EVOTEK Cybersecurity Predictions

Hit or Miss?

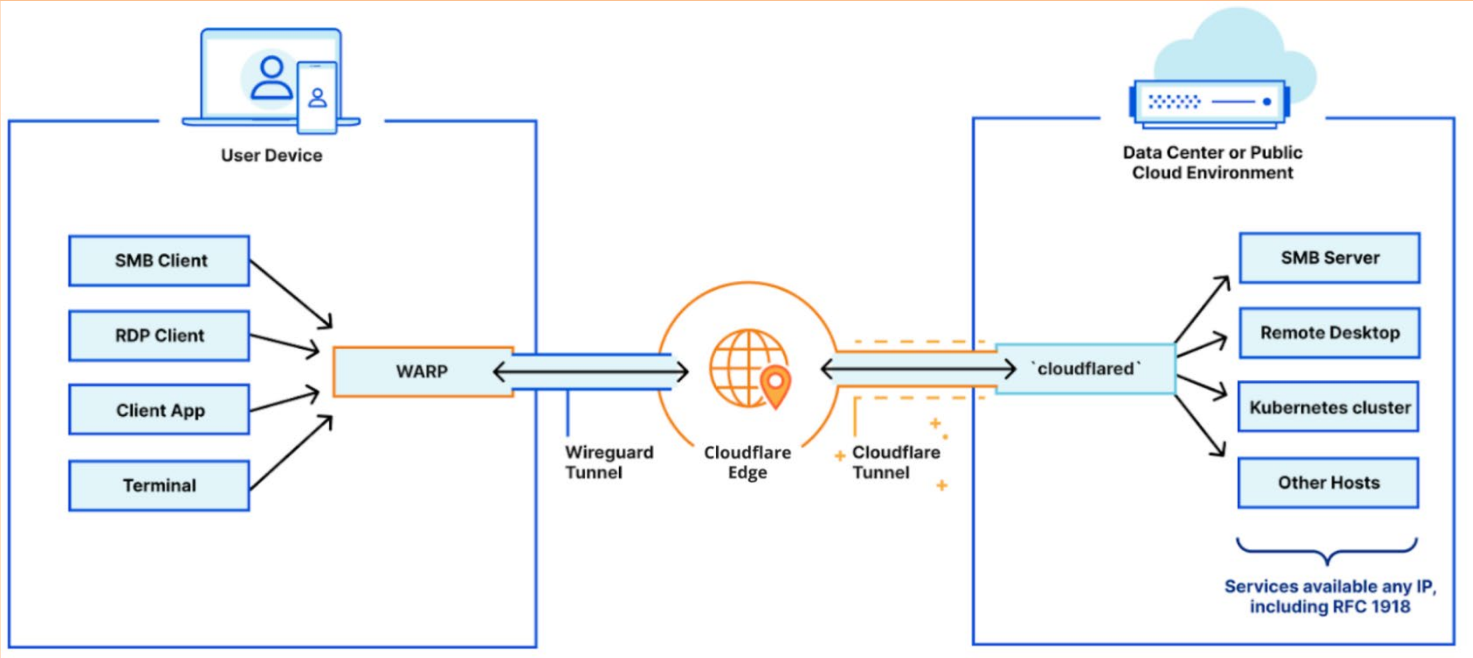
EVOTEK leadership, Matt Stamper, CISO, Executive Advisor, and Macy Dennis, CSO, provided 2021 cybersecurity predictions to CSW. Now that we are halfway into the year, let's look at whether industry movement matches expectations.

Matt Stamper - "2021 will be the year of SOAR and investments in enhanced detection technologies including deception. I am cautiously optimistic that the improvements in security automation, the outstanding work in discovering zero-day vulnerabilities, and other software flaws will improve such that we'll see real reductions in dwell time. I also predict that cybersecurity as a topic for the board of directors will continue to be front-and-center – notably for public companies who are required by the SEC to provide accurate and complete disclosures related to their cyber risks. This focus will drive enhancements as to how organizations address patching and vulnerability management for their technology stacks. Sadly, we will also see the loss of life where OT or heathcare-related technologies are compromised, exposing new levels of liability for organizations in critical sectors."

Macy Dennis –

- "Organizations will increase focus on application and cloud security-focused programs. They will enable the remote workforce, Data Protection Programs, CMMC Certifications."
- "Organizations will improve their Incident Response process and conduct more IR Workshops and Tabletops."
- "Organizations will focus on more services around DevOps, CI/CD pipeline vulnerability testing, and vulnerability management systems."
- "Products and solutions will be more cloud/SaaS focused, primarily due to COVID."
- "Clients will be more focused on outsourcing services with minimal products."

- “2021 will see many moving more systems to the cloud and SaaS solutions.
- “Organizations need to assess themselves with a risk-based focus – this will include building out a risk register and performing more threat modelling exercises to identify the organization’s overall true risk posture.”
- There is not going to be much change in 2021 with the WFH aspect. People feel safe sitting at home. But they are more likely to be a bigger target and easier to access. Those companies that didn’t plan to secure their workforce at home better will need to and, if not, will find themselves in a bad spot.
- “I predict the ransomware attacks to climb as the nation-states are using it to fund their operations. And because of this, the security budgets will increase.
- “2021 will also see Organizations focus more on a Zero Trust model.”



Zero Trust rules are enforced on the Cloudflare edge

CLOUDFLARE®

A Zero Trust solution requires operational capabilities that: 1) Never trust, always verify, 2) Assume breach - continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity, 3) Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.Top Zero Trust vendors include Akamai, Cisco, Cloudflare, Illumio, Palo Alto Networks, Symantec/Broadcom, Okta, and Forcepoint.

Karen Heumann
G2M Communications