SUCCESS STORY

Bank Leumi invests in Elastic Security to protect customers and infrastructure

Israel's leading bank strengthens cyber defenses by deploying Elastic Security as its SIEM solution.

Region
Israel

Industry
Financial Services

Solution
Elastic Security

60% cuts in log detection and analysis from hours to minutes

With Elastic Security, employees can hunt down logs for forensic analysis in a fraction of the time compared to the previous SIEM solution.

Decrease in total cost of ownership by 40%

Consolidating SIEM and data logging operations on Elastic Security significantly reduces the cost of running multiple platforms.

50% reduction in time spent resolving security issues

With Elastic Security, different technical groups can manage and detect threats using Kibana dashboards, significantly reducing the burden on the Security Data Team.

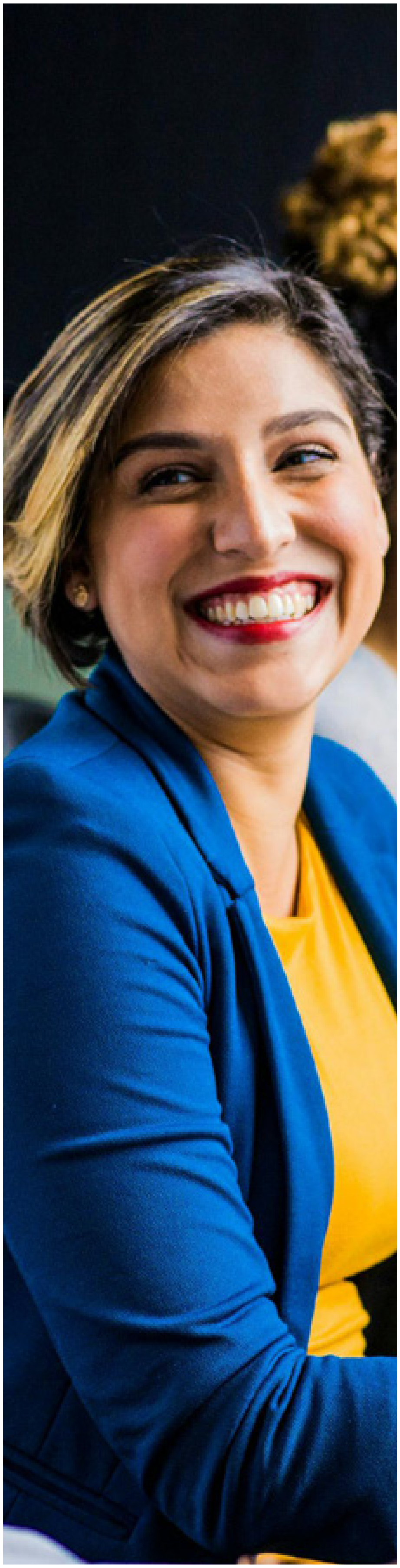
|

Founded in 1902, Bank Leumi is Israel's leading bank, with more than 7,000 employees and over $195 billion (US) in assets. Bank Leumi offers consumer, corporate, and investment banking services while pioneering digital banking solutions through various innovative online banking services.

Given the scale and diversity of its financial activities, Bank Leumi's operations generate a tremendous amount of data that must remain secure while flowing between disparate systems. Dudi Levi, Head of Data - Cyber Division of Bank Leumi, sums up the challenge. "Over the years we've seen greater digitization of the banking industry and a move to new applications and technologies such as the cloud. All these innovations require equally advanced security systems and solutions to protect the bank and our customers."

Levi's team collects and monitors complex application and systems logs from multi-environment (Cloud and On-prem), to empower its security operations center (SOC) for event monitoring and incident response. As the bank's infrastructure evolved, its previous logging and SIEM solution struggled to adapt to new circumstances, including a growth in semi-structured data generated within the bank's cloud platform.

Identifying specific logs when investigating a security event was time-consuming and, in some instances, demanded external support that further delayed SOC experts' work. Levi said, "We needed a better way of handling all kinds of data while giving our internal customers the flexibility to handle the filtering and analysis themselves."



Meeting the needs of the security team

Elasticsearch was already being used as a data lake for collecting data and logs by several teams in the bank. Bank Leumi moved to a licensed version and implemented its first Elasticsearch clusters on premises in 2019. It now has a structured process for data ingestion and analysis that applies to every use case in the organization.

The bank's experience with easy data ingestion encouraged Levi to look into Elastic's security solution when they were interested in replacing the incumbent SIEM. "When we explored all the different options on the market, Elastic Security was the best all-round security tool available," he says. It also meant that Levi's team could lean heavily on their existing Elastic expertise to meet the needs of the business.

The use of Elastic Security has broadened across the organization since it was first deployed. It now serves dozens of SOC employees and hundreds of other users who leverage Elastic in production and development environments, in the delivery of applications, and the monitoring of business transactions. "Storage in Elasticsearch also simplifies regulatory compliance and report submissions to regulators," says Levi.

> Our internal customers have high expectations around data collection and ease of use. They don't want to call us every day for help. That's why Elastic Security is so successful as the SIEM in our organization.

Dudi Levi
Head of Data - Cyber Division
Bank Leumi

Mind-blowing speed and streamlined prevention

When it comes to the speed of Elastic Security compared to the previous SIEM solution, Levi says that the difference is mind-blowing. In the past, analysts spent several hours tracking down logs for forensic analysis. With Elastic Security, it can be done in a matter of minutes. "We can accomplish so much more in less time. With Elastic, everything is just so intuitive and fast compared with the previous solution," says Levi.

In addition to the speed, Elastic Security's breadth of detection rules, especially those mapped to the MITRE ATT&CK framework, has become the backbone of Bank Leumi's cyber security operations. Elastic comes pre-packaged with hundreds of detection rules that the bank uses to protect against threats ranging from DDoS and ransomware to zero-day attacks. The bank also uses Elastic's machine-learning rules to protect against advanced attack scenarios.

Sapir Dagan, Information Security Specialist at Bank Leumi, highlights the self-service strengths of Elastic Security. Instead of calling on support, he and his colleagues can use Kibana dashboards as a data visualization tool for log analytics, security events, and threat detection. "We're a lot happier than before because we can get on with our work without interruption. Kibana is very well suited for security teams."

> Like any bank, we have a highly demanding SOC team. If Elastic Security was taken away, we would start shouting for it to be returned. It's so much faster than the previous tool.
>
> **Sapir Dagan**
> Information Security Specialist, Bank Leumi

Smart features for the future

Bank Leumi also sees the benefits of implementing ES|QL (Elasticsearch Query Language) to find specific events, perform statistical analysis, and generate visualizations. ES|QL supports a wide range of commands and functions that enable users to perform various data operations, such as filtering, aggregation, and time-series analysis. “It’s a really powerful way to transform and analyze data stored in Elasticsearch,” says Levi.

In consolidating data security on a single platform, the bank also enjoys a lower total cost of ownership (TCO). “Aside from the resilience and strength of Elastic Security, it saves us money compared with other data security solutions,” says Levi.

As the bank moves its infrastructure to AWS, Levi expects to migrate Elastic to the same cloud environment. He also plans to use Elastic searchable snapshots and S3 buckets to increase the bank’s data availability and retention period. Then, there’s the constant release of new features and security rules. “Elastic Security will enable us to stay one step ahead of hackers and other cybercriminals,” he says. “Even where it’s not possible to predict exactly how threats will evolve, I’m confident that Elastic has our backs, especially with the frequency of new releases and features on its roadmap.”

Address complex threats with Elastic Security, built on the Elastic Search AI Platform, to streamline SecOps.

Get started