citrix

5 reasons your IT team needs Citrix Analytics for Security

From malicious attacks to human error, the perils of intellectual property loss lurk around every corner. As work environments expand, so does the attack surface. Now more than ever, you need a way to keep networks, data and apps secure — without hindering the user experience or slowing progress. Citrix Analytics for Security provides the exact insights you need to protect against threats while moving forward with new technology.

Here are five reasons your IT Team needs Citrix Analytics for Security:

1. Threats are mitigated continuously and autonomously.

With thousands of security alerts flowing into IT each day, the last thing you need is more notifications to manage. That's why Citrix Analytics for Security monitors each session for you. As inconsistencies are detected, mitigative actions are applied autonomously. You can safely adopt new technologies that drive the business forward, while resting assured intellectual property will stay protected.

2. You can take steps to proactively detect and resolve threats.

With Citrix Analytics for Security, it's easy to protect against external threats. Predefined policies quickly detect anomalies, such as compromised credentials or excessive file sharing, and can be customized as needed. You can use monitoring mode to trial the experience before rolling it out to employees, and collect user feedback to eliminate any unnecessary disruptions.

3. Vulnerabilities are found fast.

It's not just malicious attack attempts you have to worry about. Human error and system glitches are often to blame for data breaches, and can take months to identify and contain. By assigning a risk score to every user action, Citrix Analytics for Security brings all vulnerabilities to the surface. Unusual logins and app usage impact the risk score, as do device IDs and IP addresses. So if a behavior is atypical, it'll be recognized in an instant.

4. Internal threats and exfiltration attempts are caught early.

Perimeter-based security solutions keep suspicious activity away from your network. But what happens after access has been validated? Citrix Analytics for Security uses machine learning to create a real-time risk profile for each user within the corporate network and continuously monitors user behavior. If activity starts to sway from standard behaviors, preventative action is taken immediately.

5. Internal threats and exfiltration attempts are caught early.

There's no need to rip and replace your current solutions. Citrix Analytics for Security is a turnkey solution that lets you leverage your existing infrastructure and investments. Just turn it on and go — no deep expertise or experience needed.

What's different about Citrix Analytics for Security?

As the only user-centric solution that seamlessly integrates into your digital workspace experience, Citrix Analytics for Security will automatically detect and mitigate malicious activity — without disrupting the employee experience.

For more information, please visit www.citrix.com/products/citrix-analytics-security