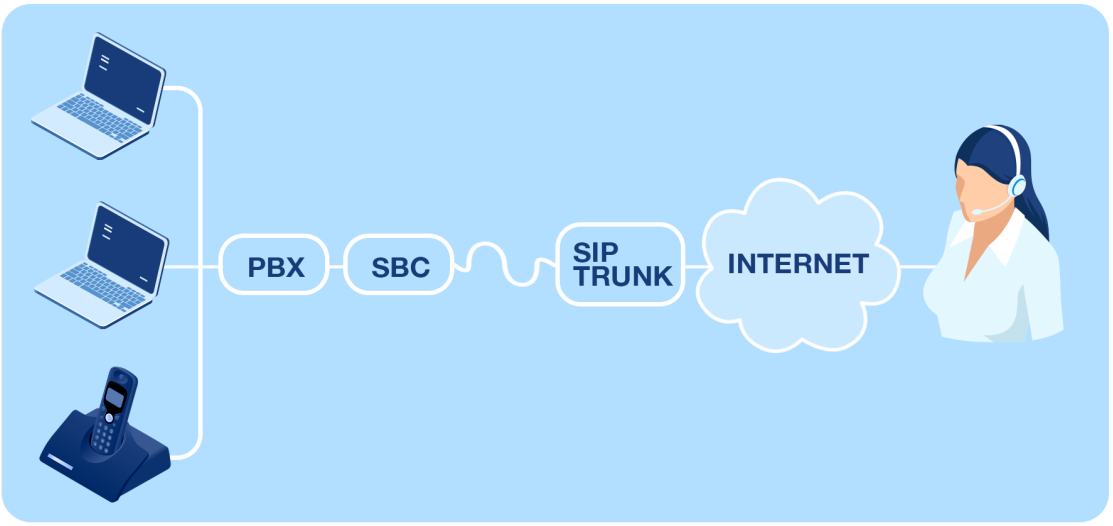
Hardware Solutions

63% of respondents to a 2019 Dell survey revealed they'd suffered at least one potential breach due to issues in hardware or silicon-level security in the past 12 months. 10% had six or more incidents.

Every solution requires hardware of some description, whether it's a simple laptop or phone or a full PBX with deskphones, conferencing hardware and gateways. One of the biggest issues with hardware, however, is that many solutions use multiple third-party devices that need to be kept updated while remaining compatible with the overall system.

Each third-party device again results in a potential point of failure as a result of these multiple chances for system vulnerabilities or incompatibilities.

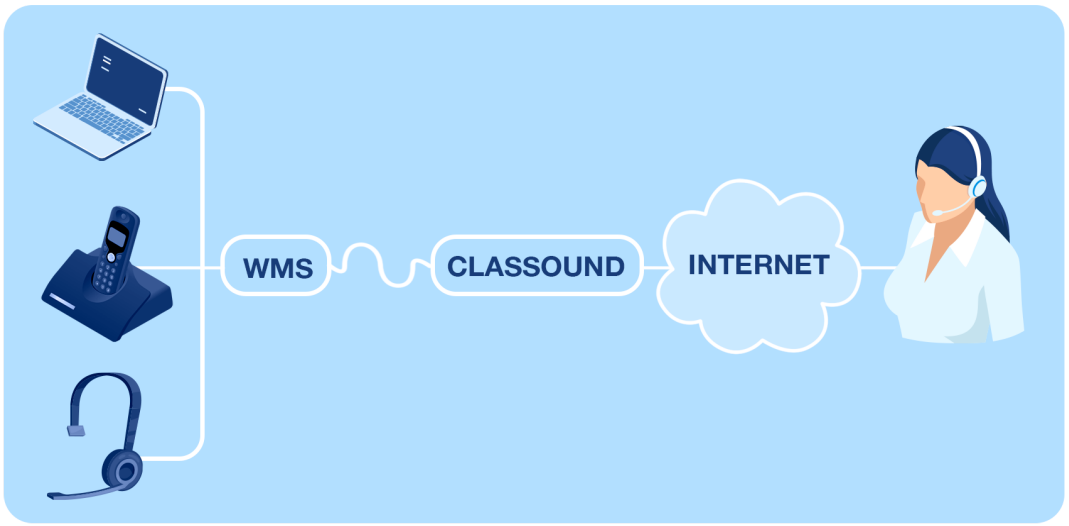
A typical system using a traditional IP PBX might look like this:



Each of these could easily be provided by a different vendor, which increases the risk of failure each time. Most solutions get around this by offering some sort of certification process, but many still are at the whims of their third-party providers. In some cases, third-party hardware, such as that from Yealink, has been shown to send data back to fourth parties.

A good telephony solution should eliminate as much hardware as possible, preferably not relying on SBCs, and using their own certified devices. If everything is compatible within a single solution, it resolves a lot of potential issues at once.

A Wildix solution could easily look like this:



Everything is designed to work in harmony with each other, reducing the risk of incompatibilities and overall issues. In addition, this means a much lower chance of unauthorized access.

The question is this: Does your comms system require numerous separate parts from different vendors to even talk to other people? Why does it need that level of complexity?

A good secure-by-design solution simplifies this complexity.

Base Technologies

There's a dizzying array of technologies behind each system. We've touched on a few, but most are a result of a mix of proprietary technologies and open-source solutions.

It's important to note that open-source solutions are not insecure; anyone can examine the source code and check it for vulnerabilities. These vulnerabilities are usually rapidly patched and repaired.

Proprietary systems may be secure, but they're not as open to scrutiny. That can be good, but it can also be bad. It depends on the design principles behind each one.

Secure by design systems, however, must abide by sound design principles. The use of WebRTC in Wildix systems, for example, means no downloads are required, resulting in a much cleaner, easier-to-handle setup process.

Wildix

System Monitoring

Even the most secure system requires some form of monitoring, and good secure-by-design principles accept there's always a risk of intrusion. This means things like:

- Automatic alerts across all devices managed by the PBX
- Alerts for attacks originating from within the system
- Integrations with common monitoring software, such as Zabbix
- Behavioral-based alerts where possible

When you're a local MSP, you must ensure your data is protected and that the systems you install are appropriately monitored. Secure by design systems either integrate or make it simple to add monitoring tools without fuss.

In this particular instance, secure by design systems don't have to be that different from secured systems, although many secured systems do not automatically include monitoring capabilities or automations.

User Design

82% of breaches involved a human element, such as social attacks, errors and misuse, according to the 2022 Verizon Data Breach Report. Many of these could be prevented by better design.

One oft-missed point of security is that it should be simple for the user to stay compliant automatically.

In 2018, there was a missile drill for state workers in Hawaii. Unfortunately, this drill resulted in an alert being triggered by a single state worker who misunderstood, and it took a relatively long time for the alert to be canceled.

One key problem was that there were far too many points at which the system could fail. Any person within the operations center could send the alert, and there was no need for a second person to check and be involved. Procedures to identify an attack were vague, and there were no preparations of what to do in the event of a false alarm.

All of this led to Hawaiians believing they were under nuclear threat for over 40 minutes.

This shows how poor procedures and personal judgment should be removed from important processes as much as possible, especially when it comes to security. From a security point of view, there should be a good process:

- Ensure the threat is genuine through clearly established procedures (including validation of data)
- Require two people to confirm (essentially 2FA)
- Send the alert through established channels
- Ensure clear procedures are in place to cancel the alert through an easy-to-use system (revocation)

The security of the original system required users to be perfect across each stage, and that simply doesn't happen.

The same applies to any hardware or software system. Unintuitive user interfaces make it harder for users to remain compliant, especially when those systems are hard to install. Shortcuts get taken for logistical and practical reasons, such as using default passwords or making systems less secure so they can talk to each other.

And when those shortcuts can be taken by everyday personnel, that's when problems really start to mount up.

Even simple things like access control lists to mitigate harm are often missing from many "secured" solutions.

A communications system that relies on users to be perfect across each step is likely to fail. The human element cannot be ignored, and that's the reason why phishing and other hacking attempts regularly succeed.

Ultimately, secure by design solutions are much more effective than secured systems as they come with much of the security you need already baked in. And if you choose the complete Wildix ecosystem, you get all that security baked in.