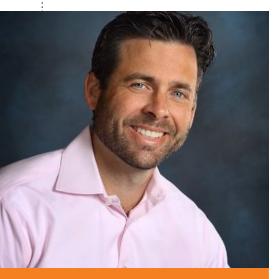# Q&A WITH ROB GREER

CMO & SVP PRODUCTS, FORESCOUT

> " ForeScout is transforming security through visibility. You cannot protect what you cannot see, and ForeScout's unique approach addresses that need. "

With over two decades of technology industry experience, Rob Greer possesses an expansive perspective and a profound background in cybersecurity. Currently, Greer leads the product and marketing organizations for ForeScout Technologies. His primary mission is to provide the glue that links together the market needs, what to build and how to go to market.

Q: WHAT ARE KEY HIGHLIGHTS IN YOUR CAREER?

I've had a unique career path. The first ten years I worked as an IT security and information technology practitioner, which enabled me to understand how to use technology to solve real business problems. I then successfully built one of the pioneer companies in the managed security services market before transitioning from a technology practitioner who worked with many vendors to actually being a vendor and playing on the other side.

Now that I am at ForeScout, my previous experience across sales, sales engineering, professional services, support, marketing and product management allows me to better partner with our customers and value added partner community as I understand their businesses and the problems they are trying to solve.

Q: WHY DID YOU JOIN FORESCOUT?

One of the reasons I joined ForeScout was the clear passion, experience and commitment of our leadership team. We have a highly engaged Board of Directors, which represents the best of the best in the cybersecurity industry. I realized there was a huge opportunity to be part of a company that offered differentiated and proven technology sold at scale to the largest institutions in the world. With my strong technical pedigree, as well as my sales and marketing background, I had a chance to really make a difference on the team and an impact with our customers and partners.

I also joined because ForeScout is transforming security through visibility. You cannot protect what you cannot see, and ForeScout's unique approach addresses that need. The company is also a unifier of the disparate information security market. We make existing IT and security tools smarter by sharing relevant device context as well as taking actions that most tools are not in a position to execute, such as taking a device off the network.

Q: WHAT IS FORESCOUT DOING IN 2017?

In 2017, ForeScout is defining IoT security. Our strategy, messaging and tactics are focused on helping organizations secure IoT by first gaining visibility and control of devices connecting to their network. Our agentless approach makes this possible at scale. Once ForeScout discovers, classifies and assesses these devices, our technology then makes other IT and security tools smarter by sharing their 'context'. ForeScout is the only player in IoT security that focuses on connecting disparate IT technologies as a full-time business – not a front for selling switches, servers, operating systems and security services.

Q: WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS AND CISOS?

The most common question I hear from customers is, "How many devices do you believe ForeScout will see that I don't already know

CALCULATING BUSINESS VALUE

According to a 2016 IDC Research Study, "IDC believes that one of the key attitudes for organizations to adopt is that of "already breached." This attitude focuses on visibility and detection, with strong remediation capabilities. Instead of perfectly protecting each and every vector, this attitude encourages constant vigilance and the ability to respond quickly, making the organization's security agile enough to meet the rapidly changing business and threat landscape. One solution that addresses this idea of pervasive device visibility and control is ForeScout's security solution."

Source: IDC White Paper; The Business Value of Pervasive Device and Network Visibility and Control with ForeScout. December 2016
For the full report, visit http://resources.forescout.com/idc_businessvalue_bdm_klogix.html

392% five-year ROI

24% more known devices

50% fewer network-related security breaches

---

about?" CISOs are able to see up to 60 percent more devices than they did prior to deploying ForeScout. This usually drives enough attention to find the necessary budget. Additionally, budget often already exists for endpoint protection, endpoint detection and response and network access control projects prior to ForeScout being evaluated.

I was recently with the CISO of a large UK bank and her biggest challenge was answering the question of 'how secure are we?' I asked her if she knew, in real time, what is connecting to the environment across the entire enterprise. This is key because having a comprehensive view of what devices are connected provides a clearer backdrop to have a conversation with the board. She said she had no idea, but knowing this would provide a sense of confidence in terms of visibility and potential exposures. I discussed with her how transforming security through

visibility is a business problem the board wants to understand. You cannot answer the question around whether or not you have security exposure without understanding what's connecting.

Q: WHAT TRENDS DO YOU DISCUSS WITH CUSTOMERS?

Organizations are recognizing that IoT is real in the campus; the days of voice, audio video, physical security systems, HVAC, etc. being whitelisted by IT are over. Organizations have adopted operational technologies (OT) that are now IP-connected – from healthcare, to retail, to power and gas, to manufacturing, and more – and they need to monitor and secure those business-critical devices that in the past were air gapped from other IT services. Organizations are also moving to the cloud across all vectors including data, apps and infrastructure. They are looking for a single pane of glass

to see and control these virtual and physical devices.

Q: LOOKING BACK, WHAT ARE SOME SIGNIFICANT SUCCESSES AND CHALLENGES IN YOUR CAREER?

Twenty-six years in the industry has given me a lot of perspective. Challenges have come in the form of technology shifts, cost-cutting exercises, acquisitions and divestitures.

I am most proud of being a CEO in the late 90s of one of the pioneers in the managed security services market. For me, looking across the cybersecurity industry and seeing so many talented and successful people that I have worked with, mentored or have been mentored by, makes it all worth it. This industry matters more than ever before, and I love being part of the community that is committed to protecting the digital world we rely on.