SingleStore™

Building Next-Generation Cybersecurity Solutions

A guide for security product teams

Table of contents

Executive summary

Cybersecurity is at a turning point. The rise of AI-driven threats, automated hacking tools and the exponential growth of security data demand a radical shift in how security products are built. The fact is, traditional database architectures fail to keep up — leaving organizations vulnerable to emerging threats.

This guide explores the future of cybersecurity solutions and the role modern data architecture plays in enabling real-time threat detection, AI-powered defenses and scalable security platforms. By leveraging modern infrastructure, cybersecurity providers enhance their ability to detect, prevent and respond to attacks — securing their competitive edge and consistently safeguarding data in a world where threats constantly arise.

Part 1: The need for modern security solutions

Building for tomorrow's threats

Cybersecurity solutions must go beyond analyzing historical data; they need to proactively defend against attacks in real time, processing vast volumes of security data instantly. Legacy systems struggle to meet these demands, necessitating a new approach.

Key requirements for modern security solutions include:

Real-time threat detection and response

Instant data processing to detect and mitigate attacks as they happen

AI-powered autonomous defense

Machine learning-driven anomaly detection and automated countermeasures

Scalability for massive data volumes

Handling billions of security events per day without performance degradation

Cost-effective operations

Efficient infrastructure that scales with demand while optimizing costs

Support for diverse data types

Logs, network traffic, behavioral analytics and video feeds must be unified for effective threat correlation

The shift to proactive security

Security teams can no longer rely solely on traditional, rule-based detection. Instead, modern solutions leverage predictive analytics, real-time anomaly detection and AI-powered automation to detect and neutralize threats before they escalate.

Part 2: The infrastructure challenge

Why traditional architectures fall short

Cybersecurity providers that rely on legacy databases face fundamental constraints, including:

Performance bottlenecks

- Struggle to process modern data volumes
- Slow query response times impede real-time detection
- Inability to scale dynamically

Operational inefficiencies

- High infrastructure costs due to inefficient resource utilization
- Complex system management requires specialized expertise
- Fragmented data environments hinder unified analysis

Part 3: Made on SingleStore: Transforming cybersecurity with modern infrastructure

Armis Security: Revolutionizing device security

Armis Security provides a multi-tenant discovery and security platform for managed, unmanaged and IoT devices. Their solution helps enterprises maintain comprehensive visibility and security across all connected devices.

Challenges

- Data pipeline costs exceeded $1M annually
- They hit performance bottlenecks with ElasticSearch
- There were constant struggles to scale with increasing data volumes

Results

- **70% reduction** in data pipeline costs
- Query performance improved from timeouts to **under 10 seconds**
- Processing **100 billion events per day**, enabling real-time visibility
- Handling **30TB datasets** in largest customer environments

Read the full story

Lumana: AI-powered video security

Lumana delivers an intelligence platform for real-time video monitoring and surveillance driven by vector similarity search. Their solution enables advanced security monitoring across vast video datasets.

Challenges

- Infrastructure was unable to support real-time analytics
- Growing need for advanced vector search capabilities
- Multi-tenant support requirements

Results

- Analysis of **millions of hours of video embeddings**
- **2-second response time** for complex searches
- **1-second real-time alerts,** significantly improving response times

Nucleus Security: Advanced vulnerability management

Nucleus Security provides a vulnerability management (VM) platform that automates processes and workflows for enterprise security teams.

Challenges

- MariaDB infrastructure failing to support security workflows
- Limited concurrency leading to slow vulnerability scans
- Poor query performance hindering security response

Results

- **60x increase** in vulnerability scans per hour
- **20x faster performance** for the slowest queries
- **80% reduction** in error rates, improving reliability
- **25% reduction** in TCO

Read the full story

Tier-1 Cybersecurity Provider: Enhanced threat detection

A leading cybersecurity and threat detection provider needed to improve their ability to identify and respond to threats in real time.

Challenges

- 3-minute latency for critical threat reports
- Limited ability to process real-time security data
- Erosion of competitive advantage

Results

- **180x improvement** in threat reporting speed
- **15x improvement** in data ingestion rates
- Support for **1,000+ concurrent queries**, ensuring scalability
- **Sub-second** threat detection and reporting

Part 4: The AI revolution in security solutions

AI-driven cybersecurity: Meeting new threats head-on

As adversarial AI and automated cyber threats grow, security providers must integrate AI-driven capabilities to stay ahead. Key areas of focus include next-generation AI security features:

Autonomous threat detection + response

AI-driven anomaly detection with real-time automated countermeasures

Predictive threat prevention

Leveraging ML models to identify patterns and preempt attacks

Adaptive defense mechanisms

Continuous learning to refine security strategies

AI-powered autonomous defense

Identifying sophisticated attack tactics across diverse data sources

Part 5: Implementation strategy: How to build a scalable, AI-ready security solution

Best practices for security solution providers

After struggling with a complex stack of MySQL, Redis and DynamoDB, Fathom Analytics consolidated their infrastructure with SingleStore. The results were transformative:

1. Focus on core differentiators

- Build on proven infrastructure rather than developing from scratch
- Concentrate engineering resources on security innovation, not database maintenance
- Leverage modern data architectures to enhance product capabilities

2. Design for scale from day one

- Architect solutions to handle **10x current data volumes**
- Consider **multi-tenancy** and **future-proof scalability**
- Optimize for **operational efficiency** to reduce infrastructure costs

3. Enable customer success with advanced features

- Provide real-time visibility into security events
- Explore flexible integration options to fit diverse security environments
- Support various deployment models (cloud, on-prem, hybrid) to meet customer needs

The future of cybersecurity depends on modern infrastructure

The cybersecurity landscape is evolving rapidly, and traditional architectures are no longer sufficient to combat modern threats. Security solution providers must rethink their infrastructure to:

- Detect and neutralize threats in real time
- Scale dynamically to handle growing security data volumes
- Leverage AI and automation for proactive defense
- Maintain a competitive edge in an increasingly hostile cyber environment

How SingleStore powers the future of cybersecurity

SingleStore enables security teams to build performant cybersecurity solutions with:

- Sub-second query performance for real-time analysis
- AI-ready infrastructure to support automated threat detection
- A scalable, cost-effective data architecture that grows with your needs

To stay ahead of emerging threats and build the future of cybersecurity, security solution providers must adopt real-time, scalable and AI-driven data architectures.

Learn more

To explore how SingleStore can empower your cybersecurity solutions, get in touch:

www.singlestore.com
team@singlestore.com

SingleStore™