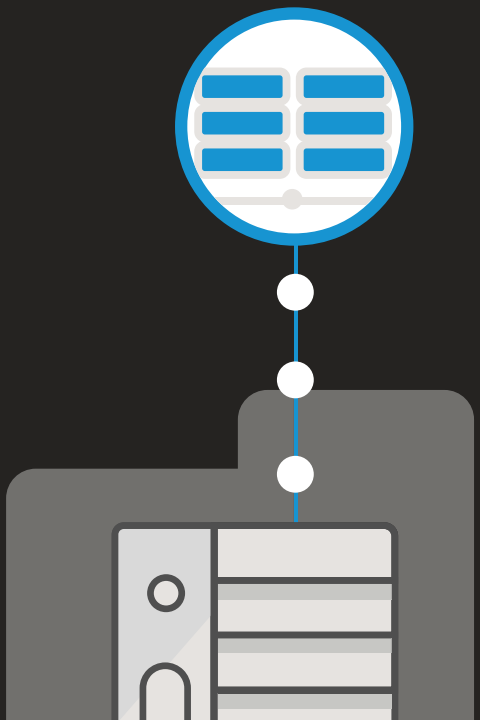
semaphore

Powering Protection:

How Critical Informatics Uses Semaphore's Business Platform to Improve Performance and Reduce Costs



Introduction

When it comes to protecting the most vulnerable organizations and institutions from cybersecurity threats, Critical Informatics stands ready with solutions that are technologically innovative and distinctively human. For over a decade, they've protected the information of those in health care, education, law, business and the public sector from a range of threats, offering Managed Detection and Response with experienced consultants capable of offering tailored solutions and investigating suspected incidents.

To get the job done, they have adopted The Semaphore Business Platform with Cloud Accelerator.

Assessing, Detecting, Responding

Mike Simon, who serves as Critical Informatics' CIO, has been in the security industry for three decades. He notes:

> **"Across the industries, there are certainly regulatory differences, but the basics are the same across the board. We look at things at the network level. We get packet capture and we get logs from security devices and we synthesize things like net flow and take all of that into account to try to understand what's happening on the customer's network."**

A key part of this work is done through CI's consulting arm, which augments their MDR solution and serves as a sort of CSO for hire for vulnerable orgs. Sometimes this involves fixing a vulnerability or investigating a threat. Other times it merely facilitates broader improvements in their customer's overall security profile. "If we're there watching how their network behaves and watching what kind of events are happening on the network," Mike explains, "the analysts and our Security Operations Center can raise their hand and say, 'Wait, this company is doing something really, let's call it interesting. Sometimes it's not a breach but we can tell them about it and the company responds, "Oh, yeah, you're right, that is interesting. Let's fix it."

All of this technology and human investigation relies on the data that comes from their collectors. That data enables significant reductions in threat dwell time because analysts can swiftly identify deviations from the norm, e.g. packet traffic or discordant login locations, within seconds of it happening. That's why Critical Informatics has 24/7 SOC team that can elevate threats immediately and make sure that an otherwise random security alert email doesn't get lost in the shuffle while relevant parties are catching up on their sleep.

Benefits of the Business Platform

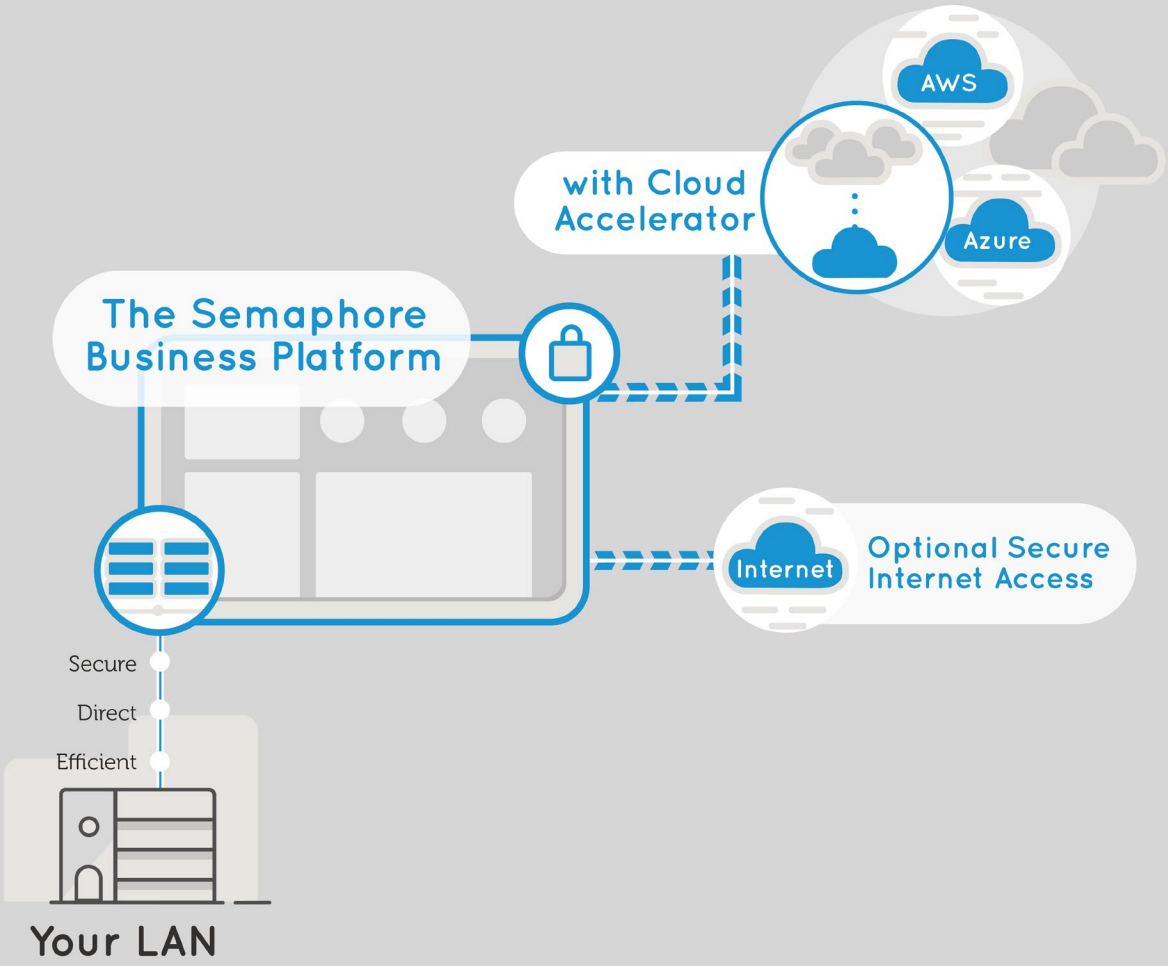
All of this, though, requires reliable and cost-effective access to and processing of that data. That's where The Semaphore's Business Platform comes in. The Business Platform allows customers to quickly and easily establish direct connections to cloud services like AWS or Azure without traversing the internet, reducing vulnerability, and increasing reliability. Data is more secure, and cloud services are faster.

As Mike notes, for a company like Critical Informatics, "that's really useful. Imagine what we do, imagine 180 collectors out in the world gathering up massive amounts of information through packet capture. We can't just send the packet capture upstream—it would kill our customers' networks. Instead, we're processing that packet capture through our IDS and that metadata about potential breaches gets wrapped up and sent to a cluster that is actually hosted on Semaphore's platform. That is what our analysts actually derive data from. When they are deep into an analysis, they're querying that cluster to find out what's going on."

That makes intuitive sense in the normal day to day operations for a company like CI, but it makes even more sense when that day to day goes askew. A little over a year ago, one of the big tech companies had a bit of a snafu with an embedded weather app. It ran amuck all over the world and generated, in Mike's estimation, hundreds of trillions of DNS queries, with the volume of DNS data from Critical Informatics collectors accelerating from 10,000 to 100,000 to several million to a billion in an incredibly short window of time.

This is exactly why hyperclouds exist, of course: to spin up another 50 instances to catch the runoff from the original ten or so. But the data egress costs from sending those packet clusters upstream would have been massive without the direct connections enabled by the Cloud Accelerator functionality in Semaphore's Business Platform. As Mike explains, recalling the incident, "when you hit those high volumes, you become really, really interested in waiving the data transit costs."

In addition, Semaphore's Business Platform allows Critical Informatics to back-up their data up into the cloud, so that it sits in an offsite location. That way, Mike says, "We move that data back the other direction as a part of our back-up strategy. For us, avoiding those transit costs and having greater reliability, and not having to actually put up a VPN, is great. In our experience, VPNs in and out of VPCs at AWS have been notoriously unreliable, whereas the direct connect is absolutely solid."



One and Done

Mike had looked into doing a direct connection with cloud services before turning to Semaphore but had dismissed the idea – despite its advantages – because of the cost and difficulty of the implementing it. "I've known about Direct Connect in general back when they originally built that out as a potential with AWS and then with Microsoft, but it was expensive," Mike recalls. "It's an expensive proposition. Even though it was a very attractive option, it wasn't something I could really justify spending money on. When I talked with Semaphore, and found out how and where it all happens, and that Semaphore can offer it extremely reliably and at a very low cost, it was a no brainer."

The decision has paid off, and the experience has been an extremely positive one. Mike notes that "the team at Semaphore has been amazingly responsive and helpful in every possible way. They're amazing onsite and off. Just every single interaction we have with them at the human scale is stellar."

Thanks to The Semaphore Business Platform, Critical Informatics can continue their work protecting organizations from the variety of security threats while reducing data transit costs and improving the reliability and performance of their cloud services. It is, as Mike puts it, "an incredible level of service that we get anytime we ask, and it keeps us coming back as customers."