citrix

Data Sheet

Stop ransomware attacks through security automation with Citrix Analytics for Security

A successful ransomware attack can cripple your business. See how proactive security and automation can detect and prevent ransomware before it strikes.

The threat of ransomware

Imagine you log on to your computer to start your workday, like any other day. You open the file you've been working on for the last week, hoping to get it to the team for review. But instead of seeing the product of hours of work, you see a message from an attacker. They've broken into your files, encrypted everything, and are demanding a ransom for you to get it back.

Unfortunately, this is a common event with serious results. Ransomware attacks like this hit a business every 14 seconds. The average ransomware attack shuts down the business for 16 days. Attackers have also gotten bolder, with the average demand to decrypt files doubling in the past year.

Why cybersecurity training isn't enough

Many organizations try to prevent ransomware through training. There's a challenge with this approach, though. Research shows that after a year of regular training, the best-case scenario is 98% effectiveness. This may sound impressive. But remember it only takes one: one employee clicking one malicious link one time. That one click can introduce ransomware that infects your entire network.

Many organizations hire a full-time security employee. They're tasked with watching company systems. The goal is for them to catch and stop attacks as they happen. This approach has downsides as well. Round-the-clock, human observation of employee activity is costly.

Human error also comes into play. This approach relies on a trained eye to detect patterns that show an attack. This person must also know how to stop the attack based on the pattern. Hiring the right person, or people, for the job can be challenging and costly.

How Citrix Analytics for Security prevents ransomware

Citrix Analytics for Security prevents ransomware attacks before they happen. It starts by using machine-learning algorithms to understand your user's behavior. It then spots unusual behavior like mass downloading and uploading of files. This activity is a signature of a ransomware attack. More than a notification system, this is when Citrix Analytics for Security springs into action. Proactive, automated actions like logging users out and locking accounts prevents further damage.

What it means for you

Citrix Analytics for Security is a cloud-based, machine-learning driven security tool that supplies proactive, automated security for your organization. With round-the-clock monitoring, Citrix Analytics for Security ensures your organization stays protected from ransomware attacks, ensuring your business avoids the costly downtime and remediation of ransomware attacks.