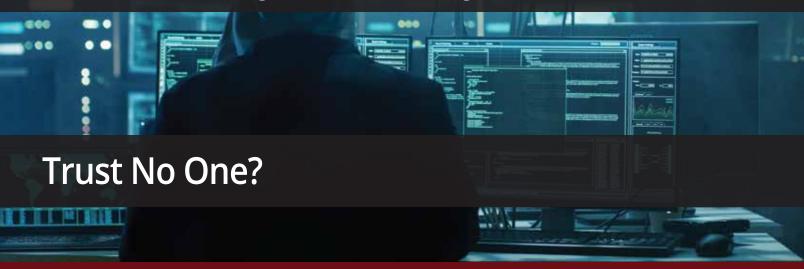


Zero-Trust Cybersecurity



Protecting digital assets is becoming harder and harder, for one alarming reason: most organizations have poorly prepared for the deluge of cloud-based applications and end-point devices. This transformation has created vulnerabilities well beyond any corporate-controlled environment, expanding the potential for data breaches into completely unchartered territory.

As the enterprise perimeter dissolves, cybersecurity today must extend beyond simply protecting on-premises data. Anyone authorized to have access to data and applications should have the flexibility of using any device, on any network, from any location. This ever-increasing desire for seamless access has created a corresponding need for end-to-end security across a myriad of applications, data centers, and devices. The cost of failing to do so is potentially huge. According to a recent study sponsored by IBM, the average cost of a single data breach is over \$3 million.

Originally conceived by Forrester, the "zero-trust" model has been gaining momentum, from Google's BeyondCorp to Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA). If implemented properly, zero-trust has the power to transform the industry.

- Will micro-segmentation and software-defined perimeters offer enough protection?
- What are the implications of default-deny
- Is zero-trust security destined to become mainstream?

Join us on April 9 to find out.

Moderator

Randy Wood, Vice President, Public Sector, Akamai Technologies

Panelists

Amir Sharif, Co-Founder, Aporeto

Andrew Rubin, CEO and Co-Founder, Illumio

Deepak Jeevankumar, Managing Director, Dell Technologies Capital

Pere Monclus, VP & CTO, Networking & Security BU, VMware

Tuesday, April 9, 2019

6:00 pm - 8:30 pm

6:00 pm: Reception and demos 7:00 pm: Panel discussion (with Q&A)

Hauck Auditorium

David and Joan Traitel Building 435 Lasuen Mall Stanford, CA 94305

Register at the link below.