CONTRAST SECURITY

CASE STUDY

Powering Storebrand's layered approach to securing financial services

Storebrand is a leading Nordic financial services company with operations spanning banking, insurance, asset management, and pension solutions. With over 2 million customers and more than NOK 1,000 billion invested in more than 5,000 companies globally, Storebrand is one of the largest private asset managers in the Nordic region and has earned a reputation for sustainable finance and innovative investment strategies. Recognized globally for its sustainability initiatives, the company was ranked as the highest-rated Norwegian company on TIME Magazine's World's Most Sustainable Companies 2024 list.

As a financial institution managing vast amounts of sensitive customer data and handling complex financial transactions, Storebrand faces a dual challenge: maintaining robust cybersecurity while ensuring the agility of its cloud-native digital services. With the rise of threats targeting financial applications, Storebrand sought a proactive security approach to protect its applications and APIs—without disrupting developer workflows or slowing innovation. Given its cloud-first strategy and recent acquisitions, a scalable, unified security framework became imperative.

Storebrand's technology landscape

To maintain its competitive edge and provide seamless financial services, Storebrand has embraced cutting-edge technology. By modernizing its infrastructure, Storebrand ensures high performance, scalability and security across its diverse business units.

Operating across Norway and Sweden, Storebrand delivers critical financial services through a diversified portfolio of subsidiaries, including:

- **Storebrand Asset Management:** A leader in sustainable investment strategies
- **SPP:** A Swedish pension and insurance provider
- **Storebrand Bank ASA:** Offering digital banking solutions
- **Storebrand Forsikring AS:** Providing general insurance products
- **Storebrand Livsforsikring AS:** Providing life insurance products

Storebrand has embraced modern cloud architectures and open-source financial modeling to optimize operations.

Key technological advancements include:

- Migrating select divisions to Google Cloud Platform (GCP) and Azure DevOps for enhanced scalability and efficiency.
- Leveraging GitHub Actions for Google Cloud Platform (GCP) and Azure DevOps (except for select divisions).
- Adopting Kubernetes-based microservices to improve service delivery.

This technology-driven approach allows Storebrand to deliver innovative financial solutions while ensuring security at scale across business units, improving operational efficiency and customer experience.

The growing need for application security

As financial services continue to digitize, the industry faces an increasing number of cyber threats. A single security breach could expose sensitive customer data, damage brand reputation, and result in regulatory fines. Storebrand recognized the need for a proactive and integrated approach to security to protect its critical applications and maintain customer trust.

The company faced several key risks:

- Preventing financial fraud and unauthorized access to banking and investment platforms.
- Securing sensitive customer data to comply with GDPR and PSD2 regulations.
- Protecting proprietary actuarial and AI-driven investment models from cyber threats.
- Mitigating API risks, particularly in REST and GraphQL endpoints exposing transaction and customer data.
- Ensuring availability and resilience, as downtime in banking and insurance applications could lead to revenue loss and reputational damage.

Previously, Storebrand relied primarily on perimeter-based security models that lacked deep visibility into runtime vulnerabilities. The shift to microservices and cloud-based architectures demanded a more dynamic approach, especially as API exposure increased. The company needed real-time security insights to detect, prioritize, and remediate vulnerabilities efficiently.

Finding the right application security solution

Given the scale of its cloud-based operations and increasing complexity, Storebrand needed a security solution that could evolve alongside its technology infrastructure. The company was particularly focused on improving application security posture while maintaining development velocity.

Storebrand identified several critical security gaps:

- Protecting applications in Kubernetes environments, where traditional network-based security measures were ineffective.
- Minimizing developer disruption, ensuring security controls could be enforced without major workflow changes.
- Gaining visibility into runtime vulnerabilities, particularly in open-source dependencies and proprietary codebases.
- Enhancing API security through real-time monitoring and automated threat prevention.

To bridge these gaps, Storebrand needed a developer-friendly security solution that could provide automated insights, reduce false positives, and seamlessly integrate into its CI/CD pipelines to enable secure, agile software development.

Why Storebrand chose Contrast Security

After evaluating several security solutions, Storebrand selected Contrast Security due to its ability to provide real-time, automated application security without impacting development speed. Contrast offered a scalable, agent-based approach that allowed Storebrand to identify and mitigate vulnerabilities dynamically at runtime.

Key benefits of Contrast Security

- **Agent-based instrumentation:** Integrates seamlessly across Storebrand's diverse environments, ensuring comprehensive security coverage.
- **Scalability and efficiency:** Lightweight agents deploy without degrading performance, keeping up with Storebrand's rapid cloud expansion.
- **Automated security in CI/CD:** Early vulnerability detection prevents bottlenecks and allows developers to fix security issues without disrupting workflows.
- **High accuracy, low false positives:** Contrast's instrumentation approach ensures security teams focus on real threats in the exact applications highlighted by Contrast in real time.
- **Real-time application security:** Protects against zero-day exploits and continuously monitors API calls.
- **Additional layer of defense:** Catching and reporting on those attacks that bypass the WAF.

By adopting Contrast Security, Storebrand embedded security directly into the development process, empowering developers to address vulnerabilities at the source rather than reactively patching threats post-deployment.

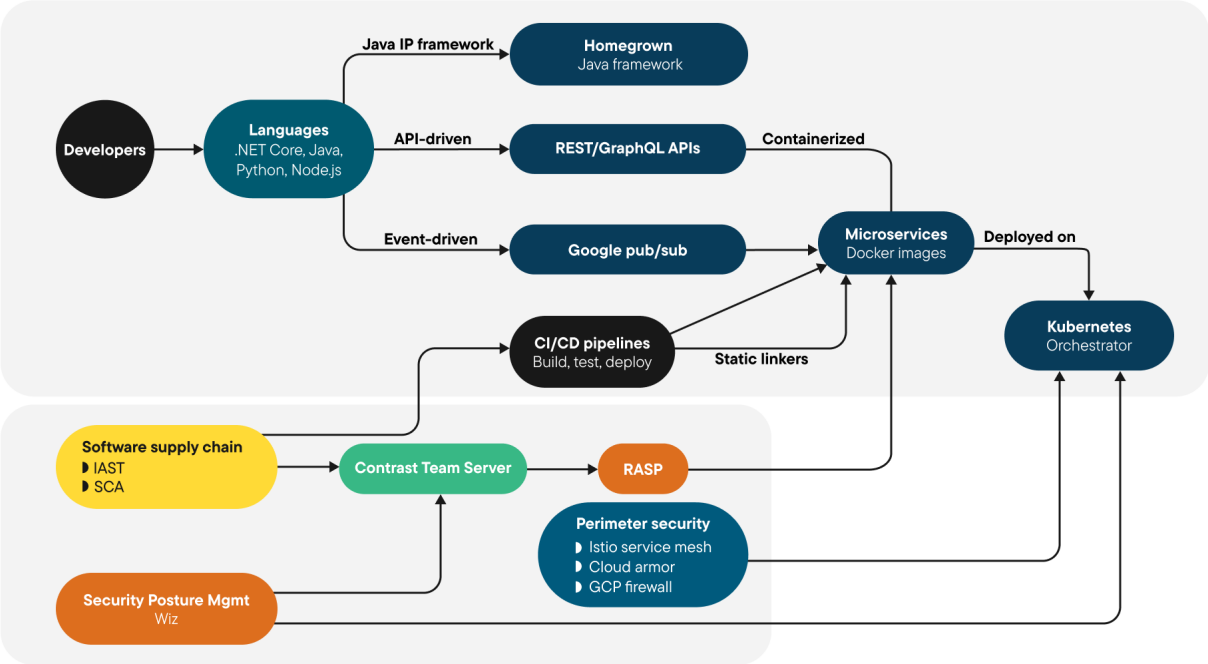
Implementation and key security wins

A crucial factor in Storebrand's security implementation was the choice of an instrumentation-based security model to augment existing eBPF (Extended Berkeley Packet Filter) solutions. While eBPF operates at the kernel level and provides observability across network traffic and system calls, it lacks the deep application context needed to pinpoint vulnerabilities within the software itself. Contrast embeds directly within applications, providing real-time detection of security flaws at the code level. This approach ensures higher accuracy, reduced false positives and the ability to dynamically block threats within the application, offering a more precise and proactive security posture compared to relying solely on eBPF's broader but less application-aware monitoring.

Storebrand rolled out Contrast Security using a phased deployment strategy, ensuring a seamless transition without disrupting core operations. The implementation prioritized automation and efficiency to effectively scale.

Key steps included:

- Automated deployment of security agents with seamless Kubernetes integration.
- Integration with cloud security tools for centralized monitoring.
- Incremental rollout—starting with runtime security, then expanding to API protection and vulnerability detection.
- Pre-production testing, ensuring security measures were robust before full-scale implementation.



Addressing critical vulnerabilities

One of the most significant security wins was detecting previously undiscovered XML injection vulnerabilities.

Contrast's real-time analysis helped Storebrand pinpoint risks as they emerged, allowing proactive mitigation before exploitation. Traditional security tools, such as Web Application Firewalls (WAFs) and static scanners, failed to detect these vulnerabilities due to their lack of application-layer visibility.

Business impact and ROI

By embedding security into the development lifecycle, Storebrand significantly improved its security posture while driving operational efficiency.

Results achieved:

- **Stronger security posture:** Proactive threat mitigation through real-time attack visibility.
- **Developer-friendly security:** Seamless integration ensured no friction in development workflows.
- **Enhanced API security:** Improved visibility into API traffic patterns, preventing unauthorized access.
- **Operational efficiency:** Automated security eliminates friction in CI/CD pipelines.

Storebrand's journey highlights the critical need for embedded, real-time security in financial services. By automating security enforcement, enabling real-time vulnerability detection, and seamlessly integrating with developer workflows, Storebrand has built a scalable security model that enhances resilience while supporting business growth.

Identify vulnerabilities and stop attacks in real-time with Contrast Security

Try Contrast

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333