Leveraging Advanced Analytics to Detect User Security Threats

Table of Contents

Combatting a changing threat landscape

The widespread adoption of cloud, mobile, IoT, and big data has accelerated the shift to a dynamic, digital workforce. Today, organizations are embracing SaaS, cloud, and mobile applications, as well as hosted services that live on-premises, or in a hybrid or multi-cloud environment. While many of these apps and services are sanctioned by IT, some are not.

Employees are also engaging in Sneakernet and Shadow IT to access apps and exchange data; bypassing their IT departments. Without end-to-end network control or visibility, IT struggles to identify and address potential cyber threats, performance issues, and unexpected changes in user behaviors.

90% of companies use public cloud solutions.[1]

The typical company now uses more than four public cloud applications, as well as more than 14 enterprise apps.[1]

There will be 30 billion devices connected to the Internet by 2020. These devices will generate more than two-thirds of business data in the same period.[1]

At the same time, bad actors are more professional and better organized. 73 percent of breaches are financially motivated and supported by organized crime, nation-states, or espionage.[2]

While the majority of breaches are instigated by outsiders, IT and security teams must also be vigilant in monitoring the network for insider threats. These can be even more problematic since they are already located within the security perimeter.

From IT managers to network and security administrators, up to the C-suite, there is a heightened focus on protecting intellectual property, customer data, and ultimately, brand reputations. IT must correlate data from disparate products and systems to gain better insights into user behaviors. They must also leverage this intelligence to proactively address potential breaches and security attacks.

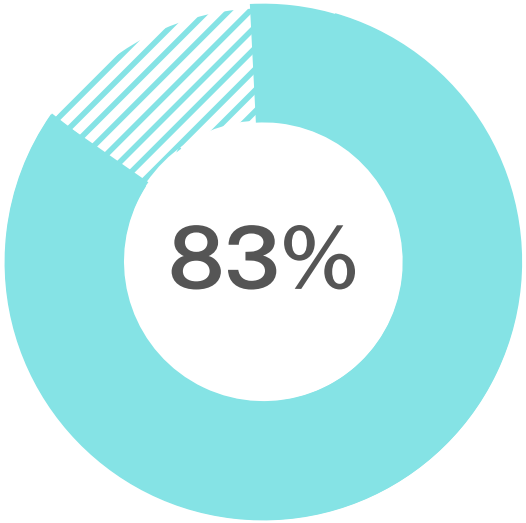
The IT challenge – monitor, analyze, and address known and unknown threats within the digital workspace

While IT still controls the corporate network perimeter and manages many business applications today, information digitalization, ubiquitous Wi-Fi, and BYOD continually expand the environment to be secured. This poses new and greater security challenges.

- There are holes and black areas where there is less or no visibility.
- There is less predictability which results in more control issues.
- Manually uncovering insider threats is nearly impossible and incredibly expensive.

IT teams currently correlate data from disparate products and systems. This expensive, time-consuming approach doesn't provide the visibility and control they need to manage and secure the digital workspace.

With complexity being the biggest enemy of security, a completely new approach is required.



That's how many businesses believe the complexity of their organizational structures and IT infrastructure is putting their companies at even greater risk for security breaches.[3]

Putting users at the center of security

Traditionally, an organization's perimeter was the data center. As networks expand, the perimeter has become more fluid, necessitating a change in security policies.

A modern, people-centric security approach allows IT to continuously identify user behaviors, determine risk profiles, and assess and address potential threats within an expanding network environment. It also requires a new approach to analytics.

Standard analytics covers basic descriptive and diagnostic insights that are often built into many traditional security products. Advanced analytics use machine learning and artificial intelligence to deliver new insights and predictions on what might happen in the future as well as a way to mitigate potential issues.

Deploying user behavior analytics for proactive security insights

A secure digital workspace provides a single conduit through which people interact with work-related apps and data. It requires a security solution capable of monitoring all interactions within the workspace and the network. This solution should apply advanced analytics to track and analyze user and entity behavior to proactively alert IT about potential issues.

It should also be capable of the following:

- Sharing intelligence across services
- Triggering contextual reactions
- Handling application and user security threats before they happen
- Uncovering application and data usage trends
- Improving application performance and supporting continuous operations
- Easy integration with an existing IT portfolio to provide complete secure digital workspaces

Gain comprehensive, actionable insights with Citrix Analytics

Citrix Analytics pulls together the entire Citrix portfolio to provide visibility into the status and context of each individual user. It offers:

- User and entity behavior-based anomaly identification
- Detection of malicious user activity
- Early detection and isolation of external attacks on applications and data infrastructure for data exfiltration
- Predictive analytics

Sense

- Turn-key data collection
- User behavior and context based

Analyze

- Correlation from multiple vantage points for accuracy
- Machine learning-based models

Respond

- Closed-loop autonomous actions
- Granular policy control

Deliver a unified, contextual, and secure digital workspace

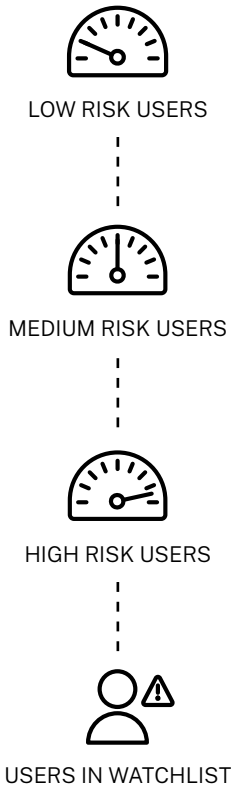
With Citrix Analytics, IT security and networking teams can protect applications, content, and networks, proactively addressing threats in today's SaaS, hybrid, and multi-cloud environments.

Because a workspace from Citrix is unified, contextual, and secure, you can take a people-centric approach to security, with centralized management and distributed policy enforcement across every control point.

- Automated aggregation and correlation of data and intelligent analytics using machine learning
- Easy access and simple onboarding of multiple Citrix offerings
- Deep insights that grow richer as more Citrix offerings are added as data sources

Citrix Analytics provides IT with complete visibility into user behavior across SaaS, hybrid and multi-cloud environments. Potential threats are addressed proactively, empowering organizations to adopt new innovations and accelerate their business growth.

Visit citrix.com/secure to learn more.



Source:
1. Citrix Synergy 2018 Presentation – “How Secure Digital Perimeter Can Help Secure Your Digital Workspace”
2. “Verizon Data Breach Investigation Report,” 2017
3. “The Need for a New IT Security Architecture,” Citrix and Ponemon Institute; 2017