Syteca

WHITE PAPER

Syteca User Activity Monitoring

Feature overview and deployment guide

- ✓ Get visibility into user actions
- ✓ Prevent insider threats
- ✓ Streamline IT compliance efforts
- ✓ Enhance workforce productivity

www.syteca.com

info@syteca.com

Table of contents

Introduction

The increasing prevalence of insider threats, combined with the rising costs of data breaches, has made user activity monitoring (UAM) a critical cybersecurity tool.

According to Verizon's 2024 Data Breach Investigations Report, 68% of data breaches involve a human element, with people being engaged through social engineering and compromised credentials. Given that a single employee can perform up to 10,000 operations daily, effective monitoring of user activity has never been more essential in order to safeguard IT environments.

$4.88 million

The global average cost of a data breach

$4.99 million

The global average cost of a malicious insider attack

2024 Data Breach Investigations Report by Verizon

Syteca's user activity monitoring (UAM) solution addresses insider-related challenges head-on by offering comprehensive monitoring capabilities, seamless integration, and customizable deployment.

This whitepaper describes the practical implementation of Syteca UAM, highlighting its core features, deployment options, installation steps, integrations, and value in mitigating insider threats.

The growing need for UAM solutions

User activity monitoring is critical for maintaining robust IT security. By providing real-time visibility of user actions, UAM enables organizations to identify suspicious behavior, prevent unauthorized access, and respond to potential security incidents swiftly.

> "User activity monitoring (UAM) is a progressive practice escorted by enterprises to keep complete track of activities performed by employees.
>
> The enterprises can more eagerly identify cautious behavior and diminish risks before they result in data breaches, or at least in time to minimize damages by implementing user activity monitoring."
>
> **The Global User Activity Monitoring Market Report** by Verified Market Research

Comprehensive user activity monitoring helps organizations address critical challenges, particularly those related to security, compliance, and operational efficiency. The main issues that call for UAM include:

- **Insider threats.** Unmonitored third-party and employee activity can lead to data leaks, loss of intellectual property, operational disruptions, and other incidents. UAM helps mitigate insider risks by identifying and addressing suspicious activity before it escalates.
- **Delayed incident detection.** Without effective monitoring, cyberattacks and malicious activity may go unnoticed for an extended period of time. UAM empowers you to promptly detect and mitigate harmful activity.
- **Strict cybersecurity requirements.** Different laws and regulations demand strict data security and accountability. UAM solutions like Syteca provide comprehensive audit trails, helping organizations oversee user interactions with sensitive data, demonstrate compliance, and avoid legal repercussions.
- **Remote work challenges.** Hybrid and remote work increases the risk of data exposure due to the nature of complex IT structures. UAM offers visibility across different devices and locations, ensuring 360-degree monitoring of your whole network.
- **Productivity concerns.** Tracking employee activity helps identify inefficiencies and patterns of unproductive behavior, allowing you to optimize resources and enhance overall organizational performance.
- **Poor incident investigation.** Should an incident occur, a lack of sufficient logs can hamper the process of performing thorough investigations. UAM delivers detailed records, providing insights into root causes, responsible parties, and vulnerabilities.
- **Policy violations.** UAM reveals risky behaviors and violations of security policies, enabling organizations to better enforce their information security practices.

By addressing these challenges, UAM empowers you to safeguard your IT environment, streamline operations, and achieve regulatory compliance. Continue reading to explore the features and benefits of Syteca UAM in more detail.

Get visibility into every action with Syteca UAM

Syteca UAM is a comprehensive cybersecurity solution that empowers organizations to secure and monitor privileged access and user activity across thousands of endpoints concurrently.

Why Syteca UAM?

Monitor user activity continuously and ethically

Continuously monitor all user activity, even if an endpoint's network connection is lost. Enable data pseudonymization to oversee user actions while preserving employee privacy.

Turn user actions into actionable intelligence

Analyze user activity logs to investigate your security landscape. Export tamper-proof recordings of user sessions for forensic investigations. Streamline compliance audits with a wide variety of reports.

Stop threats before they escalate

Receive alerts about unusual user activity and view suspicious sessions in real time. Mitigate threats promptly with automated incident response.

Boost workforce efficiency

Gain insights into employee performance with intuitive dashboards. View productivity metrics to spot areas for improvement and make the relevant adjustments to workflows.

With Syteca UAM, you gain 360° visibility into user activity, ensure compliance, and boost efficiency — all through one centralized platform.

Note: For enhanced security, you can leverage Syteca UAM alongside Syteca PAM, which enables you to granularly manage access, secure employee passwords, discover unmanaged privileged accounts, and verify user identities with ease. When combined, Syteca UAM + PAM makes every action visible and every interaction secure.

Recognized and certified by the best

aws Gartner Microsoft Azure NIST kuppingercole ANALYSTS

Key Syteca UAM features

Syteca UAM offers advanced features that deliver a clear view of employee, admin, and third-party activity across your IT infrastructure.

On-screen monitoring and recording. Capture clear, real-time recordings of on-screen activity. Recorded user sessions are complemented by indexed metadata for easy search and playback during audits or investigations.

Web & app monitoring. Ensure users adhere to your security policies with detailed insights into application and web usage. Restrict access to specific resources to enforce your information security policies.

Keystroke monitoring. Track every keystroke, system command, and clipboard operation to detect malicious and harmful activity. Create a detailed audit trail for forensic investigation and incident response.

File transfer oversight. Keep track of sensitive file transfers across messaging apps and web browsers to prevent data leaks.

USB device management. Take control of USB device connections across all endpoints. Monitor and block unauthorized USB devices, protecting your network from data theft or malware intrusion.

Default and custom alerts. Stay one step ahead of potential threats with real-time alerts tailored to your organization's needs. Promptly identify unusual user behavior and address risks before they escalate.

Automated incident response. Streamline how you intervene on potential security breaches with automated actions. Issue warning messages, block users, or terminate suspicious processes once they occur.

Productivity dashboards. Analyze team productivity with intuitive dashboards that provide an at-a-glance overview of working vs. idle time, app use, and browsing habits. Use these insights to optimize workflows.

Ad hoc & scheduled reports. Generate over 30 types of detailed reports on user activity. Schedule regular reports or create custom ones on demand for compliance audits and managerial review.

Targeted monitoring and search. Focus your monitoring efforts on specific users, departments, or activities. Exclude private or non-critical applications and websites from oversight to preserve user privacy. Leverage advanced search and filtering tools to quickly locate critical events.

Table of contents →

Monitored data pseudonymization

The **pseudonymizer** enhances user privacy by pseudonymizing personally identifiable information (PII) in user activity monitoring results, reports, and screenshots of user sessions.

Data pseudonymization

Usernames and device names are substituted with unique aliases. For example, a username like "john.doe" might be displayed as "USR-123".

Controlled de-pseudonymization

In case of security incidents, only authorized personnel can request to de-anonymize specific user data.

Pseudonymized mode is designed for organizations that need to comply with strict data privacy laws, such as the GDPR or CCPA. This is not a default feature and can be activated by contacting the Syteca Support Team.

Ensure compliance with HIPAA, PCI DSS, NIS2, DORA, NIST, GDPR, SWIFT, ISO 27001

Syteca is trusted by 1500+ customers worldwide

Platform highlights

Syteca is a comprehensive solution for managing and securing IT environments with a focus on efficiency, scalability, and protection.

Easy deployment

Effortlessly deploy Syteca across your organization in diverse environments. Whether on-premises, in the cloud, or in hybrid environments, Syteca is quick and efficient to set up.

Lightweight agent

Experience smooth operation without compromising system performance. Syteca's lightweight agent uses minimal resources, ensuring an optimal user experience and uninterrupted workflows.

Agent protection

Keep your system secure with advanced measures that protect agents from uninstallation and tampering.

Vast integration options

Enhance your cybersecurity infrastructure by integrating Syteca with SIEM solutions, ticketing systems, SSO frameworks, and more.

Military-grade encryption

Safeguard sensitive data, including passwords, audit logs, and network connections, with robust encryption protocols that meet the highest security standards.

Customizable toolset

Tailor Syteca to your organization's unique needs. Choose only the features relevant to your operations, and add advanced tools like privileged access management (PAM) to maintain full control over your environment.

High performance and scalability

Easily scale your operations with Syteca's load-balancing capabilities and extendable storage options. Whether managing a growing workforce or expanding your IT infrastructure, Syteca adapts to your needs.

Multi-tenancy support

Efficiently manage distributed offices, departments, or sub-units as separate entities within a shared environment. Maintain clear boundaries and separate settings for each unit while benefiting from centralized control and oversight.

System architecture

These core components form the backbone of Syteca UAM, ensuring seamless monitoring, communication, and data processing.

Core system components

Syteca UAM includes the following core system components:

Application Server	The Syteca Application Server is a key backend component that acts as the communication hub between agents and the system. It receives the monitoring data (screen capture recordings and associated metadata) from Syteca Clients, analyses the data, and generates alerts on potential security incidents. The Application Server handles all configurations, permissions, and backend operations.
Clients	Syteca Clients are software agents installed on target endpoints to record user activity. Clients can be deployed on machines with any type of desktop or server, including infrastructure servers, terminal servers, jump servers, as well as physical and virtual desktops (VDIs). Clients are lightweight, ensuring stable and uninterrupted system performance.
Management Tool	The Syteca Management Tool is a centralized administrative console with a web-based interface. It allows administrators to view and analyze the monitoring data received from Clients, as well as manage all Clients, users, alerts, databases, licenses, etc.
Session Viewer	The Management Tool includes the Session Viewer, which provides playback of user sessions. This YouTube-like player lets administrators view on-screen user activity in the form of a video accompanied by indexed and searchable metadata.
Database	The database manages and stores user activity monitoring data and is one of the main third-party components of Syteca. When you install the Syteca Application Server, you can choose between MS SQL and PostgreSQL to utilize as your database.

Table of contents →

Integration options

Syteca integrates with security information and event management (SIEM) systems, ticketing systems, and single sign-on (SSO) providers to enhance security and streamline IT operations:

SIEM systems	Ticketing systems	SSO providers
▪ Supports integration with SIEM systems using SysLog (over TCP/IP) and log formats like CEF and LEEF. ▪ Covers deployments involving Elasticsearch and Kerberos.	▪ Integrates with SysAid and ServiceNow. ▪ For other ticketing systems, Syteca offers an API Bridge.	▪ Compatible with Azure, ForgeRock, and Okta single sign-on authentication systems.

Platform support

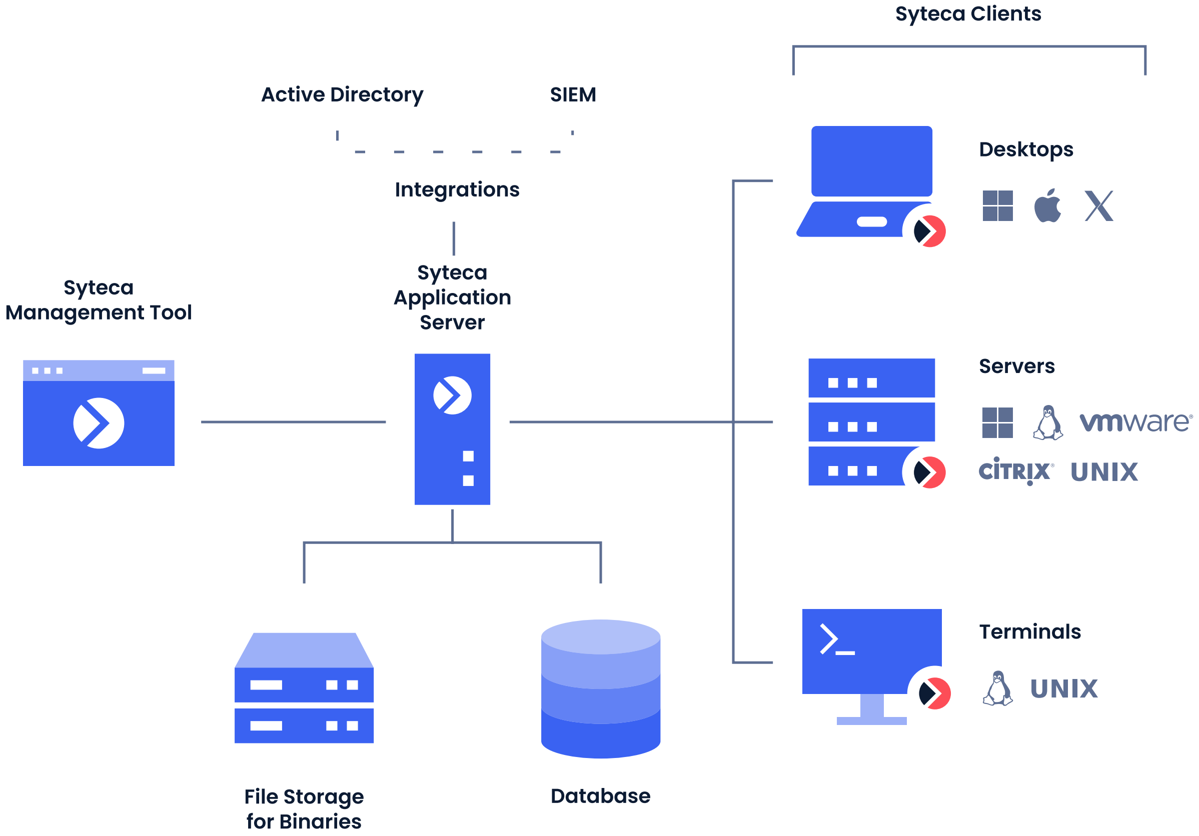
Syteca UAM provides extensive platform compatibility to ensure seamless monitoring across diverse environments.

Desktops and servers	Operating systems	Virtual environments
▪ Infrastructure servers ▪ Terminal servers ▪ Jump servers ▪ Physical and virtual desktops	▪ Windows ▪ Linux ▪ macOS ▪ UNIX ▪ X Window System ▪ Citrix ▪ Wayland	▪ VMware Horizon ▪ Microsoft Hyper-V ▪ Citrix ▪ Amazon WorkSpaces ▪ AWS (Amazon Web Services) ▪ Azure Windows Virtual Desktops

Whether you operate on desktops, servers, operating systems, or virtual environments, Syteca UAM has you covered.

Table of contents →

Deployment scheme



How Syteca UAM operates

The user activity monitoring process involves capturing, transmitting, storing, and analyzing user activity data. Here's a step-by-step explanation of how Syteca handles each of these stages:

1. Capturing user activity

Syteca continuously records user activity on endpoint computers across various operating systems. The primary data that is captured includes:

- **Videos in screen capture format** — periodic recordings of the user's screen, which can be configured to capture the entire screen or only the active window. The frequency and color depth of screen capture recordings can be customized to balance image detail and your storage requirements
- **Metadata** — additional information such as active window titles, URLs, application names, keystrokes, clipboard operations, and commands (entered in Linux terminals).

2. Transmitting data

The captured data is securely transmitted from the Client computers to the Syteca Application Server. If the connection to the server is unavailable, the Client can cache the data locally and transmit it once the connection is restored. This ensures no loss of monitoring data during network interruptions.

3. Storing data

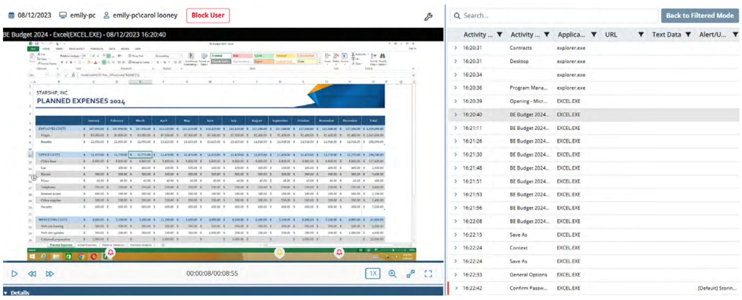
Upon reaching the Application Server, the data is stored in a centralized database. Syteca employs robust encryption mechanisms to protect data both in transit and at rest:

- All communications between Syteca Clients and the Application Server are encrypted using AES 256.
- Access to the Syteca Management Tool is established over an encrypted HTTPS connection, utilizing SSL/TLS protocols.

4. Analyzing data

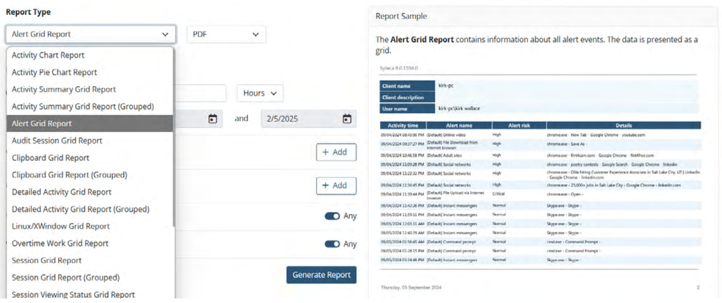
Syteca provides various tools for analyzing user activity data:

- **Session playback.** Administrators can view recorded sessions and replay certain user actions to investigate incidents or monitor for compliance. The Session Viewer allows for a detailed examination of user actions, including screen activity and associated metadata.



Activity ...	Activity ...	Applica...	URL	Text Data	Alert/U...
16:20:31	Contracts	explorer.exe			
16:20:31	Desktop	explorer.exe			
16:20:34		explorer.exe			
16:20:36	Program Mana...	explorer.exe			
16:20:39	Opening - Micr...	EXCEL.EXE			
16:20:40	BE Budget 2024...	EXCEL.EXE			
16:21:11	BE Budget 2024...	EXCEL.EXE			
16:21:26	BE Budget 2024...	EXCEL.EXE			
16:21:30	BE Budget 2024...	EXCEL.EXE			
16:21:48	BE Budget 2024...	EXCEL.EXE			
16:21:51	BE Budget 2024...	EXCEL.EXE			
16:21:53	BE Budget 2024...	EXCEL.EXE			
16:21:56	BE Budget 2024...	EXCEL.EXE			
16:22:08	BE Budget 2024...	EXCEL.EXE			
16:22:15	Save As	EXCEL.EXE			
16:22:24	Context	EXCEL.EXE			
16:22:24	Save As	EXCEL.EXE			
16:22:33	General Options	EXCEL.EXE			
16:22:42	Confirm Passw...	EXCEL.EXE			[Default] Storin...

- **Reports.** Syteca offers [a variety of reports]() that offer insights into user behavior, application usage, file operations, and more. These reports can be customized and exported for further analysis or auditing purposes.


Report Type
Alert Grid Report
PDF
Activity Chart Report
Activity Pie Chart Report
Activity Summary Grid Report
Activity Summary Grid Report (Grouped)
Alert Grid Report
Audit Session Grid Report
Clipboard Grid Report
Clipboard Grid Report (Grouped)
Detailed Activity Grid Report
Detailed Activity Grid Report (Grouped)
Linux/XWindow Grid Report
Overtime Work Grid Report
Session Grid Report
Session Grid Report (Grouped)
Session Viewing Status Grid Report
Hours
and
2/5/2025
+ Add
+ Add
Any
Any
Generate Report
Report Sample

The **Alert Grid Report** contains information about all alert events. The data is presented as a grid.

Syteca 8.0.1594.0

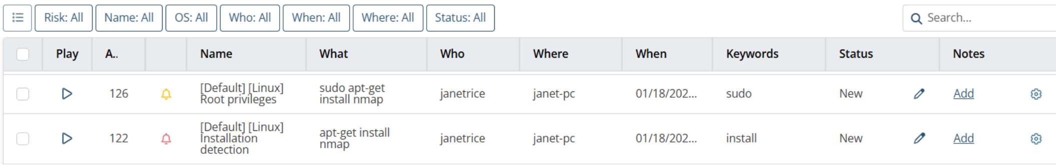
Client name	kirk-pc
Client description	
User name	kirk-pc\kirk wallace

Activity time	Alert name	Alert risk	Details
09/04/2024 08:43:00 PM	[Default] Online video	High	chrome.exe - New Tab - Google Chrome - youtube.com
09/04/2024 09:37:27 PM	[Default] File Download from Internet browser	High	chrome.exe - Save As -
09/04/2024 10:46:58 PM	[Default] Adult sites	High	chrome.exe - flirt4cam.com - Google Chrome - flirt4free.com
09/04/2024 11:09:28 PM	[Default] Social networks	High	chrome.exe - poetry contests - Google Search - Google Chrome - linkedin
09/04/2024 11:22:32 PM	[Default] Social networks	High	chrome.exe - Ollie hiring Customer Experience Associate in Salt Lake City, UT | LinkedIn - Google Chrome - linkedin.com
09/04/2024 11:36:45 PM	[Default] Social networks	High	chrome.exe - 25,000+ jobs in Salt Lake City - Google Chrome - linkedin.com
09/04/2024 11:39:44 PM	[Default] File Upload via Internet browser	Critical	chrome.exe - Open -
09/04/2024 11:42:26 PM	[Default] Instant messengers	Normal	Skype.exe - Skype -
09/04/2024 11:59:11 PM	[Default] Instant messengers	Normal	Skype.exe - Skype -
09/05/2024 12:03:11 AM	[Default] Instant messengers	Normal	Skype.exe - Skype -
09/05/2024 12:40:29 AM	[Default] Instant messengers	Normal	Skype.exe - Skype -
09/05/2024 01:56:45 AM	[Default] Command prompt	Normal	cmd.exe - Command Prompt -
09/05/2024 01:28:15 PM	[Default] Command prompt	Normal	cmd.exe - Command Prompt -
09/05/2024 03:24:48 PM	[Default] Instant messengers	Normal	Skype.exe - Skype -

Thursday, 05 September 2024 2

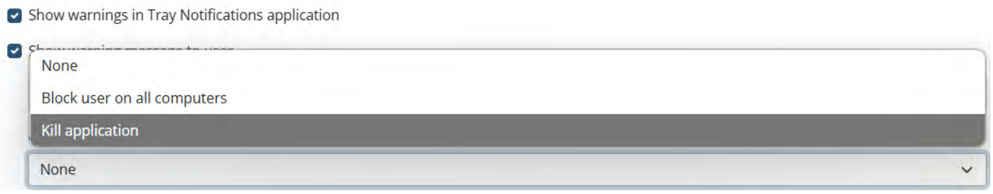
5. Responding to incidents

- **Alerts.** The platform enables administrators to configure real-time alerts and get notifications of suspicious activities.



□	Play	A..		Name	What	Who	Where	When	Keywords	Status		Notes	
□	▷	126	🔔	[Default] [Linux] Root privileges	sudo apt-get install nmap	janetrice	janet-pc	01/18/202...	sudo	New	✎	Add	⚙
□	▷	122	🔔	[Default] [Linux] Installation detection	apt-get install nmap	janetrice	janet-pc	01/18/202...	install	New	✎	Add	⚙

- **Manual incident response.** Syteca allows security personnel to change the status of alert events and add notes for documentation and follow-up.
- **Automated incident response.** The system can be configured to automatically show warnings to users who violate security policies, kill suspicious applications, and block users on all computers.


☑ Show warnings in Tray Notifications application

☑

Implementation guide

The following section outlines the essential steps for administrators to efficiently onboard users and configure the system for optimal performance.

Installation checklist

Installing Syteca involves setting up the Application Server, Management Tool, and Clients on target endpoints. The steps for installation are as follows:

- ✓ Install the Application Server on a designated machine by running the installation file (Syteca_Server.exe).
- ✓ Install the Management Tool on the necessary computers with Internet Information Services (IIS) enabled.
- ✓ Purchase a suitable product license and activate the serial key.
- ✓ Set up the network environment on computers where Clients will be installed.
- ✓ Install Clients on endpoints to monitor user activities. The installation method varies based on the operating system and deployment type:

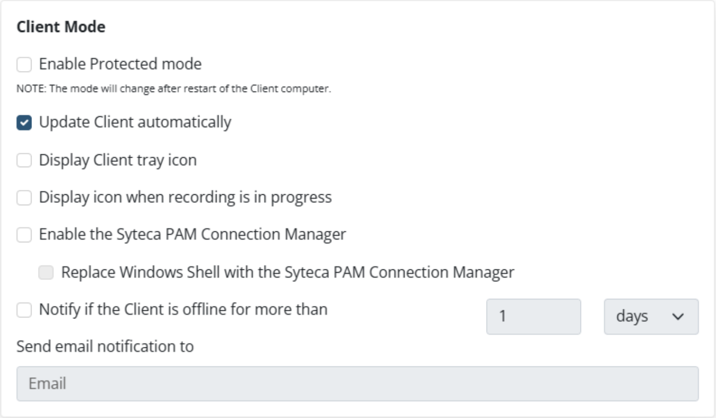
Endpoint OS	Remote installation	Local installation
Windows	Supported	Supported via an installation package
macOS	Supported via Jamf Pro or VMware Workspace ONE UEM	Supported via command line
Linux	Not supported	Supported via command line

Note: in SaaS deployments, Windows Clients can only be installed locally.

Configuring client monitoring settings

After installation, you can configure monitoring settings to tailor Syteca UAM to your specific organizational needs.

Administrators can add a descriptive note for each Client, enable Protected Mode to prevent users from interfering with monitoring, set up automatic Client updates, and more.



Client Mode

□ Enable Protected mode

NOTE: The mode will change after restart of the Client computer.

☑ Update Client automatically

□ Display Client tray icon

□ Display icon when recording is in progress

□ Enable the Syteca PAM Connection Manager

□ Replace Windows Shell with the Syteca PAM Connection Manager

□ Notify if the Client is offline for more than 1 days

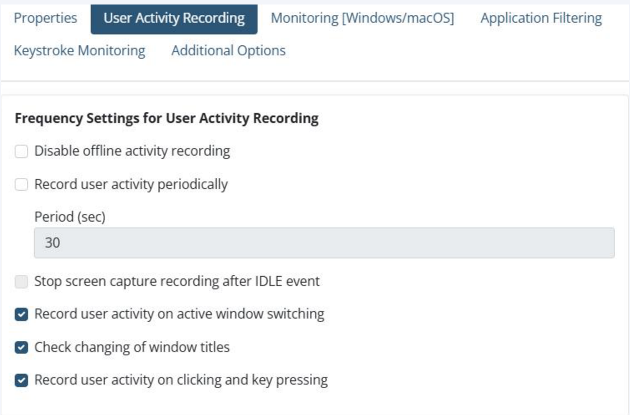
Send email notification to

Email

User activity recording

Configurable categories of user activity recording include:

Frequency settings. Define triggers for recording user activity, such as window changes, keystrokes, or time intervals, allowing tailored monitoring strategies.



Frequency Settings for User Activity Recording

☐ Disable offline activity recording

☐ Record user activity periodically

Period (sec)

30

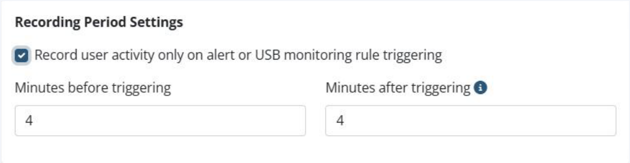
☐ Stop screen capture recording after IDLE event

☑ Record user activity on active window switching

☑ Check changing of window titles

☑ Record user activity on clicking and key pressing

Recording period settings. You can also specify the duration and timing for recording activities. For example, you can set the system to record user activity only when alert rules are triggered, specifying for how long the system should record before and after each alert event.



Recording Period Settings

☑ Record user activity only on alert or USB monitoring rule triggering

Minutes before triggering: 4

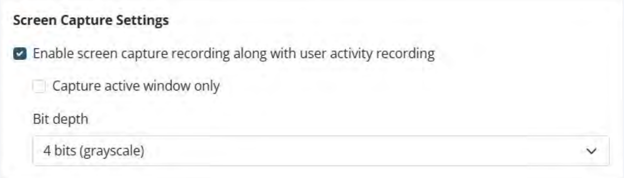
Minutes after triggering: 4

Screen capture recording settings. For the most comprehensive view of user activities, you can enable the screen capture recording option by selecting the "Enable screen capture recording along with user activity recording" checkbox.

Note: If this option is not selected, only metadata (e.g., active window title, URL, keystroke data) will be recorded.

Select **Capture active window only** option to limit screen capture recordings to the currently active window instead of the entire screen, enhancing privacy and focusing only on relevant activity.

Bit depth can also be customized, allowing you to balance image quality with your storage requirements. You can choose from 4 bits, 8 bits, and 24 bits.



Screen Capture Settings

☑ Enable screen capture recording along with user activity recording

☐ Capture active window only

Bit depth

4 bits (grayscale)

Monitoring settings

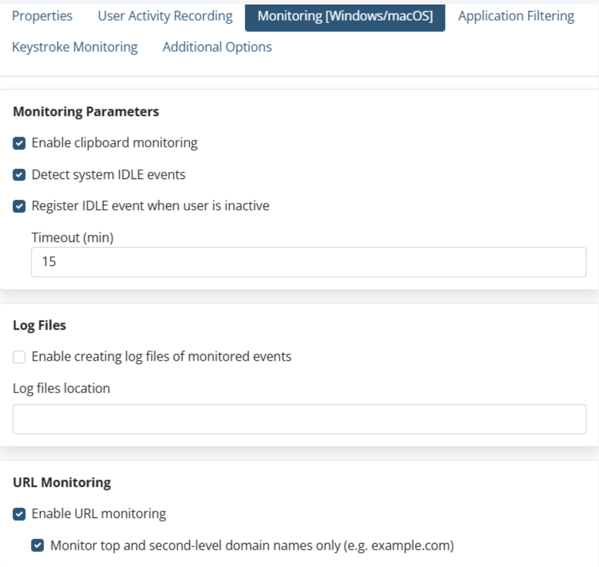
On the **Monitoring [Windows/macOS]** tab, you can further customize the user activity tracking options:

Clipboard monitoring. Enable the monitoring of clipboard activity to capture copy-paste actions that may involve sensitive data.

Detect system idle event. Register idle events when user inactivity exceeds a specified duration to identify periods of non-use.

Enable creating log files of monitored events. Switch on this feature to receive local log files of monitored events for detailed analysis.

URL monitoring. Capture information about URLs visited by the user to support web activity oversight efforts.



Monitoring Parameters

☑ Enable clipboard monitoring

☑ Detect system IDLE events

☑ Register IDLE event when user is inactive

Timeout (min): 15

Log Files

□ Enable creating log files of monitored events

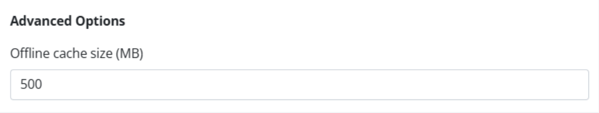
Log files location:

URL Monitoring

☑ Enable URL monitoring

☑ Monitor top and second-level domain names only (e.g. example.com)

Offline cache size. You can also define the storage capacity for data collected while the Client is offline, ensuring data is retained until it can be uploaded.



Advanced Options

Offline cache size (MB): 500

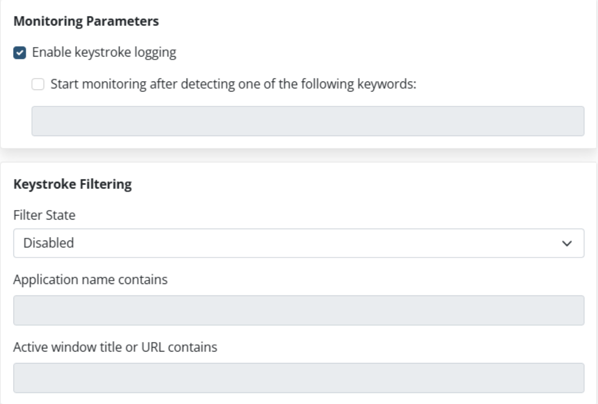
Keystroke monitoring

If your local privacy rules allow for keystroke monitoring, you can turn to our support center to switch on this feature and set up the following **keystroke monitoring parameters:**

Enable keystroke logging. Activate keylogging and capture textual input for security monitoring.

Start monitoring after detecting specific keywords. Initiate monitoring upon detection of predefined keywords to focus your attention on potentially sensitive activity.

Keystroke filtering. You can include or exclude specific applications and/or URLs from keystroke logging for more targeted monitoring.



Monitoring Parameters

☑ Enable keystroke logging

□ Start monitoring after detecting one of the following keywords:

Keystroke Filtering

Filter State: Disabled

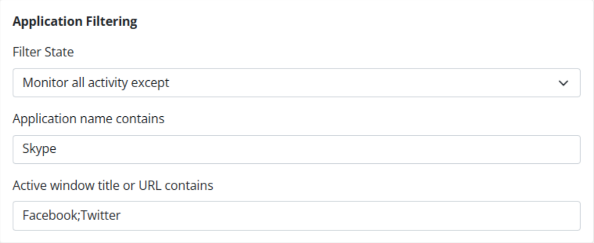
Application name contains:

Active window title or URL contains:

Filtering parameters

Syteca empowers you to concentrate on what truly matters with advanced **filtering options.**

Application filtering. Set parameters to include or exclude specific applications from monitoring.



Application Filtering

Filter State

Monitor all activity except

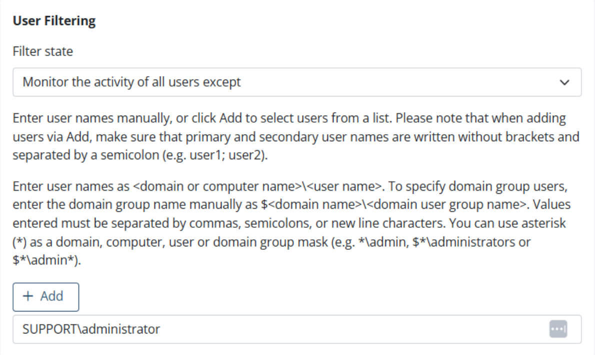
Application name contains

Skype

Active window title or URL contains

Facebook;Twitter

User filtering. Determine which user accounts are subject to monitoring.



User Filtering

Filter state

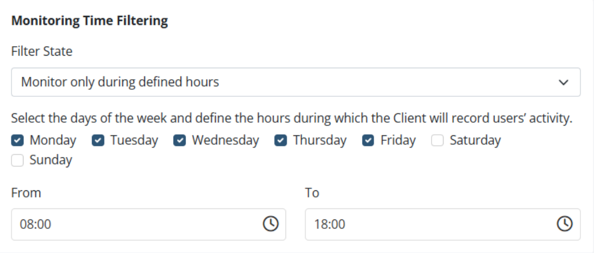
Monitor the activity of all users except

Enter user names manually, or click Add to select users from a list. Please note that when adding users via Add, make sure that primary and secondary user names are written without brackets and separated by a semicolon (e.g. user1; user2).

Enter user names as <domain or computer name>\<user name>. To specify domain group users, enter the domain group name manually as $<domain name>\<domain user group name>. Values entered must be separated by commas, semicolons, or new line characters. You can use asterisk (*) as a domain, computer, user or domain group mask (e.g. *\admin, $*\administrators or $*\admin*).

SUPPORT\administrator

Monitoring time filtering. Schedule monitoring only during specified times to align with working hours or other organizational schedules.



Monitoring Time Filtering

Filter State

Monitor only during defined hours

Select the days of the week and define the hours during which the Client will record users' activity.

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday
□ Sunday

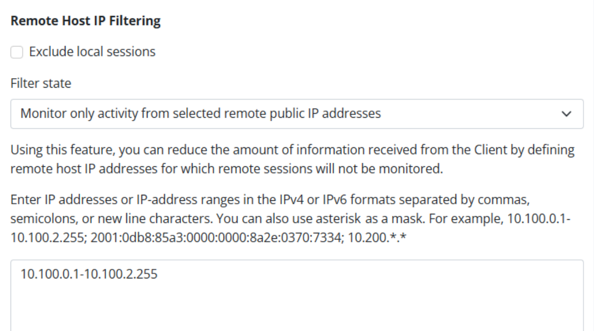
From

08:00

To

18:00

Remote host IP filtering. Set this parameter to filter monitoring based on remote host IP addresses.



Remote Host IP Filtering

□ Exclude local sessions

Filter state

Monitor only activity from selected remote public IP addresses

Using this feature, you can reduce the amount of information received from the Client by defining remote host IP addresses for which remote sessions will not be monitored.

Enter IP addresses or IP-address ranges in the IPv4 or IPv6 formats separated by commas, semicolons, or new line characters. You can also use asterisk as a mask. For example, 10.100.0.1-10.100.2.255; 2001:0db8:85a3:0000:0000:8a2e:0370:7334; 10.200.*.*

10.100.0.1-10.100.2.255

Additional options

After tailoring your monitoring scope, Syteca enables you to ensure secure and controlled access for users.

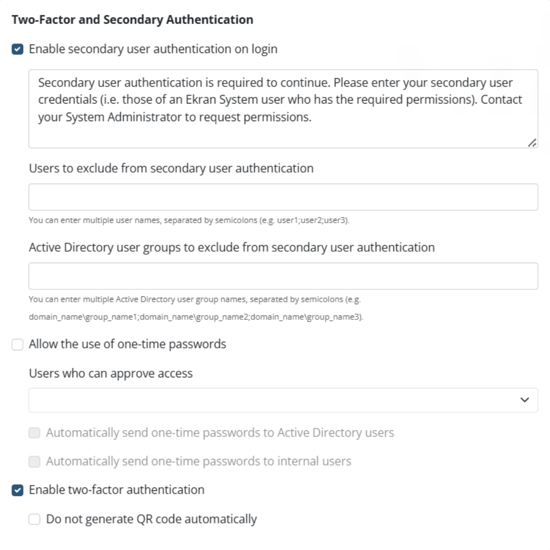
Authentication settings include:

Additional message upon login. Display a custom message to users upon login, which can include policy reminders or consent notices.

Secondary user authentication on login. Ask for additional authentication for users logging into the Client computer.

One-time passwords. Enable one-time passwords for user login, providing an extra layer of security.

Two-factor authentication. Enforce two-factor authentication for user logins, requiring a time-based one-time password.



Two-Factor and Secondary Authentication

☑ Enable secondary user authentication on login

Secondary user authentication is required to continue. Please enter your secondary user credentials (i.e. those of an Ekran System user who has the required permissions). Contact your System Administrator to request permissions.

Users to exclude from secondary user authentication

You can enter multiple user names, separated by semicolons (e.g. user1;user2;user3).

Active Directory user groups to exclude from secondary user authentication

You can enter multiple Active Directory user group names, separated by semicolons (e.g. domain_name\group_name1;domain_name\group_name2;domain_name\group_name3).

☐ Allow the use of one-time passwords

Users who can approve access

☐ Automatically send one-time passwords to Active Directory users

☐ Automatically send one-time passwords to internal users

☑ Enable two-factor authentication

☐ Do not generate QR code automatically

Additional client configuration options also include settings to minimize the impact of monitoring on network bandwidth, ensuring efficient data transmission.

Configuring the system

System configuration involves setting up notifications, domain integrations, and other system-wide settings. The available options differ based on the administrative role and deployment mode:

Single-tenant mode

Administrators can configure system-wide settings, including notification parameters, domain settings, and integrations with external systems.

Multi-tenant mode

Tenant administrators have access to settings within their assigned tenant scope. They can configure notifications, manage domain-specific settings, set up integrations pertinent to their tenant environment, and more.

For notifications, administrators can define alert messages using variables such as #name (alert name), #user (user name), #pc (endpoint name), #priority (alert priority), and #OS (endpoint operating system). This allows for dynamic and informative alerts tailored to specific events.

Adding users and defining permissions

Administrators can manage user accounts and assign permissions to control access within the system. This includes creating new user accounts, assigning roles, and defining specific permissions to ensure appropriate access levels are maintained. User management is conducted through the Management Tool's user administration section.

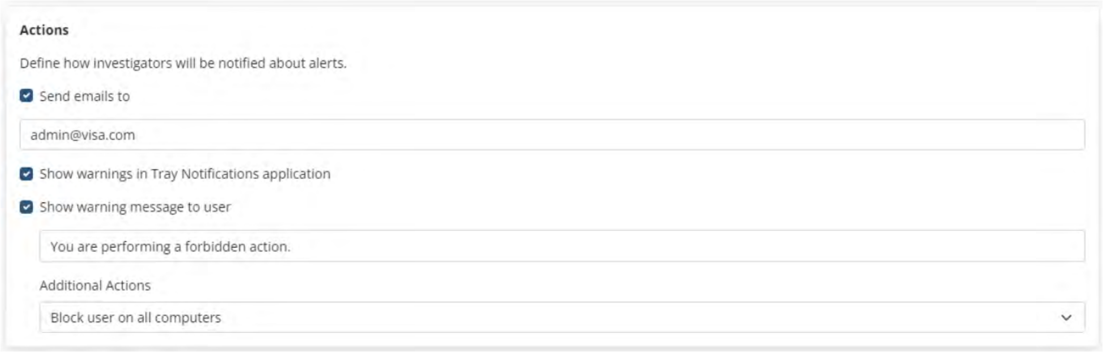
To add users in Syteca, navigate to **Users** via the left sidebar menu. Select **Add User** on the User Management page, and input the following details:

- Select the user type — **Internal User, Active Directory User/User Group**, or **Application Account**.
- **Enter user details** — a unique login name, password, and optional information.
- **Assign user groups** — specify the groups the user will belong to (all users are automatically added to the default "All Users" group).
- **Set administrative permissions** — grant the necessary administrative permissions or client permissions to the user.

Adding alerts

Administrators can configure alerts to receive notifications of specific events or policy violations. To add an alert, open the Management Tool, navigate to **Alerts**, and click **Add**. Then, name the alert, assign a risk level, define rules, and assign clients/groups applicable to this alert.

Configure automatic incident actions for the alert.



Actions

Define how investigators will be notified about alerts.

☑ Send emails to

admin@visa.com

☑ Show warnings in Tray Notifications application

☑ Show warning message to user

You are performing a forbidden action.

Additional Actions

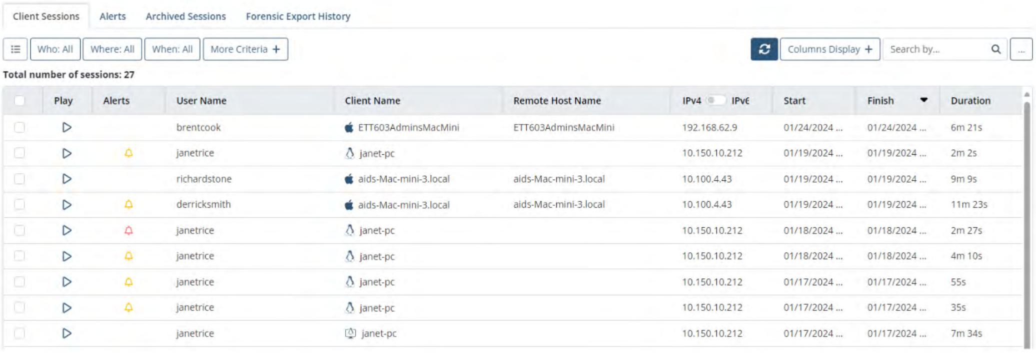
Block user on all computers

Note: Syteca offers default alerts that are triggered when users perform different types of potentially harmful actions. These alerts are enabled by default in the Management Tool but are not assigned to any Clients. For more info about default alerts, refer to the manual.

Viewing user activity data

Syteca UAM provides comprehensive tools for reviewing recorded user activity:

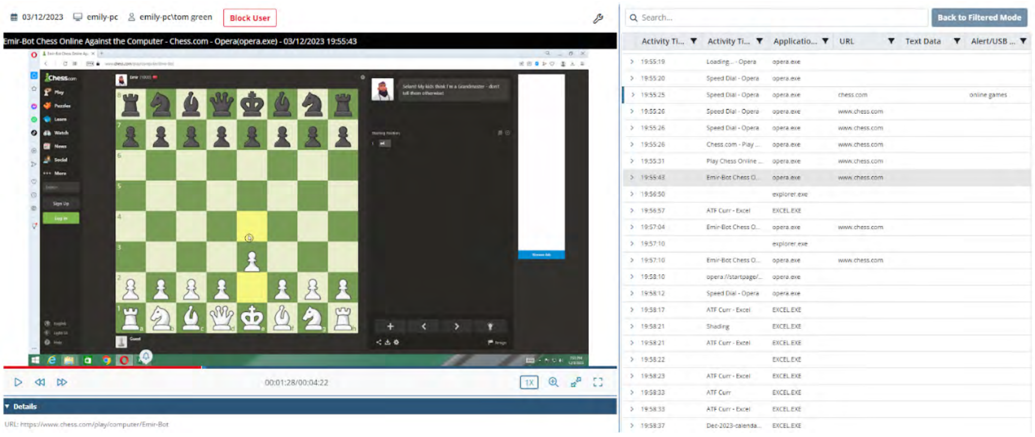
- **Client session list.** A searchable and filterable list of recorded sessions allows administrators to locate specific user activities.



Total number of sessions: 27

	Play	Alerts	User Name	Client Name	Remote Host Name	IPv4 IPv6	Start	Finish	Duration
□	▷		brentcook	ETT603AdminsMacMini	ETT603AdminsMacMini	192.168.62.9	01/24/2024 ...	01/24/2024 ...	6m 21s
□	▷	🔔	janetrice	janet-pc		10.150.10.212	01/19/2024 ...	01/19/2024 ...	2m 2s
□	▷		richardstone	aids-Mac-mini-3.local	aids-Mac-mini-3.local	10.100.4.43	01/19/2024 ...	01/19/2024 ...	9m 9s
□	▷	🔔	derricksmith	aids-Mac-mini-3.local	aids-Mac-mini-3.local	10.100.4.43	01/19/2024 ...	01/19/2024 ...	11m 23s
□	▷	🔔	janetrice	janet-pc		10.150.10.212	01/18/2024 ...	01/18/2024 ...	2m 27s
□	▷	🔔	janetrice	janet-pc		10.150.10.212	01/18/2024 ...	01/18/2024 ...	4m 10s
□	▷	🔔	janetrice	janet-pc		10.150.10.212	01/17/2024 ...	01/17/2024 ...	55s
□	▷	🔔	janetrice	janet-pc		10.150.10.212	01/17/2024 ...	01/17/2024 ...	35s
□	▷		janetrice	janet-pc		10.150.10.212	01/17/2024 ...	01/17/2024 ...	7m 34s

- **Session Viewer.** The viewer enables detailed playback of user sessions, including screen capture recordings and associated metadata.



Emir-Bot Chess Online Against the Computer - Chess.com - Opera(opera.exe) - 03/12/2023 19:55:43

00:01:28/00:04:22

URL: https://www.chess.com/play/computer/Emir-Bot

Activity Ti...	Activity Ti...	Applicatio...	URL	Text Data	Alert/USB ...
19:55:19	Loading... - Opera	opera.exe			
19:55:20	Speed Dial - Opera	opera.exe			
19:55:25	Speed Dial - Opera	opera.exe	chess.com		online games
19:55:26	Speed Dial - Opera	opera.exe	www.chess.com		
19:55:26	Speed Dial - Opera	opera.exe	www.chess.com		
19:55:26	Chess.com - Play ...	opera.exe	www.chess.com		
19:55:31	Play Chess Online ...	opera.exe	www.chess.com		
19:55:43	Emir-Bot Chess O...	opera.exe	www.chess.com		
19:56:50		explorer.exe			
19:56:57	ATF Curr - Excel	EXCEL.EXE			
19:57:04	Emir-Bot Chess O...	opera.exe	www.chess.com		
19:57:10		explorer.exe			
19:57:10	Emir-Bot Chess O...	opera.exe	www.chess.com		
19:58:10	opera://startpage/...	opera.exe			
19:58:12	Speed Dial - Opera	opera.exe			
19:58:17	ATF Curr - Excel	EXCEL.EXE			
19:58:21	Shading	EXCEL.EXE			
19:58:21	ATF Curr - Excel	EXCEL.EXE			
19:58:22		EXCEL.EXE			
19:58:23	ATF Curr - Excel	EXCEL.EXE			
19:58:33	ATF Curr	EXCEL.EXE			
19:58:33	ATF Curr - Excel	EXCEL.EXE			
19:58:37	Dec-2023-calenda...	EXCEL.EXE			

- **Metadata grid.** Along with screen captures, you can view the associated metadata — activity time, activity title, application name, URL, text data (for keystrokes and clipboard operations), and alert/USB rules.

Additionally, you can view session risk scores, alert events, archived sessions, and file upload operations.

Syteca UAM also allows you to export a Client session or multiple sessions for further investigations in either CSV file format or .efe file format that can be played back with the **Syteca Forensic Player.**

OTP Bank Analyzes User Behavior with Syteca

Maman Group Enhances Visibility into Activity of Employees, Vendors, and Subcontractors with Syteca

Super-Pharm Monitors Its Extensive Network and Controls Third-Party Activity with Syteca

Conclusion

With cyber threats escalating and regulatory requirements tightening, organizations face the urgent challenge of protecting their IT environments while maintaining operational efficiency. UAM has become a critical solution to bridge this gap, offering unparalleled visibility into user activity and potential vulnerabilities.

Syteca UAM empowers organizations to secure their networks, comply with local cybersecurity regulations, and optimize productivity with actionable insights and comprehensive real-time monitoring.

Designed for ease of deployment, Syteca UAM seamlessly integrates into diverse IT environments, allowing organizations to achieve full visibility and control over user activity without interfering with internal workflows or compromising user privacy.

Try Syteca UAM — where every action matters, shaping a safer, more efficient, and more compliant IT environment.

Book a Demo

Visit: **www.syteca.com**

or email us at: **info@syteca.com**

Syteca

About Syteca:

Syteca, Inc. is a cybersecurity software vendor headquartered in Needham, Massachusetts. Since 2013, Syteca has been providing organizations with advanced UAM and PAM solutions, helping them minimize insider risk, mitigate data security threats, and achieve regulatory compliance. Trusted by over 1,500 customers worldwide, Syteca is recognized by Gartner, KuppingerCole, and NIST.