Fight Fast:

Breach Prevention in Real Time — Any Time, Any Location

Why healthcare systems need scalable remote visibility, security and remediation

As healthcare organizations increasingly move their data and workloads to the cloud — transforming how and where they operate to deliver critical care — remote visibility, security and remediation have become required elements in breach prevention. That's because security policies and processes can no longer take for granted that IT staff will always have physical access to the network or its endpoints.

"Healthcare systems have prepared for and experienced natural disasters such as hurricanes, flooding and tornadoes. They may have experienced swine flu. But what is unprecedented is the scope and speed at which the COVID-19 pandemic is moving. This is driving a massive transition to remote workers."

CURT AUBLEY | SENIOR DIRECTOR FOR PUBLIC SECTOR AND HEALTHCARE SOLUTIONS AND STRATEGY | CROWDSTRIKE

Case in point: the current COVID-19 crisis. The pandemic has forced hospitals and healthcare systems to turn themselves inside out in response to the unprecedented surge in demand. Practically overnight, healthcare providers have launched field hospitals to expand capacity, established drive-through test centers and begun treating less critical patients via telemedicine and virtual examinations.

At the same time, these organizations are trying to ensure business continuity while protecting the health of their employees — resulting in a sudden, unplanned transition from primarily on-premises work to primarily a remote workforce.

"Planning for disaster recovery and operational continuity isn't new," says Curt Aubley, Senior Director for Public Sector and Healthcare Solutions and Strategy at CrowdStrike. "Healthcare systems have prepared for and experienced natural disasters such as hurricanes, flooding and tornadoes. They may have experienced swine flu. But what is unprecedented is the scope and speed at which the COVID-19 pandemic is moving. This is driving a massive transition to remote workers."

As a result, many healthcare organizations are discovering that their legacy policies and on-premises solutions lack the ability to operate and/or scale up rapidly, while others simply lack the technology, operational virtual processes and policies to deploy remote workforces.

"If you are using '20th century' on-premises security technologies, it quickly gets complex and problematic," Aubley says. "To securely add support for 25,000 remote workers, you have to add VPNs

"Adding 5,000 additional remote workers in an hour is no problem for a cloud provider. That is something that's a little different than traditional, on-premises security."

CURT AUBLEY | SENIOR DIRECTOR FOR PUBLIC SECTOR AND HEALTHCARE SOLUTIONS AND STRATEGY | CROWDSTRIKE

[virtual private networks] — physical VPN units — more networking equipment, and more bandwidth ... a lot of bandwidth. You also have to add servers to be able to support all of the remote workers from a security perspective."

Staying ahead of the surge

A further complication is that in the middle of a crisis or disaster, your IT team may be working from home as well.

"Asking IT to spin up hundreds or thousands of new users, train them and provide support — when also requiring them to work remotely — is diametrically opposed," Aubley says. "Who wants to be on-premises and do all of this equipment deployment work? And how long will it take them?"

Indeed, speed and simplicity for end users and IT staff alike are critical elements in any surge response. That's where cloud-based services and security offers clear benefits. Leveraging the hyper-scaling advantages in compute, storage, and network, Aubley says that a cloud solution can help organizations of any size launch and support a remote workforce securely in a time frame measured in minutes or hours, not days or weeks.

"Adding 5,000 additional remote workers in an hour is no problem for a cloud provider," Aubley says. "That is something that's a little different than traditional, on-premises security."

Speed is not merely important in remote workforce provisioning — it's also critical for continuous breach protection. Aubley recommends adopting the "1-10-60" security rule as a standard.

"Research by the CrowdStrike® Intelligence team shows that, on average, if an adversary gets into a customer's enterprise, they will dwell for two hours before breaking out and taking action on an objective," he says. "If security operations teams don't have the visibility to prevent or detect an adversary within one minute and have all of the forensics data you need within 10 minutes — so within 60 minutes you can remotely remediate — you will lose and the adversary wins."

Empowering a cybersecurity team to detect and prevent security breaches remotely and in real time is crucial when adversaries are taking advantage of crises, such as the COVID-19 pandemic, to attack potential vulnerabilities in newly extended or expanded networks.

Availability remains crucial

Beyond choosing the right technology to ensure security for your business, the COVID-19 surge provides another reminder that setting security policies and procedures must be an ongoing exercise.

"You need to continuously assess confidentiality, integrity, availability and your overall risk posture," Aubley says, keeping in mind that your number one responsibility is to maintain the integrity of systems used by healthcare workers so they can fulfill their healthcare mission.

"Are you managing risk appropriately, so that providers can deliver healthcare uninterrupted in a dynamically changing world?" Aubley says. "If the answer is anything but a confident 'Yes,' then I'd recommend you reexamine your strategy, your policy and the technology partners that you choose in helping you achieve it. Doing the 'same old, same old' in our world today does not cut it."

CROWDSTRIKE

About CrowdStrike

CrowdStrike® Inc., a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.