Forbes / Tech / #CyberSecurity
APR 3, 2018 @ 01:07 PM 2,450

The Cloud Is Rising To The Cybersecurity Challenge

Kalev Leetaru, CONTRIBUTOR
I write about the broad intersection of data and society. FULL BIO
Opinions expressed by Forbes Contributors are their own.

Guy Fawkes masks. (AP Photo/Seth Wenig)

In a world of seemingly hourly data breaches, it can seem at times that the battle for cybersecurity has officially been lost and that there is nothing more for businesses to do but wait for the inevitable breaches to come and perform damage control. Smaller businesses without the means to invest in advanced cyber defenses find themselves inundated with questionable solutions that offer few protections, while larger companies struggle to afford maintaining large staffs of top security professionals. Into this cyber Wild West, the major cloud companies have begun moving aggressively to take their own lessons learned and massive internal security

investments and make them broadly available to the rest of the world. Could this finally shift the cyber tide?

Cybersecurity was front and center at last year's Google Next cloud conference, with a wealth of announcements and reminders of how the company has begun externalizing its security prowess through a series of new offerings. Last month the company followed this up with a flurry of new announcements from access auditing to data loss prevention to identity controls to new partnerships with third party security companies, emphasizing just how much of a growth area the major cloud companies see the cyber environs.

Some of these new tools, like Google's Cloud Security Command Center, are essentially cloud-scale security scanners, designed to survey a company's entire cloud footprint, identifying potential vulnerabilities or forgotten entrance points. Given that one of the most common causes of data breaches in the cloud are misconfigured access restrictions on storage resources and forgotten or improperly secured systems, such scanners should help close the remaining gap, especially when paired with a renewed focus on user management in the cloud era. Unlike the VPN castle defenses of past, in which companies surrounded their assets with extensive monitoring, but blindly trusted anyone that got inside, cloud vendors are pushing businesses towards their own "trust nothing" model that better reflects the reality of the uncertain world in which we live. Instant infrastructure DDOS protection allows companies to better fend off crippling attacks using the same systems that protect Google itself.

Preventing malicious insiders and skilled attackers that manage to get in through the front door from walking back out the door with a company's crown jewels has gained renewed emphasis, with Google's DLP API removing many of the barriers to companies being able to implement enterprise-grade filtering, from OCR'ing of image content to contextual detection. One-click statistical outlier detection makes it easier for companies to identify inadvertent holes in their anonymization workflows. Third party partnerships offer countless additional services, while improved auditing allows total visibility into all access of a company's data.

Amazon and Microsoft have similarly invested heavily in helping their customers build security-conscious applications and infrastructures that are designed for today's world, rather than the quaint naïve blind trust of yesteryear's web. Moreover, the major cloud vendors' global footprints mean companies can mitigate their physical risk as well by distributing their applications geographically, allowing for seamless continuity of operations even in the face of natural or human disasters.

Putting this all together, Google's flurry of new security announcements last month reflect the growing emphasis cloud vendors are placing on helping businesses reimagine how they manage their data in a threatening world, from world class DDOS protection and vulnerability scanning against outsiders to powerful identity access controls, DLP and auditing against insider threats, all based on the same tools the cloud platforms themselves use to secure their own systems, built upon years of lessons learned from running some of the world's most prominent websites. Perhaps as small businesses let go of the 5-year-old unpatched server shoved in the closet and large businesses transition from home-grown patchwork systems of blind trust, the commercial world's embrace of the security-first environs of the modern cloud will slowly turn the tide against the hourly breaches that plague today's data-drenched world.