Leveling the playing field against cyber threats with machines, AI, and an ear to the ground

An executive interview with SentinelOne's Nick Warner

The mission of cybersecurity firm SentinelOne is to keep the world running by protecting and securing the core pillars of modern infrastructure: data and the systems that store, process, and share information.

Now a public company following the highest-valued IPO in cybersecurity history, SentinelOne has more than 5,400 customers that include three of the top 10 companies in the Fortune 500, hundreds from the Global 2000, thousands of small- to medium-sized businesses, governments, healthcare providers and educational institutions.

The goal is hefty one: to defeat every attack, every second, of every day. To achieve it, SentinelOne deploys innovative machine-learning and artificial intelligence for more effectiveness and accuracy than a human or a crowd–but it continues to value the crowd in order to shift and move with the needs of users and the evolution of cyber risk.

Advisen spoke to Nicholas Warner, chief operating officer, to find out more about SentinelOne and what differentiates the company from others, its value to the insurance industry, and how it stops the current plague of ransomware.

Distilled down, what are SentinelOne's values?

When I got here four years ago, the company was really just starting its go-to-market strategy. We didn't want to overcomplicate it, which many competitors do. We came up with a set of values: accountability, honesty, integrity, a customer-first centricity. We align our services and hire talent with these values. Everyone has an ownership *stake and from that, comes hustle. Our biggest asset is our people; the culture is what's special about the company. We're pretty maniacal about this customer-centric approach–listening to our customers and partners, soliciting feedback. And once we hear our customers need something, we hustle to rapidly innovate for them. For instance, we recently delivered a working version of remote-script orchestration to the market because our customers said they needed it.*

We have an amazing customer support and feedback mechanism in place because we're not going to know what they need–and we're not going to know how running our product at scale works–unless we talk to them. We're provide much more than a set-it-and-forget-it approach.

So, SentinelOne has automated products that can perform better than humans but humans remain a big part of the equation?

We're putting the human focus and attention on the parts that matter while applying machine learning and AI to all places that can and should be applied: automation, detection, and response. We believe many companies do one extreme or the other; they provide a bespoke set of software offerings but it's all tech and no support. Humans are always an important part of the equation. We just want to deploy them in the places that matter, and not where machines can do a much more scalable and performant job. Threat actors know the scales have been tipped in their favor, that this has been an asymmetric war. From a technical perspective, we're trying to even the playing field, but you have to get ideas from outside of the company.

In cybersecurity, too often a hammer gets built for a nail, and no wants to hear that something is a screw and a different tool is needed, or maybe multiple tools. The industry is littered with products that do not adapt or evolve. Attackers have become sophisticated and security controls did not evolve at the same pace. A game of cat and mouse has developed–controls evolve and adversaries' methods evolve to match them.

Since our endpoint detection and response [EDR] build-out, we have revamped and reshaped our user interface twice in four years because we're listening to the customer to understand the workflow. Now we are the highest-rated EDR vendor in the industry but the journey is still going. We're still refining. Many, many vendors never pull this off because they build something in an echo chamber, they have some success and then become irrelevant.

We're building a lot of autonomous software that does great things in an automated way but we've never lost sight of what's important to us–our people, and relying on the people who use our product and who benefit from our technology.

Who is the target customer?

We designed an enterprise software product but what makes us unique is that we can democratize this very advanced technology. Before, you needed dozens of people in a security operations center to sift through data, make correlations, trigger an alert, and initiate a response. We're doing all of that with machine learning and software that runs autonomously. So, although we have some of the largest companies in the world as clients, we also have thousands of SMBs and they are all using the exact same platform. We're finding product uptake across all sectors of the market. It addresses the macro need from a cybersecurity perspective since attacks are hitting everyone, and they are devastating to everyone.

How do you see SentinelOne's effect on the cyber insurance industry?

A SentinelOne-protected customer is a far better client to provide cyber insurance to. It's prevention-focused–we've materially advanced detection and prevention. Our Singularity Platform is a proactive, autonomous solution that boosts security teams' efficiency through security orchestration. We provide an AI-based security operation center that partners with their human SOC analysts to protect, detect and respond to cyber threats in real time. This instantly improves the risk profile of a company.

A day of reckoning has come for the insurance industry. They've realized that what was once a great growth market has become totally unprofitable and almost an uninsurable part of the market unless something really changes from the end user. Right now, end users think they are running protection but it's an antiquated antivirus product or another totally out-classed defense mechanism that doesn't work–especially against ransomware–so sadly, insurers are being inundated with claims and its economically unfeasible. You can't write enough policies or charge enough to cover the ransoms that are being demanded now.

I think the insurance industry is moving from a looming anxiousness to a widespread acknowledgment that something needs to change: "We've got to get our insureds to run better tech to prevent more of these attacks." We can prevent attacks like ransomware, which is the primary concern right now.

We are working with brokers and carriers to educate them on attacks and contemporary threat vectors. Our incident response partners sit on the panels of every cyber insurer and use our platform to respond to incidents and we are working directly with carriers to create pre-breach offerings to prevent a breach.

How does SentinelOne prevent ransomware?

Our machine-learning is super effective in detecting and preventing ransomware. We have a behavioral engine with patents around it to monitor the behavior of systems. The one Achilles heel for our industry has been ransomware but the thing is, ransomware exhibits certain behavioral patterns to enumerate files on a system and evoke an encryption command. Our EDR platform can quickly identify how it got in and respond. We've offered a $1 million ransomware warranty that we have never paid out. No technology is perfect but to date, our clients have made no claims against our warranty in the last four years. That's something insurers are really interested in hearing.

How else is SentinelOne evolving its platforms?

We have a feature in the agent called Ranger that has the capability to connect to all devices. In the past the IT team would be relied upon to deploy and install software to all machines. You can install Ranger on 1 device per subnet and it will passively/actively scan the network and identify all other machines that are protectable and then deploy and install the agent. That capability is totally unique. Ranger can also block unmanaged, suspicious devices from communicating with managed devices. That's critical for organizations that struggle with compliance.

I think a lot of people outside of cybersecurity wonder why companies aren't doing better. A big reason is that they haven't deployed advanced technology to platforms but the bad guys have. The bad guys have worms that jump from machine to machine but the cybersecurity industry does not employ the same idea.

We're investing in EDR and what we call extended detection and response –XDR– because our customers need more efficiency. Security personnel shortages are well documented and we think machine learning should automate and advise even more because the adversary will continue to evolve their tactics.