elastic | Ameritas

SUCCESS STORY

UNITED STATES | FINANCIAL SERVICES | ELASTIC SECURITY

Ameritas transforms threat detection and response using Elastic to unify security visibility

For more than 130 years, Ameritas has provided life insurance, financial services, and employee benefits to customers across the US. The company started as a community-based insurer, and its commitment to maintaining integrity and building trust with its six million customers remains central to its success. Ameritas incorporates customer confidence into everything it does, from developing new products and services to building the systems that keep the business running smoothly and securely.

34 billion logs ingested monthly

With Elastic, Ameritas ingests more than 34 billion logs per month for complete visibility across a multi-cloud hybrid environment.

60% faster time to remediate

Ameritas reduced the mean time to remediate from 75 minutes to 30 minutes through improved visibility and rule tuning in Elastic.

Turns data into business intelligence

Teams across Ameritas now take advantage of Elastic dashboards to understand what's happening in the environment.

When Delonte Johnson, Director of Security Operations & Engineering, joined Ameritas, he set out to modernize the company's security profile. He's a strong believer in the "not if, but when" mindset and knows that continuous visibility is essential. Endpoint detection and response (EDR) is foundational to this approach, providing security teams with a strong understanding of security events in the environment and how to prevent it from happening in the future.

Johnson also recognized that the company's legacy security information and event management (SIEM) platform was producing a huge volume of alerts, leading to alert fatigue. "At one point, we were getting hundreds of alerts a day with no meaningful way to prioritize them," Johnson says. "We needed a reset."

> Elastic helped us reorganize and focus on high-fidelity alerts that truly matter.
>
> **Delonte Johnson**
> Director of Security Engineering and Operations at Ameritas

The question was whether to rebuild on the old platform or adopt a solution that offered better data flexibility and more value across the business. While evaluating solutions, Johnson was introduced to Elastic, which was already in use by the DevOps team. Today, Elastic Security and Elastic Observability play key roles that allow Ameritas to scale security operations and improve threat visibility.

With improved visibility, better rule tuning, and greater context, Ameritas dramatically accelerated its response times, including time to detect and time to remediate. Mean time to remediate (MTTR) dropped from up to 75 minutes to roughly 30 minutes on average. "We cut our remediation time by more than half with Elastic," Johnson says.

Previously, the growing data volumes would have overwhelmed the team, resulting in hundreds of low-value alerts. "A lot of what should have been simple records were coming in as alerts," Johnson says. "Elastic helped us reorganize and focus on high-fidelity alerts that truly matter."

Turning visibility into intelligence

Ameritas now transforms massive volumes of data into actionable information. Elastic ingests log sources from servers and apps across the company, averaging more than 34 billion logs per month. It also supports rapid scale, such as adding a log source that contributes hundreds of millions of records, without impacting performance. Even as volumes grow, Kibana dashboards keep data organized and highlight insights, allowing Ameritas teams to make more sense of large volumes of information.

"Many SIEM platforms are designed to provide value to the security team but not the organization as a whole. Elastic's ability to transform raw data into intelligence is unmatched. We're able to build dashboards and share them with teams across the company," says Johnson. "It shows the value of the data we're collecting and inspires teams to make use of the vast information we collect."

"We made significant progress toward improving our security maturity," says Johnson. "A big part of that came from better collaboration with IT and business stakeholders. Elastic played a significant role in this improved collaboration."

> Elastic lets us see the complete picture without multiple screens or manual correlation.

Delonte Johnson
Director of Security Engineering and Operations at Ameritas

Understanding a growing attack surface

With enterprise-wide visibility into the security posture, Johnson and his team were better prepared to handle the growing technology foundation. Ameritas expanded into a hybrid environment spanning on-premises systems and multiple major cloud platforms. This provided higher performance and availability as the number of internal and customer-facing digital tools increased. Elastic allows the security team to see everything that happens across the environment.

"As our cloud environment grew, Elastic was essential in helping us understand our attack surface," Johnson says. Automated controls help spotlight configuration drift or exposed assets, and machine learning features detect anomalies that might slip past humans, from DDoS attacks to potential fraud.

Elastic support for the Elastic Common Schema (ECS) also helped Ameritas gain a full understanding of what's happening across its digital foundation. "I can search an IP across web application firewalls, sign-in logs, and application logs, all with a single query," says Johnson. "Elastic lets us see the complete picture without multiple screens or manual correlation."

Making security a priority for everyone

With Elastic making information clearer and more accessible, Johnson and his security team are transforming the way that security is viewed across the entire company. The security team runs a weekly, organization-wide call to discuss emerging threats, recent alerts, and trends seen in the Elastic dashboards. This keeps security front of mind for all teams, encouraging them to find ways to balance security risk and business risk.

“We don’t want to put up so many controls that we restrict business,” says Johnson. “We need to find the right balance, and we can’t do that alone. Elastic helps our teams work together effectively toward a shared security goal. We’re able to show attacks, trends, anomalies to support our business cases.”

Johnson also works closely with the Elastic team to supplement the capabilities of the security team. “We built a strong partnership with Elastic over time where we can go to them with a variety of challenges and they work collaboratively with us to find a solution,” Johnson says.

This collaboration, both internally and externally, along with the focus on transparent security, contributed to Ameritas being named one of Forbes’ Top 100 Most Cybersecure Companies for 2023.

> Security doesn’t work in isolation. Elastic gives us a platform where we can all speak the same language, understand the risks, and respond together.
>
> **Delonte Johnson**
> Director of Security Engineering and Operations at Ameritas

Preparing defenses for the future of cybersecurity

Johnson’s security roadmap focuses on modernizing identity management, automating risk and governance, and continuing to develop skills and technology to face the increasingly complex cybersecurity landscape. Elastic remains central to this strategy, particularly as Ameritas prepares to embrace more automation and AI to combat cyber threats.

The key to preparing for the future of security, according to Johnson, involves strong relationships across the business. “Security doesn’t work in isolation,” he says. “Elastic gives us a platform where we can all speak the same language, understand the risks, and respond together.”

