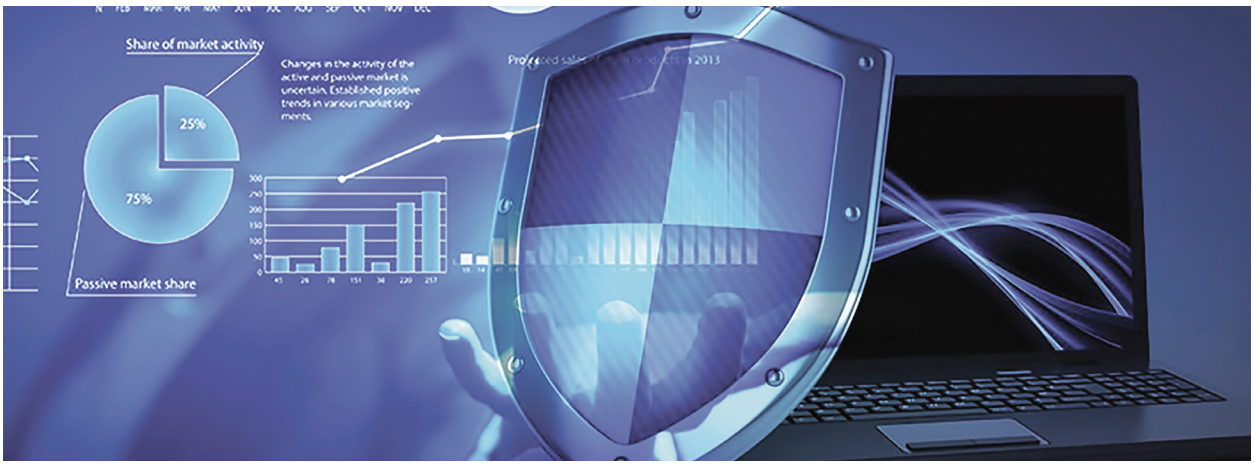
Lacework:
Avant-Garde Security



In today's highly dynamic cloud environment, Lacework brings speed, automation, and scale to cloud security so that DevOps and security teams can keep data and application secure. Lacework redefines security by enabling configuration assessment, behavior monitoring, threat and anomaly detection, and incident investigation. The firm supports public and private clouds, VMs and containers, Docker or Kubernetes, Linux or Windows Server, and therefore, enables security teams to protect data in the cloud and maintain compliance.

In discussion with CIO Applications' Stefan Dyckenhoff, President & CEO talks about how Lacework helps firms bring speed and automation to every cloud security process.

Could you give us a detailed insight of Lacework and explain how it has been effective in mitigating cybersecurity hurdles?

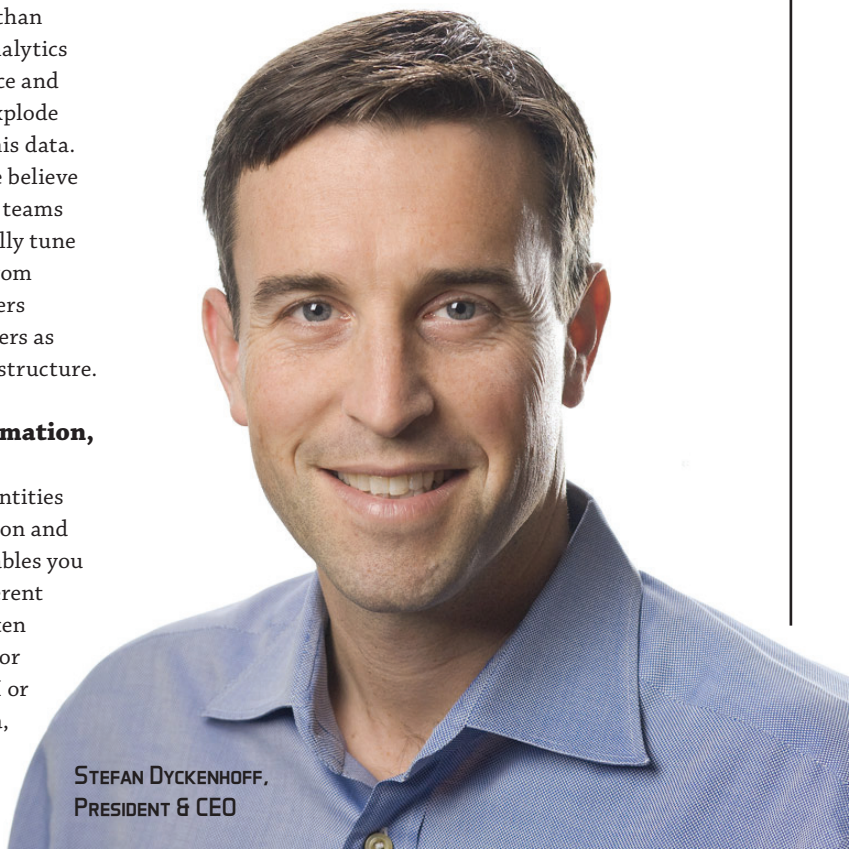
When we stepped into the cloud cybersecurity arena, the cloud-operating model was still emerging. We realized that the next generation of security solutions was about automation and analytics; hence, we recruited a team with expertise in cybersecurity, Big Data, and DevOps. With a group of relatively diverse people, we conceptualized Lacework with a mission to automate cloud security, allowing our customers to safely innovate in cloud environments. We address numerous pain points presented by public cloud operating models and think distinctively about how security works and how effectively it can be delivered to security teams. The cloud is built differently: the attack surface is different, threat vectors focus at the application and user level as opposed to the machine and network level. The level of automation we bring to cloud security enables security teams to operate at the same pace as DevOps operates cloud environments and publishes new code.

> Our vision is to be a trusted SaaS platform that covers all aspect of security

How has Lacework become a game changer through solutions that it offers?

We aim to empower clients with a holistic and trusted SaaS platform that gives them a competitive edge from a security standpoint. We address four core points-compliance, visibility, threat detection and investigation in the platform.

We focus on collecting far more data from the cloud than other approaches. Because we curate data keeping analytics in mind, we give clients more insights into compliance and security risks. The 'secret sauce' is that you cannot explode the cost or the compute footprint as you collect all this data. With automation becoming a pillar of technology, we believe in building a product that both security and DevOps teams can embrace, hence, we eliminate the need to manually tune policies, analyze and correlate data across systems from network to applications. We built a solution that covers traditional VM-based architecture as well as containers as they get integrated into every customer's cloud infrastructure.



On the Polygraph technology bringing automation, scale, and speed to cloud security:

Polygraph monitors the activity and behavior of all entities in your cloud. It emphasizes organizing all information and connecting massive amounts of metadata, which enables you to automatically learn the relationship between different entities in your cloud. We built a collection of about ten polygraphs that we track over time. Some track user or network behavior while others track application, VM or container behavior. With polygraphs organizing data, you are assured of compliance and if something goes wrong, you get specific high-value alerts that can be investigated quickly. With Polygraph, your security can keep up with the pace at which you deploy new applications in the cloud.

How has Lacework helped a client overcome business challenges and attain desired outcomes with its solution?

Snowflake, a cloud-based data-warehouse provider realized that handling security changes only once a month was insufficient, as application and code changes were happening at lightning speed. The hectic task of managing and updating security rules with the conventional security tools they were using was increasingly overwhelming their security team. When Lacework stepped in to help identify and trace the attack patterns of PEN testing, it also gave them full visibility into what was happening in their cloud environment. They soon realized that, with Lacework, the couple of hours spent daily to update rules and review incidences could be cut down to 50 minutes of analysis.

With an aim to provide avant-garde security, what makes unique Lacework in this arena?

We believe that the polygraph technology is fundamentally new and is able to process a hundred times more data efficiently and cost-effectively. This enables us to process and make sense of the large volume of API events generated in cloud environments like AWS where everything is controlled and orchestrated through APIs. We are a multi-cloud platform, but are very focused right now on AWS because that is where we see many customers experiencing challenges with security. So we have built core capability that allows us to both gather more data and better insights and move faster.

Most important, the heart of any successful company is its culture and Lacework brings people from different spaces to think about the cloud security problem. We put a lot of efforts into building collaboration across different disciplines and enable a high-performance culture. We believe in the 'survival of the fittest ideas'.

How does the future look for Lacework?

Our vision is to become a trusted SaaS security platform that covers all aspect of a customer's business in the cloud. We are also engaging with established companies that are moving their business to the cloud. Security for these companies is not just an obstacle to overcome. The ability to innovate fast in the cloud and do so safely is a business enabler. Our goal is to capitalize on the opportunity to redefine a security stack that works for cloud environments. CA

CYBERSECURITY SPECIAL

CIO APPLICATIONS

APRIL - 2018
CIOAPPLICATIONS.COM

Company:
Lacework

Key Person:
Stefan Dyckenhoff
President and CEO

Description:
The firm supports public and private clouds, VMs or containers, Docker or Kubernetes, Linux or Windows Server

Website:
lacework.com

Top 25 Cyber Security Companies - 2018

In today's connected world, there is a sharp increase in the use of digital technologies, making businesses more agile and adaptable. However, this has lead to a surge in the number of potential ways cybercriminals can gain access to enterprise networks. Cyber attacks are constantly evolving and its detection is becoming tougher by the day, therefore, it is necessary for businesses to have apt cybersecurity measures in place to thwart these threats. At the helm of helping advance cybersecurity, experts are leveraging the latest technologies and architecting solutions that can proactively identify and eliminate these new-age threats.

Organizations are taking steps like patching and updating systems, regularly backing up data, and strengthening real-time defenses to tackle different kinds of attacks. Innovative technologies like artificial intelligence and machine learning are being used to predict and accurately identify attacks. Multifactor authentication is being implemented by businesses as they are more secure, usually involving biometrics like voice, retina, and fingerprint recognition, thereby making it harder for an attacker to breach a network. Technologies like encryption and tokenization are applied to protect data, dramatically reducing its exposure and risk. Furthermore, deep learning with its ability to identify safe and unsafe software is a significant boon to security practitioners who seek to decrease the time taken for advanced threat detection and eradication.

In the light of this, a distinguished panel comprising CEOs, CIOs, CTOs, and analysts including the CIO Applications editorial board has evaluated and selected the leading cybersecurity solution providers that have in-depth expertise and are at the forefront of tackling any type of cyber attack.

We present to you CIO Applications' "Top 25 Cybersecurity Companies – 2018."

44790 S. Grimmer Blvd
Suite 202, Fremont, CA 94538
T:510.757.1040

www.cioapplications.com