Detect and prevent insider threats with Citrix Analytics for Security

With legitimate access to your most sensitive corporate assets, malicious insiders can cause more damage and leak more data than the most skilled attacker

Access drive productivity

Accessing apps and files drives productivity for your employees, partners, and contractors. Consider a call center agent. They can't do their job without access to your CRM. An accountant can't balance the books without accessing spreadsheets. And an HR rep can't administer benefits without seeing employee's personal information. Frictionless access to these business-critical apps drives productivity.

Balancing productivity and security

Access is necessary for employees to stay productive. But staying balanced with security measures is just as important. Many security strategies employ a "castle-and-moat" approach. These policies put strict controls on outsiders to keep them outside. But those already "in the castle" can move about with little oversight or restriction.

Malicious insiders can exploit this strategy. Their unrestricted access leaves them to take sensitive company data. Take a salesperson leaving for a competitor. They can download client information to give them an advantage at their new company. A payroll administrator can take employee information to sell on the black market. A disgruntled employee can steal data just to wreak havoc.

These employees all have legitimate access to your apps and data. So, it can be difficult to detect and prevent these attacks before they happen.

How Citrix Analytics for Security prevents insider attacks

Citrix Analytics for Security takes a proactive approach to stop insider threats. It uses machine learning to create a baseline of normal user behavior. This enables it to detect when user behavior is outside the norm. Indicators of an insider threat include:

- significant data downloads
- heavy use of the clipboard
- accessing apps at unusual times

After recognizing these activities, Citrix Analytics for Security springs into action. Automated policies can:

- log users out of accounts
- expire links to shared documents
- notify users their behavior has been flagged

What it means for you

Balancing employee experience with data security is tough, no matter the size of your business. Making sure employees with privileged access don't leave with company data is of high importance. Citrix Analytics for Security helps create that balance with no sacrifice. You can supply the same level of apps and data to your employees. But machine-learning algorithms detect and prevent against insider threats. This balance helps keeps employees productive and data safe.