

## Case Study

# Max Stock Enforces Security Policies And Meets Compliance Requirements With Syteca

## Challenge

Max Stock Ltd. has a complex on-premises infrastructure with multiple terminal servers to support its retail operations. With many employees and third-party vendors constantly accessing critical systems, the company faced increasing challenges in securing its sensitive assets.

They couldn't see what users were doing on endpoints, nor could they detect or respond to policy violations in real time. Lack of clarity during investigations of suspicious user activity made it difficult to assign responsibility.

Max Stock needed a security solution capable of delivering granular access controls, visibility, and real-time threat detection across all servers in order to:

- Ensure users adhere to policies
- Protect IT systems against unauthorized access
- Prevent insider threats
- Eliminate compliance gaps

## Solutions

Max Stock contacted one of Syteca's partners to explore several solutions to secure its infrastructure. However, most solutions fell short in delivering the depth of session recording and seamless integration across multi-server environments and cashier systems that the customer demanded.



"We required granular privilege control combined with real-time threat detection — across non-standard terminal servers and on-premise systems."

Chen Goldfarb, CIO at Max Stock

## Customer profile



**Max Stock Ltd.** is the largest Israeli retail chain selling non-food consumer goods. It has approximately 2,500 employees and operates 65 branches all over Israel. Max Stock offers affordable everyday essentials, including household items, toys, school supplies, and apparel.

### Pending issue:

Lack of visibility and control over the activity of privileged users and third-party vendors within the company's IT perimeter

Eventually, Max Stock chose Syteca because it offers "the best balance of functionality, ease of deployment, regulatory compliance support, and cost efficiency."

Syteca was deployed seamlessly across 25 servers, two jump servers, and more than 400 cashier registers. The entire rollout was completed within a month.

Providing 360-degree visibility, robust access controls, and compliance support, Syteca delivered immediate value across Max Stock's operations.



## Ensuring complete visibility at corporate endpoints

To secure its operations and reduce insider risks, Max Stock needed complete visibility into how users interacted with its systems and data. With Syteca User Activity Monitoring (UAM), the company gained detailed insight into employee and vendor sessions across all endpoints.

Every session is now continuously recorded, capturing screen activity, applications used, websites visited, and devices connected. This allows Max Stock's security team to monitor user actions in real time and review audit trails later during investigations.

It's also essential for Max Stock to make sure workstations are used only for business tasks. Syteca helps enforce this policy by showing users a warning message if they try to open unauthorized websites or apps.

Additionally, Syteca helps detect and respond to policy violations. If someone tries to use a prohibited tool or app, the security team receives an alert and can act immediately.

**Within just 3 months after deployment, Syteca has already alerted Max Stock's security team of two cases of negligent behavior: a third-party support specialist who accessed their personal Gmail account and an employee who was running WhatsApp on a company server. Identifying these cases enabled Max Stock to provide feedback to vendors and employees, helping prevent future violations and minimize security risks.**



## Enforcing access control policies

Max Stock required strict access control across its IT infrastructure, where privileged users, internal IT administrators, and third-party vendors frequently access sensitive systems. Syteca Privileged Access Management (PAM) gave them granular control over who can access what by configuring permissions for each user and vendor.

With Syteca PAM, Max Stock can now manage access to its endpoints through access approval workflows, time-based access restrictions, and one-time passwords. Syteca also offers two-factor authentication (2FA), which allows Max Stock to verify the identities of all users attempting to access its systems.

To top it off, Syteca's UAM capabilities help Max Stock review cases when employees or third-party vendors access assets they don't typically require for their job. Max Stock's CIO says, "Now I can see if some users open files or folders that they shouldn't open on the server, even if they have privileged access permissions." It enables the company to detect potential privilege escalation or abuse and take corrective actions to protect sensitive data.



## Supporting compliance efforts

Maintaining compliance with frameworks like PCI DSS, ISO/IEC 27001, and data privacy regulations is crucial for Max Stock. Syteca helped them meet these requirements by automating access control workflows and providing visibility into day-to-day operations for quality audits of user activity.

Syteca further simplifies compliance by offering over 30 types of user activity reports, all exportable for review. In addition, Syteca enables the Max Stock IT security team to export entire user sessions in a tamper-proof format, providing evidence for forensic investigations or external audits.



“Syteca ensures that my organization meets all regulatory requirements while fully implementing information security policies in a continuous and controlled manner.”

**Chen Goldfarb, CIO at Max Stock**

## Results

Deploying Syteca enabled Max Stock to achieve the following outcomes:



### Enhanced security

By managing access rights and monitoring user sessions, Max Stock can ensure that internal teams and third-party providers operate within defined boundaries, improving overall security.



### Fast threat detection and response

With real-time alerts and automated response activities, the Max Stock security team can quickly identify unauthorized actions and take immediate action to mitigate risk.



### Compliance readiness

Syteca's feature set helped Max Stock align with key regulatory requirements, including PCI DSS and ISO/IEC 27001. A variety of reports and audit-friendly session logs have simplified compliance and reduced the manual workload during audits.

Within just three months, Syteca helped Max Stock create a more secure and compliant environment within their endpoints. Max Stock's CIO has enthusiastically expressed his satisfaction with the platform and has even advised colleagues to consider deploying it in their organization.

Here's what he says about their journey with Syteca:



"Outstanding experience — Syteca cybersecurity solution works as promised, support is excellent, and the improvements to our security operations have been very significant."

**Chen Goldfarb, CIO at Max Stock**

## Want to see Syteca in action?

Request a demo at

[www.syteca.com](https://www.syteca.com)

