

Protecting the data of one of the largest retailers in Russia



Magnit blocks emerging security threats while boosting insight, control and workplace flexibility with an easy-to-manage privileged access management (PAM) solution.

Customer:

Magnit

Industry:

Food Retail

Country:

Russian Federation

Website:

www.magnit.com

Challenge

With 1.37 trillion rubles in sales in FY 2019, Magnit must protect sensitive corporate data from hackers who aim to breach systems by gaining access to privileged user accounts.

Solution

- One Identity Safeguard



Boosts security in just days.



Increases insight into privileged users' access.



Improves threat detection and mitigation response.



Saves time with flexible, easy-to-use tools.



Facilitates remote access.



Gains voice in feature development.

“We significantly **improved the level of security** and insight into who accesses our infrastructure with our One Identity Safeguard privileged access management solution, even though the number of remote-access sessions **increased by leaps and bounds.**”

Alexander Vasilenko,
Director of Infrastructure and
Information Security Department,
Magnit

Retailers manage significant numbers of financial transactions, which makes them an attractive target for criminals. Using malware and other tactics, hackers often breach systems by gaining access to the accounts of privileged users, such as IT administrators and financial workers. Once they have access, hackers can steal bank account and credit card numbers — and other sensitive data — without detection for months or longer.

To proactively protect its data against such attacks, Magnit, Russia’s second-largest retailer, needed a privileged access management (PAM) solution. In addition to managing information about the 1.37 trillion rubles in sales it earned in fiscal year 2019 (FY 2019), Magnit manages the data of 300,000 employees and more than 21,000 locations, which include supermarkets, pharmacies and cosmetic and convenience stores. Alexander Vasilenko, director of the Infrastructure and Information Security Department at Magnit, says, “We view PAM as an integral component of security systems. Privileged users have access to the type of information, which, if disclosed, poses significant risks for the operational stability of the entire company.”

Deploys leading, easy-to-manage PAM solution in just days

After narrowing PAM solution choices to One Identity Safeguard, WALLIX and CyberArk, Magnit chose One Identity Safeguard. “For us, the most important parameters were privileged account monitoring, product stability and ease of administration,” Vasilenko says. “One Identity Safeguard met all these requirements, and we especially liked that we did not have to redesign our existing work processes or install agents on servers or employee workstations.” Magnit rapidly implemented One Identity Safeguard on its own. “Thanks to detailed instructions and responsive support from One Identity engineers, deploying and configuring the system only took a few business days.”

Improves threat mitigation and staff efficiency

Magnit has improved its ability to detect threats, which reduces mitigation response times and boosts efficiency. That’s because Magnit uses automated workflows to authenticate access, record privileged

user sessions, analyze behavior and immediately alert IT personnel about any anomalies. “We can get the data we need to investigate incidents and restore the timeline of events with One Identity Safeguard, which helps us prevent any leaks of confidential information,” says Vasilenko.

Facilitates remote-work model with minimal expense and effort

When the COVID-19 pandemic erupted, Magnit had to enable staff to work from home. Equipment shortages meant many employees could use their own devices, which introduced additional security threats. “With One Identity, we could rapidly switch to a new work format without introducing major changes,” Vasilenko explains. “And we significantly improved the level of security and insight into who accesses our infrastructure with our One Identity Safeguard privileged access management solution, even though the number of remote-access sessions increased by leaps and bounds.”

Blocks threats with continuously innovative capabilities

To combat emerging threats, Magnit works closely with One Identity to help evolve its products. “One Identity takes into account the needs of its customers,” says Vasilenko. “We are constantly communicating with One Identity about new functionality and making suggestions about how to improve products, including the Safeguard for Privileged Analytics module. That way, we can continue to enable more flexible opportunities for our employees to work — and rapidly block attack attempts and malicious activity before they result in any consequences.”

“We can get the data we need to **investigate incidents and restore** the timeline of events with One Identity Safeguard, which helps us **prevent any leaks of confidential information.**”

Alexander Vasilenko,
Director of Infrastructure and
Information Security Department,
Magnit

About One Identity

One Identity, a Quest Software business, helps organizations establish an identity-centric security strategy. With a unique identity and access management (IAM) portfolio, our award-winning offering includes identity governance, AD-centered IAM, privileged access management and Identity SaaS solutions, One Identity helps organizations secure their enterprise end to end, smoothly make their digital transformation, eliminate identity challenges and reduce their attack surface from internal and external threats. Our unequalled commitment to our customers’ long-term IAM success is evident in our 7,500 customers worldwide that rely on us to manage more than 125 million identities. For more information, visit www.oneidentity.com.

The One Identity logo is a trademark of One Identity LLC and/or its affiliates. Other trademarks are property of their respective owners. Availability and terms of our solutions and services vary by region. This case study is for informational purposes only. One Identity LLC and/or its affiliates make no warranties—express or implied—in this case study. 2021 Quest Software Inc. All Rights Reserved.