Q&A WITH MEERAH RAJAVEL

CHIEF INFORMATION OFFICER, FORCEPOINT

As an experienced IT executive, Meerah Rajavel excels at delivering transformation, innovation, profitability, and agility for business through technology. She is a passionate leader who inspires and motivates teams to achieve extraordinary business outcomes through entrepreneurial thinking and collaborative cross-functional partnerships. Currently the CIO of Forcepoint, a global cybersecurity leader, Meerah is responsible for digital and operational transformation with a strong focus on customer centricity, scale for rapid growth, and operational efficiency while minimizing risk.

We interviewed Meerah to learn more about her role as Forcepoint CIO, and how Forcepoint continues to be a market leader.

Q: WHAT ARE THE CORE FUNCTIONS OF THE CIO AND IT AT FORCEPOINT?

My team and I have three main functions:

1. Engine of operational excellence

I look at IT as the engine that provides productivity and scalability with operational excellence. Forcepoint is in a phase of rapid growth and my team and I make sure our company scales in a profitable fashion.

2. Nervous system of the company

If you think about IT today, we are the nervous system of the company because we provide foundational infrastructure, similar to how the brain connects the various parts of the body and allows it to perform. IT must work through a significant amount of reliability, availability, and performance factors in order for us to operate smoothly.

3. Guardian of the galaxy

As CIO, I am responsible for the security of the company. But I must also let the business run at the speed they want to run, just in a safe and secure fashion. My job is to protect, not to be a naysayer.

Q: WITH SO MUCH CLUTTER IN THE MARKET, HOW DOES FORCEPOINT DIFFERENTIATE?

The fundamental crux of Forcepoint's differentiation is our human-centric approach to cybersecurity: when identity compromise is the leading cause of data breaches, only by understanding the typical behavior of every user on a network can you easily spot the abnormalities and the risks. Our Risk-Adaptive Protection solutions automatically enforce security policies depending on the level of risk. This adaptive security allows us to provide the highest levels of user and data protection, while giving people the freedom to do their jobs.

Moving from threat-centric to behavior-centric. You cannot only have dynamic products, you must also enforce constantly. Our unique approach to enforcement is how I believe we differentiate ourselves in the market. Through our risk-adaptive technology, users only receive meaningful events and alerts, and the security response and enforcement can be automated based on the risk threshold rather than relying on human intervention. Instead of chasing thousands of alerts, which is not effective, security teams only take action on fewer, higher quality alerts. It is humanly impossible to deal with all the alerts and events without intelligent automation like we provide in place.

At Forcepoint, we truly believe we are going to change the paradigm by focusing on people and all of their digital identities interacting with critical data and technology. Whether they're humans, accounts, or bots, these entities are controlling how data is moving and who should have access to what data. So, from our point of view, understanding the behavior of people is the most effective way you are going to manage and control the flow of your data.

FORCEPOINT

Creating frictionless security. We really believe in the notion of providing frictionless security, which means security teams maintain control, but the security implemented does not introduce friction to the business. Staying frictionless, maintaining control, and preserving privacy--all three are important.

There are so many security players in the market, and security has been a fragmented market for a long time. Today, if you ask any CIO, CISO, or board member what they are looking for, it all comes down to frictionless security—providing the kind of safety the business needs without compromising productivity. How do you keep control over data without introducing the friction? That is the problem Forcepoint is solving.

Q: WHAT IS THE IMPACT OF DIGITAL TRANSFORMATION ON SECURITY?

Digital transformation comes with significant benefits to the business, and opting-in or opting-out is not an option. Opting-out puts you at a large disadvantage compared to your competition.

Digital is disrupting every single industry, and it does not matter whether you are talking to the CISO, CIO or CTO, they all agree. These executives all say their organization demands innovation and speed from them. They are also concerned about how to manage risk, including security, scalability, and performance.

This changes the role of security. Security used to be the 'fence builders' — saying who is and who is not allowed inside. But today, there is no fence. The world is cloud, mobile and IoT, and these environments are synonymous with digital transformation. Even within your own premises, if you take machine learning into account, all of a sudden you are talking about requiring a different level of security. CIOs and CISOs need to understand that introducing new technology means introducing new vulnerabilities -- and you need to bring in security early on in the conversation.

Q: WHAT IS THE "FORCEPOINT ON FORCEPOINT" PROGRAM?

The objective of our "Forcepoint on Forcepoint" program is to use our own cybersecurity products and make them the core components of how we provide security to our own business. I call it drinking our own champagne — we create quality products that we would use ourselves.

It is important to me to protect Forcepoint with our own technology. I call my team the first and best team of Forcepoint product users. We are the lighthouse customer, which means we tell the product team what the customer's pain is, so they can really steer the boat to address the pain. We are also customer zero, which means before the product is released, we have already implemented it in-house.