Introducing Citrix uberAgent: Best-in-class EUC monitoring

Citrix's recent acquisition of **vast limits GmbH**, the German-based company behind **uberAgent**, marks a significant enhancement to the suite of Citrix observability solutions.

This strategic move not only broadens the capabilities of Citrix's existing solutions set, encompassing Citrix Director, Monitor, Probes, Analytics for Performance, and Analytics for Security, but also introduces **a new era of end-user computing (EUC) observability.**

uberAgent's capabilities aren't just limited to Citrix. You can leverage its monitoring capabilities to observe Windows AVD and W365 Cloud PCs as well.

The flexibility and openness of uberAgent is a testament to the existing data export strategy of Citrix observability solutions, as uberAgent supports Splunk Enterprise, Splunk Cloud, Elasticsearch, Kafka, Kibana, Azure Monitor, or multiple backend platforms with different granularity and insights at the same time.

This flexibility allows customers to address regulatory requirements and compliant reporting in on-premises environments, all while collecting infrastructure monitoring metrics for DevOps teams, to name some of the many use cases.

What sets Citrix uberAgent apart

Citrix uberAgent stands out by providing unmatched visibility across physical and virtual Windows server and client operating systems, as well as macOS endpoints.

This agent-based solution complements the agentless approach of Citrix Director and Citrix Analytics by extending monitoring capabilities to a wider array of endpoints and system insights, providing a deeper analysis of infrastructure and endpoints performance along with security observability capabilities.
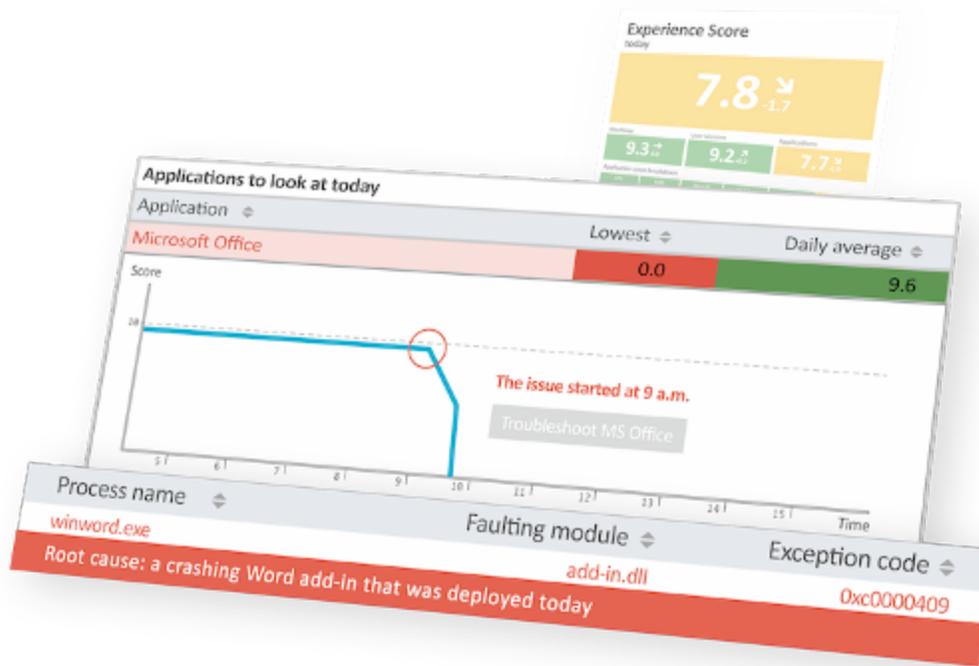
Application crash insights of installed application Microsoft Word

The single, lightweight agent monitors both security and performance while adding **less than 0.5 percent additional CPU load** to the system! Because of its lightweight agent, uberAgent offers unmatched enterprise scalability with the current **largest deployment coming in at over 250,000 active users**.

vast limits pioneered the EUC and Digital Employee Experience (DEX) monitoring domain by providing insights into installed browser performance and adoption statistics natively via API or browser extension. Equipped with these capabilities, customers can provide **Application Performance Monitoring (APM)** and security insights into **Internet Explorer, Edge, Chrome, Firefox, and the Citrix Enterprise Browser**.

Average request duration (s)

Legend:
- app.frontapp.com
- podio.com
- www.deepl.com
- youtube.com
- egnyte.com
- www.google.com
- salesforce.com
- stackoverflow.com
- adobe.com
- meet.google.com
- uberagent.com
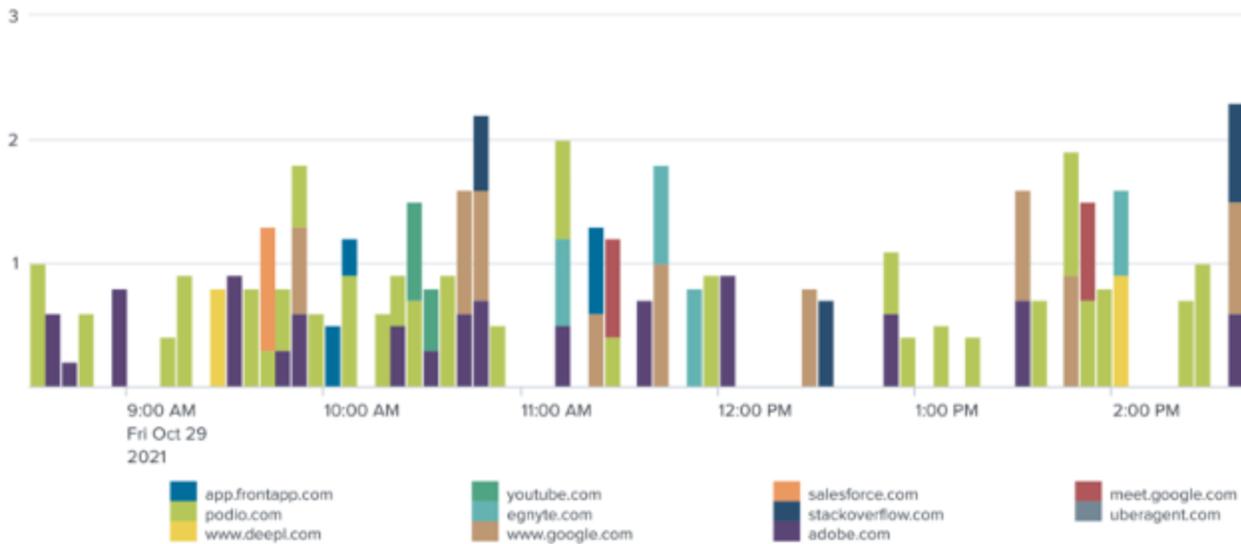
Native Browser monitoring for Edge, Chrome, Firefox and Citrix Enterprise Browser
Unlike Citrix Director, which primarily focuses on servers and clients within a Citrix deployment, uberAgent encompasses all aspects of the user experience across various platforms. This includes metrics for installed application UI rendering delay and network delay which Citrix engineers and architects require to **effectively investigate bottlenecks and application performance issues**.

Average latency over time: SAP

Legend:
- Avg. initial TCP send latency (ms)
- Avg. TCP send latency (ms)
- Avg. TCP send jitter (ms)
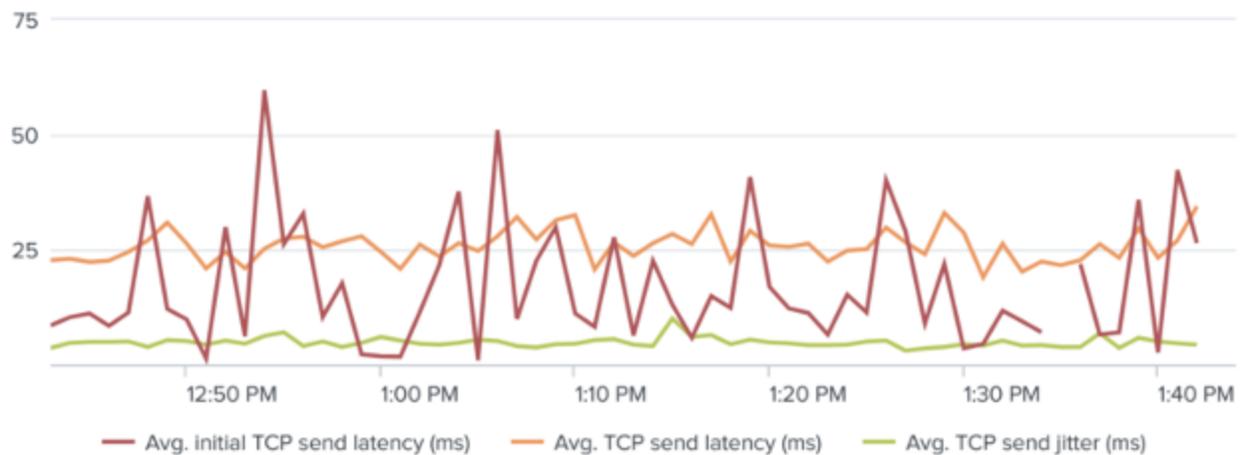
Troubleshooting slow SAP GUI: Application Performance Monitoring (APM) of network latency and jitter

While Citrix Analytics excels in detecting security and performance anomalies and providing diagnostic insights, uberAgent enhances these with detailed granularity. uberAgent has the ability to collect events and metrics once and then utilize them for both performance and security purposes. This method represents the most efficient deployment option available in the market today for customers.
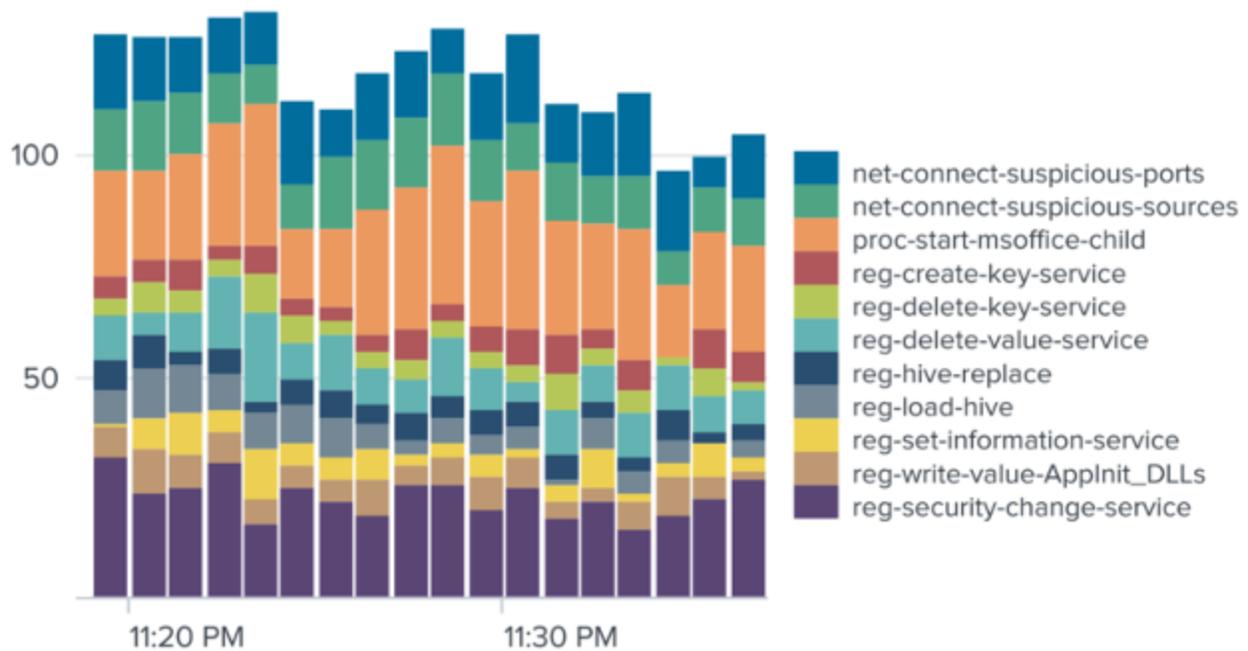
Granular and deep insights into registry and network behavior of applications

With uberAgent's revolutionary yet highly efficient threat detection engine, threat hunting and Security Operations Center teams (SOC teams) gain a new tool to **augment their existing Endpoint Detection and Response (EDR) and Extended Detection Response (XDR) solutions on both physical and virtual endpoints.** The inclusion of the **MITRE ATT&CK framework** is just one of the many features of uberAgent, offering comprehensive security coverage through a single agent.

Risk Modifiers Over Time

Risk Modifiers By Annotations

enriched_ann otations: T1047 - Windows Management Instrumentation
count: 8,966
count%: 52.847%

Risk Score By Annotations

Risk Modifiers By Threat Object

Risk Score By Object

risk_object ⇕	risk_object_type ⇕	risk_score ⇕	source_count ⇕	count ⇕
NIGHTLY1	system	3886225	1	72402
NIGHTLY2	system	695750	1	25785
NIGHTLY3	system	41825	1	1427
NIGHTLY8	system	40500	1	1382
NIGHTLY9	system	32500	1	1056
NIGHTLY4	system	19175	1	560
NIGHTLY5	system	15200	1	471

Most Active Sources

source ⇕	risk_score ⇕	risk_objects ⇕	count ⇕
uberAgent ESA - ES Risk Analysis	4731175	7	103083

Recent Risk Modifiers

risk_object ⇕	risk_object_type ⇕	threat_object ⇕	threat_object_type ⇕	source ⇕	risk_message ⇕	risk_score ⇕
NIGHTLY1	system	powershell.exe	process	uberAgent ESA - ES Risk Analysis	Tag: proc-start-suspicious-script-execution-from-temp-folder Process (ID): powershell.exe (376) Process path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Command line: powershell.exe -command "get-content 'C:\windows\TEMP\uberAgent9228.ps1' | powershell.exe -noprofile -" Parent (ID): cmd.exe (6680) Application (version): Microsoft Windows OS Lifetime (s): 0.008 Is elevated: 1 Is protected: 0 Process.Hash.MD5: BE6B845E3B7BCBB4511D221A5BFC216E Process.Hash.SHA1: 54B9D724C4C80807F6554DDCC85C112947C6A696 Process.Hash.SHA256: E8578E4D0486370C4D636841BA775A1D938B667726602AFDF4564EF9E8367570 Process.Hash.IMP: 741776AACCFC5B71FF59832DCDCACE0F	75

uberAgent ESA collected data visualized within the out-of-the-box available "Risk Analysis" dashboard in Splunk Enterprise

Integration with existing Citrix solutions

A key advantage of uberAgent is its **seamless integration and automatic detection** of existing Citrix solutions such as the Virtual Delivery Agent (VDA) or Delivery Controller. This allows IT professionals to leverage a unified backend for data collection and analysis by simply **deploying the lightweight agent on all of their IT managed clients and servers**.

The newly offered capabilities are crucial for tech teams aiming to optimize performance, enhance security, and improve user experience across the board.

Leveraging the Citrix Platform License

The introduction of uberAgent is perfectly aligned with the new Citrix Platform License, an all-in-one licensing model that grants unlimited access to Citrix's entire product suite. This unified approach simplifies the procurement process for organizations, ensuring they have all the tools needed to support a dynamic and secure IT environment without the complexity of managing multiple licenses.

The strategic importance of uberAgent

The acquisition of uberAgent by Citrix is a response to the growing demand for holistic and deeper monitoring capabilities to keep pace with the complexity of modern IT environments. uberAgent's ability to provide deep insights into endpoint performance, installed applications, and browser usage complements the Citrix vision to deliver a superior digital employee experience.

This acquisition underscores our commitment to empowering IT professionals with the tools they need, including the data sharing capability. Our new capabilities allow operations teams to consume data relevant to their task metrics in business intelligence tools, such as PowerBI, Grafana, or Tableau.

Observability simplified with uberAgent

The addition of Citrix uberAgent signifies a pivotal advancement in our observability offerings, providing tech professionals with an innovative and enterprise-grade solution. By offering detailed insights into a wide range of client and server OS endpoints and seamlessly integrating with existing Citrix solutions, uberAgent empowers IT teams to manage, monitor, and navigate the complexities of modern environments more effectively than any other vendor in the EUC space.

With the Citrix platform, organizations can now leverage this powerful tool to ensure their End-User Computing environments are not only efficient and secure but also aligned with the evolving needs of their users and business priorities.