Amazon Web Services (AWS)/Cloud Security - CounterSnipe IDS/IPS Case Study

The following case study has been written in partnership with Christopher Hawkins, Wepa Server Team Manager, and Izz Noland, Wepa Senior System Administrator. The goal of the case study is to illustrate the need for cloud-based security, the options and alternatives to address that need, and the capabilities and advantages of a CounterSnipe – Suricata network-based Intrusion Detection System.

Wepa Background:

Wepa has been providing kiosk-based printing services to schools and universities for over 6 years. Wepa's printing service revolves around distributed print stations supported by a back-end cloud and physical infrastructure. Because student printing can be charged to a student's university account or a student's credit card, having a secure Payment Card Industry (PCI) Compliant IT infrastructure is critical to Wepa's success.

The Problem:

"As we have grown from a startup to a mature company, the PCI issue was one of the challenges that led us to look for an intrusion detection and prevention system (IDS/IPS)," said Mr. Hawkins. WEPA doesn't store any cardholder data, but in order to be PCI compliant (Section 11.4 of PCI 301), integrating a robust IDS/IPS solution was required.

Defining Requirements and Evaluating Alternatives:

After investigating many options, Wepa decided that the first stage of their cloud migration would utilize Amazon Web Services (AWS). AWS was the clear market leader in terms of a comprehensive platform of integrated tools, including Identity and Access Management, Inventory & Configuration, Monitoring, built-in firewalls, and encrypted data storage. AWS would secure the underlying infrastructure that Wepa's virtual machines would sit on (ZenHost, routers, and switches). However, the AWS network layer security was fairly basic and Wepa would be responsible for securing their own applications and data. What Wepa lacked at AWS was the ability to detect intrusions and manage security across all of their servers and infrastructure in one place. This is where the conversation turned to the need for a cloud-based intrusion detection solution.

As security experts know, when an organization moves to the cloud it loses control over the physical layer and the AWS environment is no exception. Like many other organizations, Wepa was using a combination of solutions for security and monitoring at other layers but lacked a way to centrally see and manage everything that was on their network layer. This was further complicated by the fact that their infrastructure was mainly relocating into the cloud but would still extend into their local datacenter as well. "That was the point when we really started looking at what kind of distributed security software we needed to implement," according to Mr. Hawkins. The WEPA team then began investigating what kind of perimeter controls they could deploy that would run equally well in Amazon Web Services (AWS), the local datacenter, and an eventual mix of other cloud platforms.

"Wepa is a big open source and Linux shop and almost all of our infrastructure is based on that," says Mr. Noland. So when they look for ways to purchase software, the open source community is the first stop. "We find they (open source technologies) are very stable, very well supported, and there is a huge community around it," said Noland. However, Wepa also needed something with commercial support so they wouldn'thave to hire someone or invest a huge amount of time in building and supporting a custom solution.

As Wepa went in search of an open source IDS/IPS solution, they first considered Snort, a network intrusion detection system created by Martin Roesch in 1998 and owned by Cisco since 2013. Though originally open source, Snort is now owned and operated by Cisco. "We were familiar with SNORT but we didn't choose it because of the need to have a mirror port or span port on a physical switch. That will not work on AWS and you cannot use Snort sensors," according to Noland. WEPA decided to investigate Suricata, a world-class open source network security engine owned and managed by The Open Information Security Foundation (OISF), a 501(c)3 non-profit organization, and the Suricata user community since 1998. Suricata was the perfect solution to the cloud security problem because it operates a layer above the network and switch level but a layer below the applications that were sending and receiving traffic. As a result the sensors could be easily deployed directly to the virtualized servers without any loss of security. "By analyzing the traffic at the first point where it enters the virtual server, we can maintain the same level of security as we'd have by analyzing it before it leaves the network," Hawkins said. WEPA then looked at different commercial IDS/IPS solutions and decided to take a close look at CounterSnipe's Active Protection System (APS) Intrusion Detection/Intrusion Prevention Solution, which is built on Suricata.

The CounterSnipe – Suricata Solution

"We got an in-depth APS demonstration from CounterSnipe, then moved to a proof-of concept in-house," according to Mr. Noland, who conducted the testing. With CounterSnipe's Threat Management Console (TMC) set up, Wepa was able to deploy sensors to their testing environment to thoroughly evaluate their offering.

CounterSnipe's APS includes tools to correlate, analyze and remediate detected vulnerabilities. "We also favor CentOS as an operating system, so it was a big deal that CounterSnipe is compatible with CentOS. The implementation path was very straight-forward," said Mr. Noland.
"There was an option to run CounterSnipe's Threat Management Console within AWS, but that would have required us to move a lot of traffic through a VPN tunnel and we had some concern about how much bandwidth it would require. We decided in the end to run CounterSnipe's TMC in WEPA's local data center," he adds.

According to Mr. Noland, "before we had CounterSnipe in place, we had some level of prevention (blocking ports), but we weren't able to monitor the attack surface in the way we wanted and the controls were not very fine grained." The big advantage to having CounterSnipe was having one console where Wepa could view real time intelligence about security events, and also make changes and have everything flow out where it needed to. It was easy to update rules through CounterSnipe's TMC and this was a big time saver for Wepa as well.

"Leveraging AWS and CounterSnipe together has allowed us to do a lot with limited staff," says Mr. Hawkins. Mr. Noland adds that "CounterSnipe's ability to work with us to provide hands on support and the extra features that we asked for was very important. Asking for a feature improvement and getting it a few months later in the next release was really great."

About WEPA (Wireless Everywhere Print Anywhere)

WEPA is a Print Management Solution developed specifically to remove the cost and pain of student printing managementin higher education and university settings. The school no longer has to manage printing at all, and students have the convenience of uploading their digital contentto the WEPA print cloud from any device and then retrieving their physical documents from any WEPA print station at a later time. The Cloud Storage feature allows users to print from their current file storage solutions by accessing their account and all files directly at the print station. WEPA integrates with the following cloud storage providers: Box, Dropbox, Google Drive, Office 365, and OneDrive. WEPA also integrates fully with existing LDAP/AD/Shibbolethauthentication systems and multiple campus card providers, ensuring convenience and easy maintenance of student accounts for school IT Departments. For more information, please visit www.wepanow.com

About CounterSnipe

Founded in 2013, CounterSnipe Systems recently released Active Protection System APS v9.0, which combines asset discovery, vulnerability scanning and a state-of-the art IDS/IPS engine (Suricata™), with updated malware and vulnerability rulesets (ETPRO™), making CounterSnipe one of the most comprehensive and current Active Protection Systems (APS) on the market. CounterSnipe offer a unique combination of software, services, and training to help organizations secure their in-house or cloud-based/hosted information infrastructures, with a modular and expandable approach and flexible licensing, thus eliminating huge investments associated with dedicated appliances. Our systems are well suited to be deployed by large corporate enterprises, financial, educational, government, managed hosting and service providers. For more information, please visit www.countersnipe.com

AboutSuricata and The Open Information Security Foundation:

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). OISF is led by world-class security experts, programmers, and others dedicated to open source security technologies. As the need for robust and relevant security technologies grows, OISF and the technologies, such as Suricata, they support are ready. OISF is committed to open source security technologies and the communities that keep them thriving has been unwavering.