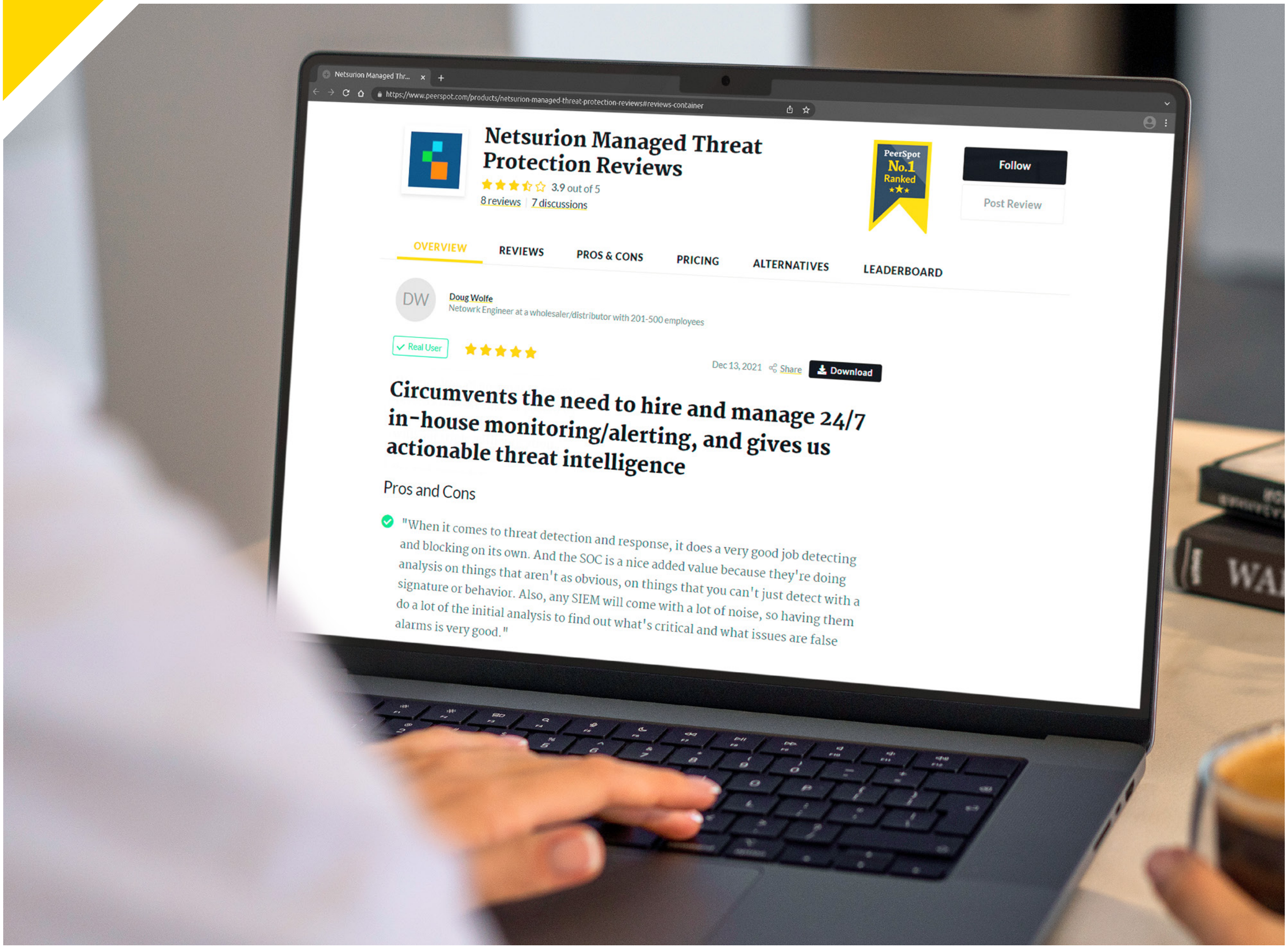
PeerPaper™ Report 2022

Based on real user reviews of Netsurion on PeerSpot

Understanding the Advantages of Managed Threat Protection vs. DIY SIEM



Netsurion Managed Threat Protection Reviews

★★★☆☆ 3.9 out of 5

8 reviews | 7 discussions

Doug Wolfe
Netowrk Engineer at a wholesaler/distributor with 201-500 employees

★★★★★

Dec 13, 2021

Circumvents the need to hire and manage 24/7 in-house monitoring/alerting, and gives us actionable threat intelligence

Pros and Cons

✓ "When it comes to threat detection and response, it does a very good job detecting and blocking on its own. And the SOC is a nice added value because they're doing analysis on things that aren't as obvious, on things that you can't just detect with a signature or behavior. Also, any SIEM will come with a lot of noise, so having them do a lot of the initial analysis to find out what's critical and what issues are false alarms is very good."

PeerSpot

CSO

Contents

Introduction

Effective cyber defense relies on a careful choreography between people and technology. This sounds great, but there are two profound problems that surface in most IT and security departments: The people are hard to find, and the technology is challenging to use. Recruiting staff who know how to effectively operate SIEM technology can be a major challenge. What's more, SIEM platforms themselves are not easy to set up and maintain.

The combination of people, process, and technology through managed security services and SIEM platforms is emerging as an increasingly popular alternative, as exemplified by Netsurion's Managed Threat Protection. This solution embodies comprehensive SIEM functions that provide the same, or in some cases, better analytics, and threat intel, while providing the Security Operations Center (SOC) expertise to ensure success. Operational outcomes improve along the way. In this paper, PeerSpot users of the Netsurion Managed Threat Protection solution discuss how it helps them run successful security operations that prevent, detect, and respond, which was not possible with SIEM only.

Netsurion Managed Threat Protection Use Cases

PeerSpot members are using Netsurion Managed Threat Protection in a variety of use cases. For example, a VP of IT Systems at Carteret-Craven Electric Cooperative, a manufacturing company with over 50 employees, described using Netsurion to ensure that they are fully compliant with PCI DSS, the payment card industry security standard. He said, "We needed someone with that expertise because we don't have a dedicated, trained security professional." The company turned to Netsurion for that service and has been pleased with the results.

A leisure and travel company with over 1,000 employees uses Netsurion Managed Threat Protection on-premises. According to a Lead Security Analyst at the company, "We have the agent running on our Windows systems and we have the Linux systems pumping the syslog data to the Netsurion server."

"We're using it as a decentralized SIEM product and it's one of the only ones out there," said a Cyber Security Specialist at a small financial services/private equity firm. They use Netsurion to manage workstations and servers at 13 portfolio companies, with each company managing 10 to 20 companies—approximately 300 - 400 companies altogether.

"It was effortless to tune it for our software"

Read review »

“super easy to get up and running compared to some of the other solutions I’ve seen”

Read review »

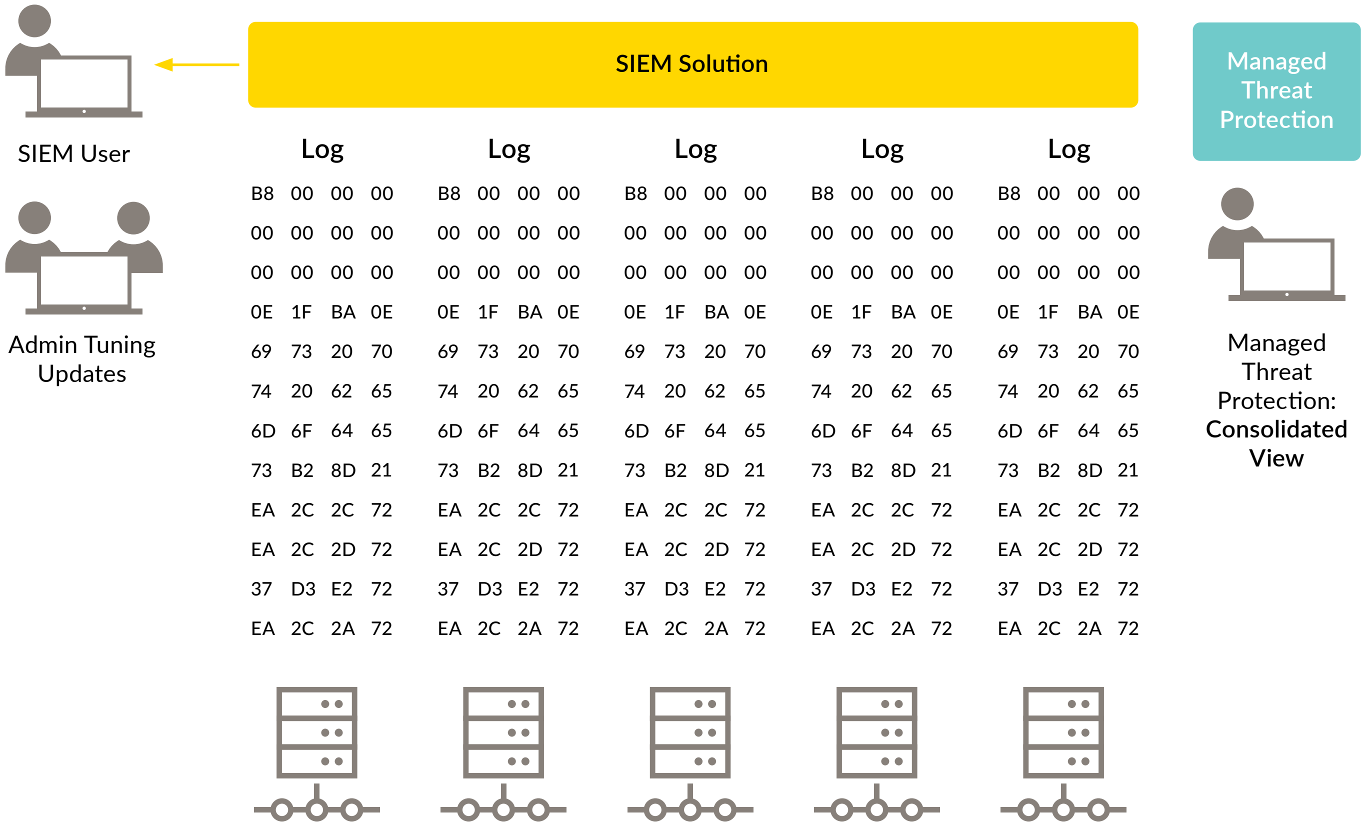
He added, “We use Netsurion for things like log forwarding and we deploy it on every workstation. It’s a manual process. There is an installed agent, and as long as it has internet connectivity, it goes and talks to the centralized server. Netsurion’s SOC monitors the logs for all those devices. This approach is beneficial because the firm does not have a centralized enterprise network. There are a lot of different companies involved.” He then said, “The Netsurion agent has to be installed on every endpoint and allowed to communicate directly with the internet.”

A healthcare company with more than 5,000 employees uses Netsurion for both PCI DSS and HIPAA compliance, as well as to implement best security practices. According to their Senior Director of Information Security, the company had no visibility into the environment before implementing Netsurion. Further to this point, the wholesaler/distributor Network Engineer noted that, as a managed SIEM, Netsurion collects log information/events from different systems. “We use that database to do our own infrastructure investigation and threat research.”

An IT Director at Global Connections described how easily Netsurion’s Managed Threat Protection handled a similar risk management concern. “It’s a deny-all policy, so there’s an access list on each machine. It was effortless to tune it for our software...and was super easy to get up and running compared to some of the other solutions I’ve seen.”

Comparison: Netsurion Managed Threat Protection VS SIEM Only

Benefits of Netsurion Managed Threat Protection over SIEM include saving money from not having to add full-time employees (FTEs) to administer and tune the SIEM over time. Key personnel become free to perform other duties. This is particularly useful for smaller security organizations. Figure 1 compares the work required to manage a SIEM versus taking advantage of the full scope of Managed Threat Protection.


SIEM Solution
SIEM User
Admin Tuning Updates
Managed Threat Protection
Managed Threat Protection: **Consolidated View**
Log
Log
Log
Log
Log

```
B8  00  00  00    B8  00  00  00    B8  00  00  00    B8  00  00  00    B8  00  00  00
00  00  00  00    00  00  00  00    00  00  00  00    00  00  00  00    00  00  00  00
00  00  00  00    00  00  00  00    00  00  00  00    00  00  00  00    00  00  00  00
0E  1F  BA  0E    0E  1F  BA  0E    0E  1F  BA  0E    0E  1F  BA  0E    0E  1F  BA  0E
69  73  20  70    69  73  20  70    69  73  20  70    69  73  20  70    69  73  20  70
74  20  62  65    74  20  62  65    74  20  62  65    74  20  62  65    74  20  62  65
6D  6F  64  65    6D  6F  64  65    6D  6F  64  65    6D  6F  64  65    6D  6F  64  65
73  B2  8D  21    73  B2  8D  21    73  B2  8D  21    73  B2  8D  21    73  B2  8D  21
EA  2C  2C  72    EA  2C  2C  72    EA  2C  2C  72    EA  2C  2C  72    EA  2C  2C  72
EA  2C  2D  72    EA  2C  2D  72    EA  2C  2D  72    EA  2C  2D  72    EA  2C  2D  72
37  D3  E2  72    37  D3  E2  72    37  D3  E2  72    37  D3  E2  72    37  D3  E2  72
EA  2C  2A  72    EA  2C  2A  72    EA  2C  2A  72    EA  2C  2A  72    EA  2C  2A  72
```

Figure 1 – SIEM solutions are generally more labor-intensive and time-consuming to manage in comparison to a comprehensive solution like Netsurion Managed Threat Protection.

"does a very good job of detecting and blocking on its own"

Read review »

As the wholesaler/distributor Network Engineer put it, Netsurion provides employee time-saving benefits. He said, "If we didn't have the managed component, I would probably have to spend most of my day in the SIEM, personally." He also pointed to the value-add of the extra oversight and expertise. "The Netsurion EventTracker SOC does a very good job of detecting and blocking on its own," he said of Netsurion's detection and response capabilities.

He then added that Netsurion's SOC is "a nice added value" because the team consists of cybersecurity experts who conduct "analysis on things that aren't as obvious." Because many SIEMs "come with a lot of noise," as he put it, relying on the SOC team to conduct "a lot of the initial analysis to find out what's critical and what issues are false alarms is very good."

"If we didn't have the managed component, I would probably have to spend most of my day in the SIEM, personally"

Read review »

The VP of IT Systems at Carteret-Craven pointed to the ease-of-use, explaining that his team found Netsurion's Managed Threat Protection to be much easier than the company's previous solution. Netsurion has enabled them to consolidate cybersecurity technology, including SIEM and network traffic analysis.

Improved Log Handling and Analysis VS SIEM

Netsurion Managed Threat Protection enables improved log handling and analysis when compared to DIY SIEM. For Carteret-Craven's VP of IT Systems, this meant having a resource advantage. He said, "It takes the load off of our systems administrator from having to manage, vet, and analyze logs. Netsurion's Managed Threat Protection service has been invaluable to us in terms of being able to narrow the scope of what really needs to be looked at and prioritizing things that deserve our attention."

He then shared how applying that time-saving expert filter paid off in terms of high security rankings. Third-party security assessors have ranked Carteret-Craven high in terms of cybersecurity maturity when compared to other small businesses. Their Security Specialist likewise found that working with Netsurion and their 24/7 SOC allows them to benefit from large quantities of data despite the size of the organization. "We don't have the in-house expertise or the time," explained the Security Specialist.

"has been invaluable to us"

Read review »

Further Operational Advantages of Managed Threat Protection

Other operational advantages of using Netsurion Managed Threat Protection include better threat intelligence and improved detection and response. Monitoring is available 24/7/365 and is valuable for companies that want the coverage, but don’t want the staffing headaches and expense that come with it. Netsurion Managed Threat Protection frees staff for other duties as well. Users get visibility and insights into security events with a consolidated single view.

Better Threat Intelligence

A benefit of Netsurion Managed Threat Protection was better threat intelligence for the wholesaler/distributor Network Engineer. He described his scenario, saying, “If an endpoint user visits a site that attempts a download, a ‘drive-by’ type of situation where it tries to run an obfuscated URL through a PowerShell or the like, we’ll get an alert from the Netsurion SOC so we can take remediation actions for that particular endpoint.”

Time-saving

A Senior Director of IT at a healthcare company with over 5,000 employees observed that integrating Netsurion with the MITRE ATT&CK threat intelligence resource offers improved threat protection for his organization. Every alert includes a reference to a MITRE ATT&CK technique, enabling the client to identify threats that might have otherwise been missed.

The IT Director at Global Connections similarly noted the importance of Netsurion as a source of directional insight because Netsurion helps with the MITRE ATT&CK framework. It is a resource that provides a base idea of what is happening in their infrastructure and where a surface attack vector could be. As he shared, "The embedded MITRE ATT&CK framework helps us pinpoint exactly what we should be looking at."

> "helps us pinpoint exactly what we should be looking at"
>
> **Read review »**

The leisure/travel company Lead Security Analyst described a moment when Netsurion Managed Threat Protection played a critical role in the company's security: "When there was a vulnerability in our Microsoft Exchange platform, Netsurion alerted us to eliminate security gaps that cyber criminals could exploit." He then added, "The embedded MITRE ATT&CK Framework was paramount in our decision to choose Netsurion because the MITRE Framework is the industry standard for threats. I believe it has helped with the time it takes to identify and understand sophisticated threats."

Threat Prevention

Netsurion Managed Threat Protection enables threat prevention, as the Senior Director of Information Security at the healthcare company found. He said, “If a user starts an unusual process that isn’t on the whitelist, Netsurion’s team can detect it and prevent it from executing. Afterward, they’ll notify us by telephone, so we can respond and clean up whatever damage has occurred.”

> “The threat detection and response are excellent”
>
> Read review »

Improved Detection and Response

The wholesaler/distributor Network Engineer gave statistical evidence of Netsurion’s positive impact on security, saying, “Our detection time is shorter than it was and they’re well within the SLA for both detection time and remediation. Since MITRE ATT&CK was added in, we haven’t seen anything take longer than it’s supposed to. The alerting times are also very short.”

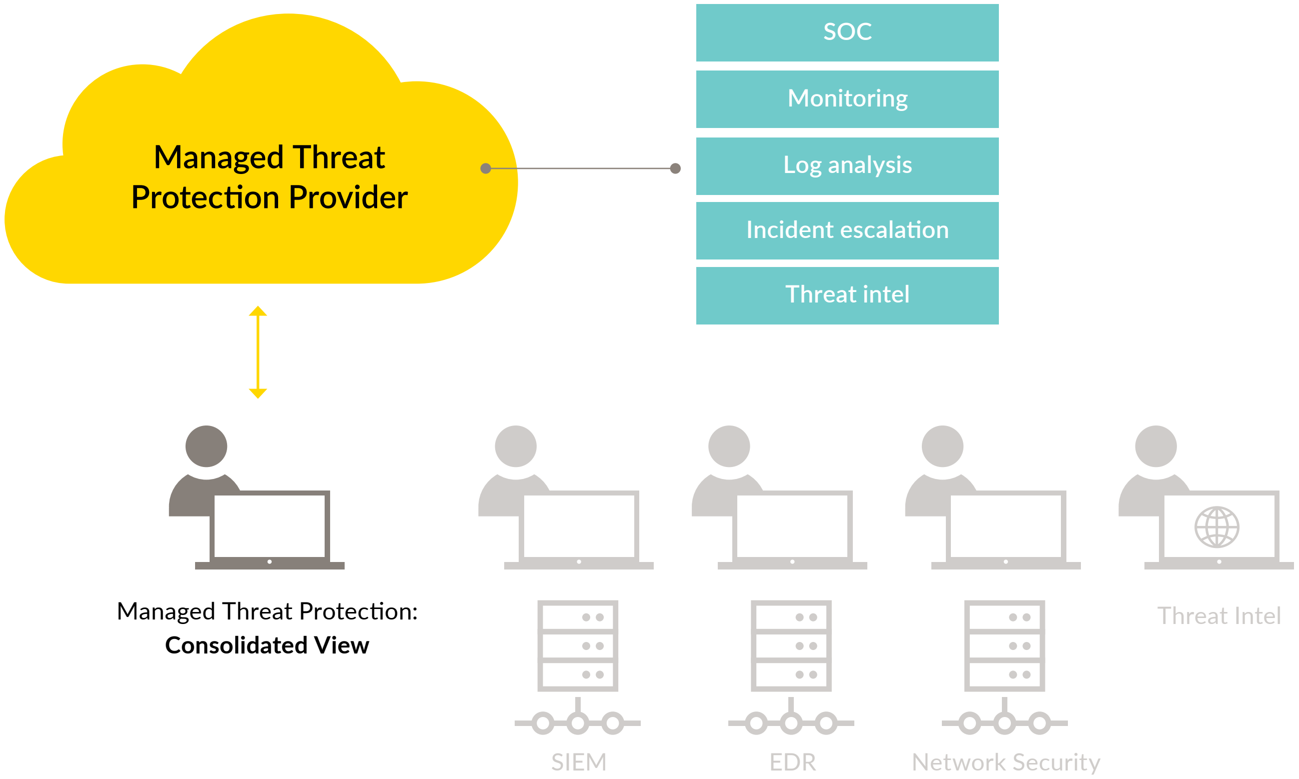
The IT Director at Global Connections offered a similar assessment, sharing, “The threat detection and response are excellent. We’re doing internal PCI scans now based on what we originally discovered with this product, and it’s a necessary piece of our overall threat protection landscape.” He had considered limiting or getting rid of certain servers, perceiving them to be liabilities. Netsurion’s threat detection provided directional insight that validated his concerns, giving him vital information to take back to his CFO. The healthcare company’s Senior Director of Information Security also saw signs of improved detection and response. In his case, Netsurion has reduced the amount of time it takes to identify and respond to constantly evolving threats.

24/7 Monitoring

"The 24/7 monitoring and alerting have positively affected our security maturity rankings," said the travel/leisure company Lead Security Analyst, adding, "because now we have people with eyes on our security events 24/7. With the hosted SOC, we don't need to have a large team on our side."

On a related note, the IT Director at Global Connections explained that he sees Netsurion as an extension of his own team. In addition to freeing up his own time as described above, he estimates, "It saves close to 75 percent of a one FTE in our existing staff. To get 24/7 monitoring, we'd have to have at least three people with no vacations for those people. That would add up to a whole bunch of FTEs."

Figure 2 - Netsurion Managed Threat Protection frees resources from having to fully manage SIEM, Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), Network Traffic Analysis, Vulnerability Management, Threat Hunting, more.



Freeing Staff for Other Duties

Speaking as the only security person in a company with more than 5,000 employees, the Senior Director of Information Security at the healthcare company found that Netsurion freed time for his employees which positively affects work-life balance. He estimates that Netsurion has saved the equivalent cost of three full-time employees at 40 hours a week.

The COVID-19 pandemic put a spotlight on the issue of employee time. According to the IT Director at Global Connections, the Netsurion SOC solves small-business problems exacerbated by the pandemic. He revealed, “We were a small shop to begin with, and when the pandemic hit, we lost 60 percent of our workforce, including my department and the other technology services departments here. We needed something actionable.”

Saving money

Visibility and Insights

The visibility and insights offered by Netsurion can serve both to provide new information and to confirm perceptions of what might be happening in an environment, while offering a roadmap to resolution. “We’ve been under attack since the day we opened,” recounted the IT Director at Global Connections. He added, “Netsurion provides excellent visibility into how often it’s happening and what techniques cyber criminals are using.” In his view, Netsurion “solidified” a lot of suspected issues and made it a little easier to tailor solutions than it would have been without the actionable intelligence.

He went on to describe the impact on resource allocation, saying, “Netsurion’s Managed Threat Protection didn’t reduce the amount of time we had to devote to everything else, but it supplemented our visibility. They also got us up and running in a week. So, while I won’t say that it freed up my staff to do other tasks, it saved me from having to assign staff or take staff away from current projects.”

At the healthcare company, the Senior Director of IT described Netsurion’s Managed Threat Protection as a vital tool for someone like him, who was new to the company and the environment. He pointed out, “Netsurion’s Managed Threat Protection is valuable for me to see what processes are being executed in the environment to ensure that nobody is running something that may have malware or infections. Netsurion’s log aggregation feature is something I use heavily.”

24/7
monitoring

A Consolidated Single View

The IT Director at Global Connections spoke about a consolidated view as not just a practical feature of functionality, but also as a strategic advantage when seeking executive sponsorship for change. He said, “Consolidating services really helped us gain C-level buy-in. This wasn’t just to monitor logs and check for some malicious entries; Netsurion provides a complete cybersecurity solution that allowed us to recoup money in other areas because we could consolidate everything in one cyber solution.”

Consolidation was also considered a material advantage at the healthcare company with over 5,000 employees. According to their Senior Director of IT, with Netsurion, the company has consolidated a lot of its cybersecurity technology. He offered this case in point: “Netsurion can aggregate the log files from a Cisco Meraki wireless access point,” he noted. “That minimizes the time necessary to investigate. I take their data, and I know where to start.”

Understanding of Assets

The Senior Director of Information Security at the healthcare company wrote in his PeerSpot review that if one does not have a solid understanding of your inventory of assets, it’s going to cause problems in the future. He alluded to the advantage of Netsurion’s EventTracker SIEM as a tool which provides him the opportunity to “see what’s out there.” “This is especially crucial,” he explained, “given that we have some BYOD devices that are not allowed on the network. I was able to spot those devices and enable conditional access through our Azure Active Directory.”

The alerting times are also very short

Summary

Security operations requires people, process, and technology resources that are out of reach for many companies. SIEM alone is challenging, but Netsurion's Managed Threat Protection enables the same or better operational outcomes with a proprietary SIEM platform and the SOC expertise to properly manage it 24/7. Better outcomes include improved log handling and analysis, along with better threat intelligence. Prevention, detection and response get better, too, according to Netsurion users on PeerSpot. The 24/7 monitoring available with Netsurion Managed Threat Protection saves security teams from the stress and expense of staffing such extensive coverage.

It also frees security team members for other duties. With Netsurion, all stakeholders get visibility and insights into threats and security events through a single, consolidated view. The pressures facing security organizations are unlikely to get less intense as time goes on. With Netsurion Managed Threat Protection, it is possible to build a strong cyber defense capability even as the threat environment and staffing constraints become more severe.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.