CUSTOMER STORY: SECURITY + OBSERVABILITY

Software & Technology · Legacy SIEM → Elastic

Coretek consolidated its managed SOC and observability onto one Elastic platform

Coretek, the largest US Azure cloud solution provider, consolidated its managed SOC and observability onto one Elastic platform, run by a joint team on a single consumption-based model across 50+ client estates.

50%
fewer alerts, ~50 obs clients, day one

70–80%
fewer alerts, security vs. prior SIEM

~$20K → ~$4K
same coverage, one client comparison

Afternoon
kickoff to a live platform

The challenge

- ✕ Security and observability ran on separate tools and cost models with no shared context.
- ✕ Prior SIEM cost blew client budgets, was worst for non-Microsoft data, and lost deals on price.
- ✕ 90-day retention missed the one-year audit mandate; a new data source was a multi-day setup.
- ✕ Infrastructure alerts fired on a threshold with no logs or context to explain why.

The solution

- ✓ Consolidate both practices onto Elastic Cloud on Azure: one joint team, one shared architect.
- ✓ Run the managed SOC on Elastic Security; migrate ~50 clients to Elastic Observability.
- ✓ Script client onboarding end to end through Elastic's APIs and Agent Builder.
- ✓ Centrally managed detection rules; every alert lands on one Kibana investigation timeline.

How it works

1. Isolate + unify
Per-client deployments; one SOC/NOC view

2. Collect anywhere
Any source normalized in ~5 min

3. Detect as code
Central rules via API; legacy auto-migrated

4. Onboard fast
Tenant, SSO, policies scripted in an afternoon

5. Investigate
Context on the timeline, not a blank search

Before

- Working a single alert meant moving between three and five separate tools.
- Thousands of alerts a day and heavy false positives kept junior engineers in the noise.
- 90-day retention plus a separate audit store; onboarding a new source took multiple days.

After

- → ~50% fewer alerts (observability) and 70–80% fewer (security), from consolidation, not suppression.
- → One platform, consumption-based, shared across security and infrastructure teams.
- → 365-day on-platform retention; a one-year audit answered in a single query.

A new client's monthly SIEM bill came in just under $20,000. We showed them the same coverage on Elastic for about $4,000. That was the moment it clicked internally: This is the solution we lead with now.

— Tyler Hopperton, CISO, Coretek

Why it matters beyond one platform

In a managed-service market defined by margin pressure, Coretek treats platform economics, flexibility, and modern machine learning as its competitive edge. The same principles apply whether you are consolidating your first two tools or scaling to hundreds of client environments: API-driven provisioning, centrally managed rules, and one shared investigation context. Coretek is now extending anomaly detection and Agent Builder toward auto-remediation and adding APM for the 60 clients it onboards next and the 200-plus cloud-solution-provider clients beyond them.

See how running security and observability on one Elastic platform cuts alert noise or **start a free trial**