WHITE PAPER

Plixer vs Cisco Stealthwatch: A Technical Comparison

Plixer

With limited resources and the ever-looming threat of a data breach, IT teams are struggling to stay ahead of the next threat. Solutions like Plixer Security Intelligence and Cisco's Stealthwatch offer teams an advantage in the fight against cybercrime. But there are distinct differences between Cisco's and Plixer's solutions.

Additionally, in June 2021, Cisco announced an end-of-life notice for the core Stealthwatch technologies and continued their effort to move customers to their two separate security products: Cisco Secure Network Analytics (SNA) and Cisco Secure Cloud Analytics (SCA). But both SNA and SCA operate in a similar way to Stealthwatch and share the same shortcomings.

Whether you're looking to replace Stealthwatch or add a network security solution to your tech stack, the following will help you understand the advantages of Plixer's offering.

Intelligent threat detection

A data breach can greatly damage your business. According to the latest IBM & Ponemon report on the cost of a breach, most businesses saw a 38% loss of their overall value. Unfortunately, a threat may be present for months before anyone notices and often only after an incident has occurred—that same report found on average it takes 287 days to detect a breach.

Threats may be difficult for other security systems to detect because cybercriminals often gain a foothold on the network through legitimate credentials and approved services. As an example, you can look to the recent announcement by Palo Alto Networks that indicates that attackers can use the BRc4 tool to evade endpoint detection and response (EDR) solutions and anti-virus products. For that reason, it's critical that businesses can detect unusual behavior on the network, as this is often the first clue that the network has been compromised.

When comparing the threat detection capabilities, Plixer and Cisco take a similar approach. In part, because we share the same data ingestion source, and our detection algorithms share similar features. Both Plixer and Cisco provide intelligent threat detection by ingesting network flow data sources—i.e., NetFlow, IPFIX, sFlow, jFlow, Flow Logs, etc.—to monitor and analyze all the devices interacting on the network. When the behavior of any type of device starts to look odd, it triggers an alert—and in certain cases, a response—to provide real-time threat detection for investigation and response.

If you're currently using Cisco Stealthwatch and are concerned about switching to another product, you can rest assured that threat detection capabilities, data sets, and training will not be distinctly different from the process you currently have in place.

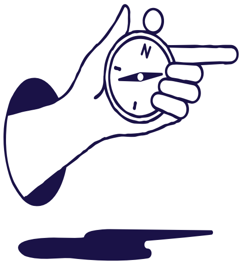
Unlike Cisco, however, Plixer provides an extra layer of threat intelligence. Plixer Security Intelligence platform gives you sophisticated threat analysis, prioritized alerts, and custom sensitivities. Only Plixer allows you to easily customize the detection sensitivity for specific assets, ports, or protocols and refine those thresholds to align with the normal ebb and flow of your traffic. Generating flexible, daily models of network traffic means you are always keeping pace with your evolving traffic patterns.

Additionally, Plixer's sophisticated ML capabilities tap into tens of thousands of traffic behavioral models to augment our ability to detect unusual behavior. This works in tandem with our ability to detect the latest Indicators of Compromise (IoCs) via a STIX/TAXII feed. And finally, only Plixer gives you the ability to create custom ML definitions through an easy-to-use UI.

This means that Plixer's threat detection customizations allow you to eliminate false positives and spend more time investigating and responding to real threats.

Flexible deployment and easy management

IT teams across the globe are struggling to find and maintain talent. A recent survey of security operations teams found that 20% are ready to leave the field. A talent shortage coupled with historically constrained budgets is a perfect storm for security teams of any size. For that reason, it's important that a new technology needs to provide immediate and continual value.



Most NDR solutions, however, have large upfront investments, recurring hardware updates, and lengthy deployments. This is not true of Plixer. Plixer Security Intelligence platform is easy to deploy because Plixer taps into your existing network infrastructure. That means there's no upfront investment or recurring hardware to replace, no lengthy deployment or upgrade project to manage, and no need to prioritize portions of your network over others. Instead, you get near-instant visibility across your entire network.

Additionally, Plixer offers you flexible deployment options so you can work within an on-prem environment, from a public or private cloud, or in a hybrid environment. This allows Plixer to easily adapt and scale to your network needs and comfortability.

A common criticism we hear from current and former Cisco Stealthwatch customers is that the upgrades were arduous, expensive, and time-consuming. The switch from Stealthwatch to SNA or SCA is even more intensive if you're currently on Stealthwatch, as it requires an overhaul of your existing system and is more expensive. This is especially true if you are in a hybrid environment or are currently in an on-prem environment but have plans to move to a cloud-based solution in the future.

Because Cisco only offers you an on-prem or a cloud-based monitoring service, you would need to run both platforms to gain visibility across your network environment. Additionally, both products are SaaS-based, which means that you must commit to a cloud provider for network security. While this is likely the way of the future, it ignores the organizations that are not ready for the cloud or have reason to be wary of deploying these kinds of services via the cloud.

Plixer cuts the complexity of arduous deployments and upgrades, so you can spend your time focused on keeping your business secure from a breach.

Extended network intelligence

No one security tool is going to be a silver bullet to cyberattacks. For decades, the industry has been reacting to new challenges rather than advancing for the threats of tomorrow. The big vendors, like Cisco, promise an out-of-the-box solution that can provide a single ecosystem to curtail, detect, investigate, and respond to threats. The idea is great, in theory. But single platform vendors continue to fall short of their promise.

Time and again, security teams prefer a best-of-breed approach over a single vendor. A report from ESG found that over half prefer best-of-breed cybersecurity tech stack. The qualifier to that answer though was the ability to integrate well with other products.

Many vendors like Cisco, though, tailor their solutions to work best with their own products. This is what's known as vendor lock-in. A company like Cisco would rather you buy from their suite of products to keep expanding your investment with their solutions. Being locked into one vendor, though, makes it more difficult to rip out any one technology—even if that technology is not serving you.

That's a problem.

Your security stack needs to be effective and easy to use. But it also needs to provide value beyond its intended use.

Plixer has dozens of integration partners. We understand that network security intelligence is one layer in your overall security posture, so feeding the analysis and detections found in Plixer Security Intelligence to other solutions, is vital to protecting an organization. We integrate with the most common SIEM/SOAR products, ticketing systems, and dozens of technology partners that help you detect, investigate, and respond to threats. Our dedication to building an integrated solution allows you to build a best-of-breed technology stack to stay innovative and scalable.

With a growing number of devices present on the network, it's important to understand the riskiness or vulnerabilities of managed and unmanaged devices. Plixer utilizes the data on the network to provide agentless device discovery, profiling, and risk scoring to help organizations identify and be alerted of all devices on the network. This gives you a very resource-light way to see all the devices on your network and determine their vulnerabilities at a glance. Cisco, on the other hand, has only limited device information.

Additionally, unlike Cisco, Plixer's platform can be used for both security and performance intelligence. Cisco's SNA and SCA are purely focused on threat detection, which makes it necessary for NetOps and SecOps to purchase different solutions to analyze network flow data. Plixer eliminates this need by providing a platform that any IT team can harness for network intelligence. With Plixer, you can maximize your investment by investing in a single solution for both network security and performance analysis.

Conclusion

Your network is your business. Not only is it the operational foundation on which nearly all other work happens, but it also provides your business the ability to scale and gain a competitive edge. Within the network is a storehouse of data that can help optimize your business performance and security. When properly harnessed, intelligence extracted from the network can provide tremendous value.

Plixer gives you the pervasive network visibility necessary to detect threats that have bypassed other security tools. By analyzing flow data from existing network infrastructure, you don’t need to invest time or resources to add sensors or agents to monitor network behavior. Our easy-to-deploy platform provides fast value to the security and network team and integrates with the tools you already rely on for security and performance.

Get started with Plixer today.

About Plixer

Plixer provides a single platform for Deep Network Observability, delivering the visibility and context needed to manage the immense opportunities and risks of a digital business. As a leader in the Network Detection and Response & the Network Performance Monitoring and Diagnostics markets, Plixer provides the comprehensive intelligence needed to analyze, evaluate, and visualize the millions of conversations that cross networks every second.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.