cbts

CBTS resolves incidents in seconds with platformization, featuring Cortex XSIAM

paloalto | CORTEX

RESULTS — Faster, smoother, simpler, smarter security.

13 seconds
median time to resolution, reduced from days

100%
incident close-out rate, up from dozens unresolved each day previously

20
SOC tools consolidated to 1

80%
increase in visibility into network traffic

CUSTOMER
CBTS

INDUSTRY
High Technology

COUNTRY
United States

PRODUCTS & SERVICES

AI-Driven SOC Platform
- Cortex XSIAM®
- Cortex XDR®
- Cortex XSOAR®
- Cortex Xpanse®

Network Security
- Next-Generation Firewalls
  - Software Firewalls
  - Hardware Firewalls
- Prisma® SASE
  - Prisma Access
  - Prisma SD-WAN
  - ADEM
- CDSS
  - Threat Prevention
  - URL Filtering
  - Enterprise DLP
  - SaaS Security

CBTS is a visionary, flexible, and nimble technology services provider embracing a "Consult, Build, Transform, Support" approach to solving challenges. Stationed in three main offices and 18 branches around the world, its workforce serves clients in 57 countries. From design and implementation to maintenance and optimization, CBTS combines deep technology experience with the expertise of professionals who bring a personal approach to IT transformation.

In 2024, when it spun off from its parent company, Altafiber, CBTS was given the opportunity to stand up a new security infrastructure—albeit quickly and with a lean team. Leadership was determined to strengthen security, reduce complexity and inefficiency, boost visibility, and embrace automation and AI by bringing together multiple functions and tools into a single modern platform. After a thorough review of several top solutions, the team opted to go with a platform approach from Palo Alto Networks®.

### CHALLENGE

Facing high stakes, burdened by legacy.

- The risk of exposing customer data was extremely high, given the organization's role as a managed security service provider (MSSP).
- A lack of automation and visibility from a complex mix of security products was reducing speed and effectiveness in detection and response.
- A Zero Trust infrastructure was impossible to build with existing point security tools and would have required unattainable resources to become viable.
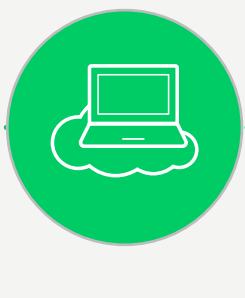

Path to platformization
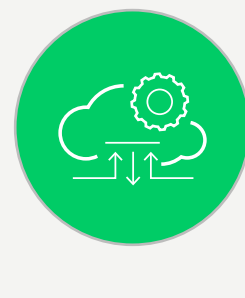
SOC modernization
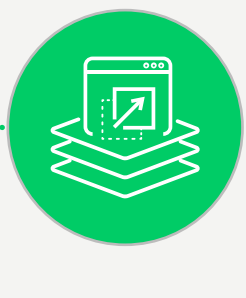Cortex XSIAM
Cortex XDR
Cortex XSOAR
Cortex Xpanse
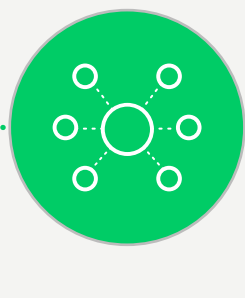
Network security
Software Firewalls
Hardware Firewalls
CDSS
ADEM

Secure remote access
Prisma Access

Branch transformation
Prisma SD-WAN

SOLUTION

A complete transformation of enterprise security.

When splitting from Altafiber in 2024, CBTS security leaders seized the opportunity to rebuild. "We had the chance to start over and really evaluate," says Chris DeBrunner, Vice President of Security Operations. From network security to data protection, endpoint security, vulnerability management, identity management, and a SIEM, CBTS was determined to put the strongest possible infrastructure in place—and bring it all together in a single solution.
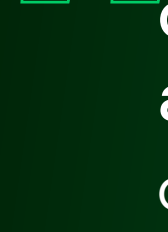
> "We needed a cohesive, supported platform—essentially one place, one screen, one data source—and we needed an opportunity to truly automate within that platform."
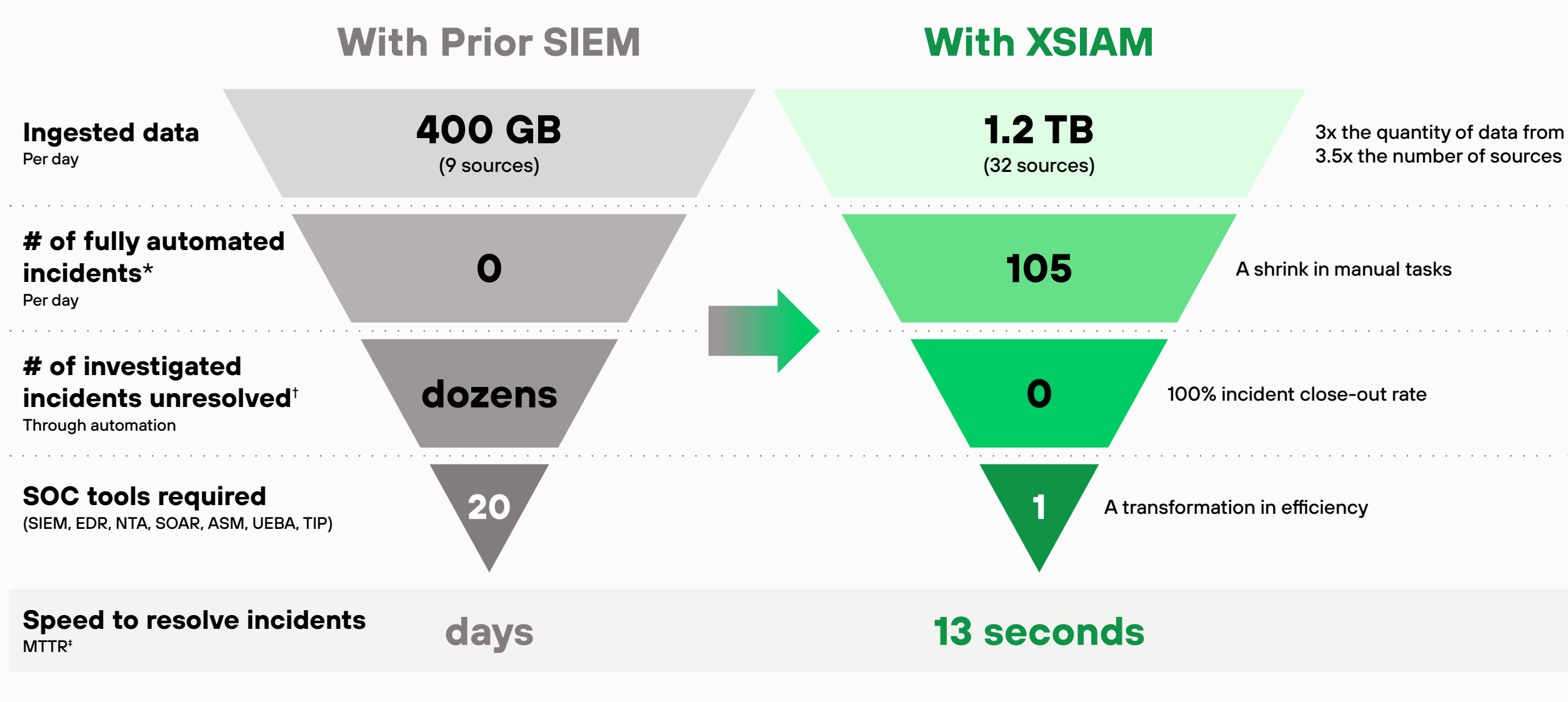>
> Chris DeBrunner, Vice President of Security Operations, CBTS

Unifying data, simplifying management

In the previous infrastructure, multi-console complexity had been a constant headache. With disparate vendors, support agreements, data sources, and integration capabilities, the CBTS SOC had been overwhelmed by labor-intensive tasks, making the team more error-prone and less effective. To begin its transformation journey, CBTS chose Cortex XDR for endpoint security, XSOAR for incident response automation, and Xpanse for attack surface management. "Cortex was our number-one choice for XDR," DeBrunner explains. "Looking at how it compares to competitors, it's always been top-notch."

The next step was to unify the platform on XSIAM, bringing together all major security capabilities (including SIEM, EDR/XDR, SOAR, ASM, and many more) under one platform, with one frontend and one backend. XSIAM is comprehensive and therefore much easier to support, enabling DeBrunner's team to spend less time chasing alerts and more time on strategic directives—and to accomplish more with a static headcount. XSIAM also unlocked CBTS's ability to automate and integrate.

Advanced capabilities lead to improved security posture

	With Prior SIEM	With XSIAM	
Ingested data *Per day*	400 GB (9 sources)	1.2 TB (32 sources)	3x the quantity of data from 3.5x the number of sources
# of fully automated incidents* *Per day*	0	105	A shrink in manual tasks
# of investigated incidents unresolved* *Through automation*	dozens	0	100% incident close-out rate
SOC tools required (SIEM, EDR, NTA, SOAR, ASM, UEBA, TIP)	20	1	A transformation in efficiency
Speed to resolve incidents *MTTR*	days	13 seconds	

*# of alerts received by automation playbook (including those that only receive first approval from SOC analyst to close)
*# of alerts investigated/closed (e.g. containing uncontained)
*(MTTR = Median time to resolution (time from alert to case resolution))

Automation to the rescue

Given the latent overwhelm in the CBTS SOC, automation was a must-have. With 108 playbooks and counting, the team has leveraged nearly every out-of-the-box option as well as built its own to automate many of the analysts' day-to-day actions—resulting in a 25% increase in efficiency. Similarly, CBTS's MSSP customers have seen huge gains in efficiency by using automations in Cortex.

6B+ → 0
events → unresolved incidents

> "Every every single incident gets touched by automation and it's triaged and closed usually within 30 seconds."
>
> Chris DeBrunner, Vice President of Security Operations, CBTS

A software approach to network security

In CBTS's own environment as well as its role as an MSSP, next-generation firewalls are critical for protection, including within hybrid clouds and on the public cloud. CBTS chose the VM-Series software firewall for several reasons: 1) its flexibility and scalability are essential to cloud migrations; 2) it provides the high security efficacy necessary for protecting data and systems; and 3) its unified management makes it easy to run on all of CBTS's environments.

50%↓
reduction in VM-Series software firewalls deployment time

Global remote access, fast and secure

For remote connectivity, Prisma Access has boosted efficiency and collaboration within the CBTS office. The organization added ADEM (Autonomous Digital Experience Management), which provides insights into user experience, app performance, and overall network health—enabling the organization to troubleshoot and even remediate issues across its entire network.

With the Cloud-Delivered Security Services (CDSS) behind Prisma Access inspecting all traffic, "We now have more visibility—in the neighborhood of 80% more," DeBrunner marvels. Prisma Access has increased even more than that. "All of the incidents that come in are well articulated, and we're able to respond very, very quickly."

Serving customers—and learning from them

As an MSSP, CBTS has unique challenges as each customer comes with a different security environment and tool set. "Having the multitenant ability within the Palo Alto Networks suite makes the work much more efficient," DeBrunner says. The ease of deployment, including training and rollout, is another major benefit. To some extent, adoption of Palo Alto Networks products was actually driven by insistence from CBTS's customers.

> "On the MSSP side, we chose to go forward with Palo Alto Networks products because they're a great suite. Our customer base demanded that we get to know the portfolio."
>
> Chris DeBrunner, Vice President of Security Operations, CBTS

Embracing the automated future.

As a technology services organization, CBTS is responsible not only for staying at the forefront of developments in AI but also for guiding its customers through them. "We knew that AI would be a key differentiator within the Palo Alto Networks portfolio," DeBrunner says, "and it has been." In 2025 and beyond, his team plans to unlock the full potential of AI capabilities within XSIAM, adding telemetry and data sources and more fully automating triage and remediation. Additionally, CBTS recently added Prisma SD-WAN to help its customers deliver fast, secure, and reliable connectivity to their branches.

Learn more about Cortex and Network Security solutions on our website.
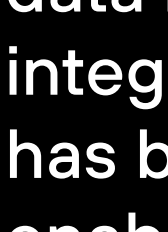
> "The platform approach—having all the data in a single place with all those integrations, plus the AI capabilities—has been a game-changer. It's enabled me to keep my headcount flat and to have our team focus on the more high-value strategic pieces of keeping our business safe."
>
> Chris DeBrunner
> Vice President of Security Operations
> CBTS