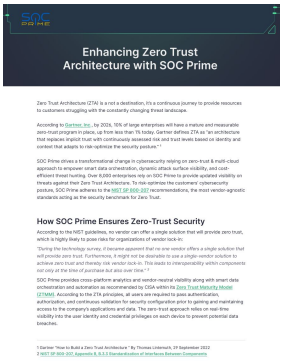

Enhancing Zero Trust Architecture with SOC Prime

Case Study

Thank you for downloading this SOC Prime Case Study. Carahsoft is the official government distributor for SOC Prime cybersecurity solutions.

To learn how to take the next step toward acquiring SOC Prime solutions, please check out the following resources and information:

For additional resources:
carah.io/SOCPrimeResources

To request a quote:
carah.io/requestaquote

For additional Odaseva solutions:
carah.io/SOCPrimeSolutions

For additional Cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
SOCPrime@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/SOCPrimeContracts

Enhancing Zero Trust Architecture with SOC Prime

Zero Trust Architecture (ZTA) is a not a destination, it's a continuous journey to provide resources to customers struggling with the constantly changing threat landscape.

According to Gartner, Inc., by 2026, 10% of large enterprises will have a mature and measurable zero-trust program in place, up from less than 1% today. Gartner defines ZTA as "an architecture that replaces implicit trust with continuously assessed risk and trust levels based on identity and context that adapts to risk-optimize the security posture." [1]

SOC Prime drives a transformational change in cybersecurity relying on zero-trust & multi-cloud approach to empower smart data orchestration, dynamic attack surface visibility, and cost-efficient threat hunting. Over 8,000 enterprises rely on SOC Prime to provide updated visibility on threats against their Zero Trust Architecture. To risk-optimize the customers' cybersecurity posture, SOC Prime adheres to the NIST SP 800-207 recommendations, the most vendor-agnostic standards acting as the security benchmark for Zero Trust.

How SOC Prime Ensures Zero-Trust Security

According to the NIST guidelines, no vendor can offer a single solution that will provide zero trust, which is highly likely to pose risks for organizations of vendor lock-in:

"During the technology survey, it became apparent that no one vendor offers a single solution that will provide zero trust. Furthermore, it might not be desirable to use a single-vendor solution to achieve zero trust and thereby risk vendor lock-in. This leads to interoperability within components not only at the time of purchase but also over time." [2]

SOC Prime provides cross-platform analytics and vendor-neutral visibility along with smart data orchestration and automation as recommended by CISA within its Zero Trust Maturity Model (ZTMM). According to the ZTA principles, all users are required to pass authentication, authorization, and continuous validation for security configuration prior to gaining and maintaining access to the company's applications and data. The zero-trust approach relies on real-time visibility into the user identity and credential privileges on each device to prevent potential data breaches.

---

1 Gartner "How to Build a Zero Trust Architecture " By Thomas Lintemuth, 29 September 2022
2 NIST SP 800-207, Appendix B, B.3.3 Standardization of Interfaces Between Components

SOC Prime ensures zero-trust cyber defense by embracing the following core principles aligned with the NIST recommendations:

- **Keeping all the data where it lives.**
  SOC Prime's Attack Detective provides complete visibility based on the organization-specific logs to query data in its native location. This enables avoiding data duplication or distribution and possible permission inconsistency for the same data across different locations, which ensures compliance with zero-trust basic tenets and is aligned with the least privilege principles according to the operative definition of ZTA as per NIST recommendations.

- **Core zero-trust logical components: Data Plane and Control Plane.**
  SOC Prime ensures role-based access that separates data plane and control plane according to NIST 800-207 Special Publication and ensures that no SIEM or EDR access credentials are shared or inherited within the Company profile[3]. Access to the organization's data and each SIEM environment cannot be automatically inherited according to company access request procedure. Different accounts are used for SOC Prime's Attack Detective policy configuration and for data storage access in different tenants with a clear segregation between the control plane and the data plane.

- **Adherence to zero-trust basic tenets.**
  SOC Prime's Quick Hunt and The Prime Hunt solutions natively integrate with ZTA by leveraging the relevant access rights and permissions for each security analytics per each SIEM, EDR, or BDP platform using existing authentication and authorization mechanisms.

Multi-Layer Security Protection Backed by the ZTA Model & Sigma Language

SOC Prime Platform runs on ZTA milestones backed by the Sigma language, an open standard for threat detection, to empower cyber defenders with the world's largest repository of detection algorithms for any technology. Sigma rules from SOC Prime Platform can be used in multiple layers of a ZTA model to detect any current and emerging security threats and adversary TTPs.

6,300+
Queries for Threat Hunting on Endpoints use case

650+
Threat hunting queries for NTA solutions

650+
Threat hunting queries for Cloud Security use case

3 NIST SP 800-207, Section 3, 3.4 Network/Environment Components

SOC Prime Platform acts as a valuable tool for teams looking for ways to enhance their cybersecurity posture and better protect their digital assets within a ZTA model.
SOC Prime Platform follows ZTA principles at the following cybersecurity layers leaving no chance for a threat to go undetected on your watch:

- **Device layer**
  Sigma rules for EDR solutions are aimed to help detect and respond to current and emerging threats on individual devices. These rules can cover a wide range of threat vectors, including malware infections, fileless attacks, and suspicious system behavior. In 2021-2022, Sigma rules addressing the Threat Hunting on Endpoint use case were the top content priority covering 50.5% of all consumed detection content from SOC Prime Platform.

- **Network layer**
  Sigma rules for network traffic analysis (NTA) solutions that can help detect and respond to threats on the network. These rules can cover a wide range of threat vectors, including network intrusions, lateral movement, and data exfiltration attempts.

- **Application layer**
  Sigma rules for applications that can help detect and respond to vulnerabilities exploitation attempts. These rules can cover a wide range of threat vectors, including SQL injection.

- **Cloud layer**
  Sigma rules for PaaS and IaaS that can help detect and respond to threats in cloud environments. These rules can cover a wide range of threat vectors, including misconfigured resources, unauthorized access attempts, and data exfiltration attempts.