concise



6 Ways to Improve Your IT Security Architecture

www.concise.com

6 Ways to Improve Your IT Security Architecture

Every business needs to be concerned about cybersecurity. Your data is a target for cybercriminals, and the reality is, cyber-attackers are becoming more sophisticated every day. This is an even bigger concern for U.S. businesses, as new research from Juniper Research estimates that over 33 billion records in the U.S. will be stolen in 2023. One of the most important aspects of your cybersecurity strategy is a strong IT security architecture.

“... new research from Juniper Research estimates over 33 billion records in the U.S. will be stolen in 2023.”

Why Do You Need a Strong Security Architecture?

Modern businesses must have a reliable security framework in order to thrive. It's the foundation of any strategy to protect your most valuable information assets. You'll realize many benefits from a strong security architecture, including:

- Fewer breaches of your network
- Ensured compliance with key data security standards
- Enhanced trust and credibility with your clients and partners
- Preventing the loss of business

As a leader in corporate IT solutions, our team is focused on delivering managed IT services that improve your cybersecurity and reduce IT costs. To build a more robust IT security architecture, here are the six things we recommend.

Bypass Switches

Bypass switches are a good start for your cybersecurity efforts. By installing bypass switches between network and security tools, you can improve your network's availability and reliability. Direct deployment of security tools can deliver an improved line of defense; however, they can also result in a single point of failure should they falter. With an internal bypass within the security tool, you'll be able to minimize this risk.

An external bypass will also provide you with risk mitigation. It will remove the pain of direct deployments of inline tools as it offers both on-demand and automatic fail-over abilities with little impact on the network. The switch is always in the network and can be placed in bypass mode, enabling monitoring and security devices to be upgraded, added, or removed without any interruption to your business.

Threat Intelligence Gateways Threat intelligence gateways are a smart technology that creates new opportunities, as noted by Gartner. They can be deployed at the entrance or exit of your network as a means to decrease false-positive security alerts. They also help exclude traffic to and from bad IP addresses.

“With a threat intelligence gateway, you can filter the traffic and can see dramatic reductions on false positives.”

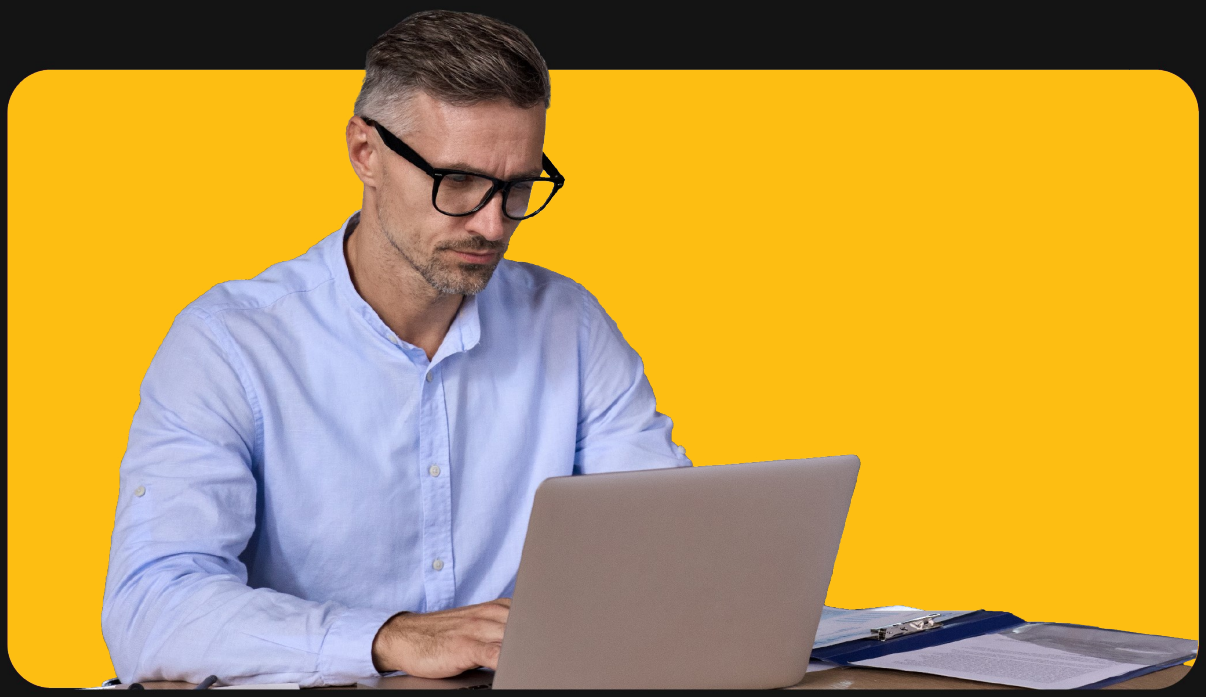
Even with firewalls and security tools in place, businesses still suffer breaches or miss important clues to potential threats. Typically, these missed moments are due to the heavy influx of alerts, putting a drain on your infrastructure and security experts.

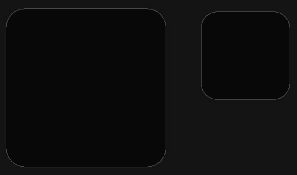
With a threat intelligence gateway, you can filter the traffic and can see dramatic reductions on false positives.

Network Packet Brokers

You can also strengthen your network architecture by offloading S SL decryption from existing security components, such as firewalls and WAFs, to network packet brokers or other devices. This reduces latency and enhances the efficiency of your security tools.

Your firewall or security tool has the ability to decrypt traffic, but it also impacts CPU performance, slowing a security tool's processing capabilities dramatically. Why? Because those devices are performing additional tasks like analyzing data for security threats.





This can make SSL decryption a burden for your operations and may increase costs. To avoid this, many will just turn off data decryption features on security tools, leaving you open to risk.

A better solution is the network packet broker (NPB), which can perform data encryption or offload the function to a separate decrypting device. Once decrypted, the NPB forwards it to a security tool for further analysis.

Serial Tool Chaining

Serial tool chaining uses pre-set sequences for data analysis and will route suspect data serially to various security tools for additional inspection and resolution. You can use it to investigate suspect data, improving the data inspection process. You can effectively automate the inspection process to save time and resources while enhancing the quality of your network.

With serial tool chaining, actions occur in the proper order ensuring nothing is overlooked.

Superior Network Testing and Simulation

Network assessments and continued testing and simulation are vital to improving your network architecture. You should test all your security tools in a lab prior to official deployment. That way you'll be able to understand exactly how they will perform.

With malware and DDoS simulations, you can create realistic traffic to put your tools to the test and identify any issues. You can also take it a step further by customizing traffic mixes and parameters that are most likely to occur in your environment.

Since the cyberthreat landscape is constantly evolving, make sure to run regular tests on your security infrastructure. Keep testing in your lab with new and emerging “what if” scenarios. You can also test to validate software updates to your security tools.

You may even want to engage in simulating specific attacks to determine an attack pattern and how that type of attack will behave in your network.

Plan for Mobile Devices

There are a tremendous amount of security concerns when it comes to mobile devices in the workplace, as noted by the experts at Deloitte. Bring your own device, or BYOD, continues to be a growing trend with 59% of businesses favoring that strategy.

So, if you allow BYOD and actually depend on employees to use their mobile devices, you must have a documented policy in place that focuses on the unique security risks of mobile devices, which may include things like requiring employees to enable automatic security updates and using company password policies.



The reality is that mobile devices are part of your network, and to leave them out of the story is to expose yourself to risk. It's better to be prepared for the worst-case scenario.

Threats to your network aren't going to wane any time soon, so the best approach is to be ready and utilize as many tools and strategies as possible to keep your network secure.

You may not have the internal resources necessary to manage and maintain your security, so find a trusted partner like our company. We've been helping SMBs with IT solutions for years and take your data security seriously.

Contact us today to learn more about how we provide cybersecurity.

Contact Us

www.concise.com | 248-745-8255

2350 Franklin Rd, Ste 200
Bloomfield Hills, MI 48302