INTEZER PROTECT

Case Study

iSECURITY
A Calian Company

Chris Stewart, Director of Security Operations

Chris's technical and cloud security expertise span over 10 years and include designing, deploying and overseeing Security Incident and Event Management (SIEM) systems. His familiarity with industry regulations is reflected through his involvement with SaaS and IaaS deployments in the US, UK and in Canada to meet regulatory requirements such as HIPAA, FIPPA and GDPR. Chris oversees iSecurity's Security Operations Center. His industry certifications include Certified Ethical Hacker (CEH) and Certified Information System Security Professional (CISSP).

> **It was important that we found a solution that secures container runtime environments, as we migrate actively to Kubernetes and have a number of Kubernetes customers."**

iSecurity installed Intezer Protect on their Linux VMs and Kubernetes which hosts their internal SaaS platform infrastructure.

Built for Linux and Easy to Deploy

"I have 20 plus years of Linux experience. I was a Sysadmin before the security world for 15 years running Linux. Linux is really my enjoyment in life. I've used a number of solutions in the past and they are always so heavy. The tools worked fine but I found that they consumed high CPU and added 20-30 percent overhead onto any system. The heavier the system workload was, the heavier the resources required by the AV agent.

What I like most about Intezer Protect is that it is light and easy to install. I put it in the automation of Ansible and we were able to push it to all the endpoints very efficiently. When looking at the elastic search database that the tools are running on, and the log ingestion, we don't see any performance impact, or very little impact when you look at the heavy server workloads being run."

> **There are very few solutions which track running memory processes. Most solutions just scan files but that leaves you blind to in-memory attacks."**

CIS Benchmarks

"CIS benchmark standards and vulnerable packages are two features alone that give us visibility into where we stand from a patch management and security hardening standpoint. Intezer has coupled that with something that is more efficient than a standard EDR.

Intezer Protect gives us **immediate value from the patch management side** of the house. There are various ways out there to get patch management information, whether through vulnerability management solutions or patch management software, but I don't think the maturity is there on the Linux side.

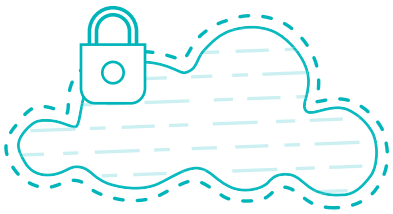
With Intezer, it's nice to see the correlation between vulnerabilities and patches at the same time. CVEs and missing patches are what I'm looking for to improve our patch management process and to accommodate critical CVEs based on what Intezer is presenting to us.

Given the high number of vulnerabilities out there, Intezer's runtime threat detection and response capabilities give us a much needed safety net if we miss something. In the event an attacker exploits an unknown vulnerability we are able to detect and terminate the threat in production, giving us time to properly respond and remediate."

Intezer helps support compliance efforts for CIS benchmarking and SOC 2 among others.

SOC 2 Compliant

"A common way that companies address SOC 2 Type 1 compliance is by having an Antivirus installed on all endpoints, whether that be servers or workstations. Because of the high workload and volume of CPU that we consume on a daily basis, I was hesitant to go down the previous path of taking an AV. It can introduce significant overhead.



With Intezer Protect we didn't see any performance impact when pushing to production. This allowed us to become SOC 2 compliant **without requiring an increase in hardware or financial costs** from a compute standpoint. As Intezer has added features, it continues to add more value from a regulation, patch management and overall security best practices standpoint."

Protect 10 hosts for free