Contrast SECURITY

SOLUTION BRIEF

Contrast Security and zero trust

Zero trust background

Implementing zero trust begins with the assumption that networked IT systems are compromised. It's assumed that threats to networks, systems, applications and data are constant. Users, both internal and external, attempting to access systems, resources and data should not be trusted until their identity is verified. Closely aligned with zero trust is the concept of least privilege: i.e., providing users and processes the minimum level of access necessary to perform a task. Zero-trust security is a focus shift to a trustless system that prevents unauthorized access to systems with very granular access control enforcement. Ultimately, the goal is to prevent data breaches and other significant security events that harm the enterprise, employees and customers.

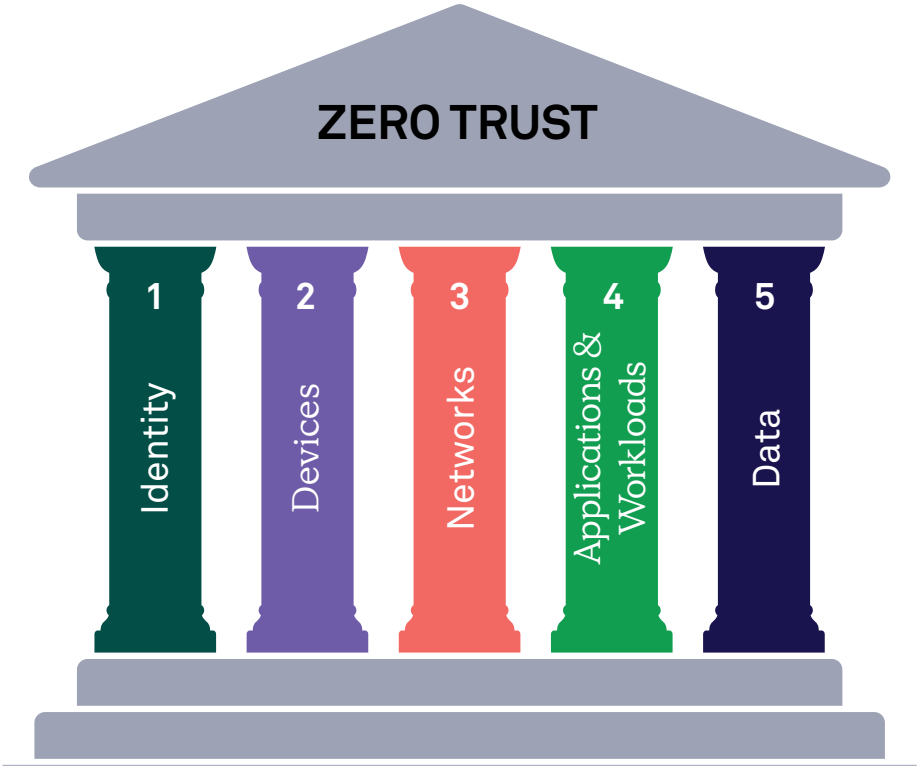
WHAT PRE-DATES ZERO TRUST?

For decades, security measures have relied heavily on perimeter solutions, including firewalls and virtual private networks (VPNs). By surrounding the network with a perimeter wall, in theory, only authenticated users can access the system, applications, data and other resources. A significant drawback to this security method is that it doesn't account for user behavior once inside the perimeter. A malicious user can take advantage of a variety of techniques and vulnerabilities to gain access to a system and once in can cause a lot of damage.

Contrast SECURITY

WHO PROVIDES ZERO TRUST?

Given that zero trust spans endpoints, networks, systems, applications, data stores, identity and access control, and more, it's not a solution delivered by a single vendor. CISA (the U.S. federal cyber defense agency – Cybersecurity and Infrastructure Security Agency) has published a Zero Trust Maturity Model. The model is designed to help other government agencies transition to zero trust. However, it's also a useful model for any entity to consider. The model has identified five pillars on which to focus:



In addition, CISA has developed a maturity model within each pillar. The journey begins at "Traditional" and progresses through Initial, Advanced and Optimal.

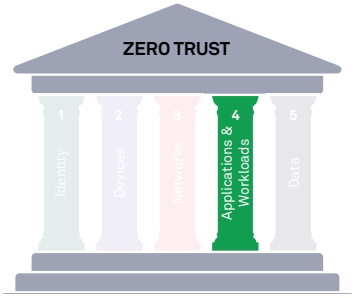
WHERE CONTRAST SECURITY CAN HELP

We'll focus on Pillar 4, Applications and Workloads. This is an area where Contrast Security really excels. So, what's in Pillar 4? It defines Applications and Workloads as including "systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments."[1]

HOW DOES CONTRAST SUPPORT ZERO TRUST?

Elements called out in the table below are precisely what the Contrast Secure Code Platform is designed for: i.e., to harden the runtime environment to reduce threats — including zero-day attacks — and to secure every line of code with Interactive Application Security Testing (IAST). Contrast makes this seamless to the developer by turning every test into a security test. Many other Contrast platform capabilities support other elements of Pillar 4, including visibility and analytics, through a concise dashboard and integrations to other security offerings in use by the Security Operations Center (SOC). Governance through policies and Software Bills of Materials (SBOMs) are also included in the Contrast Secure Code Platform[2].

Contrast SECURITY



In this table, the functions of the Pillar 4 maturity model are shown along with the support Contrast Security provides to help organizations navigate from traditional to optimal zero-trust security.

CISA Applications & Workloads maturity model, Pillar 4 and Contrast Security support:

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
1. Application Access (Formerly Access Authorization)	Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least-privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.
Contrast support: Contrast helps to ensure that attackers cannot exploit application/application programming interface (API) vulnerabilities to bypass access control mechanisms. However, Contrast doesn't enforce access control itself.				
2. Application Threat Protections (Formerly Threat Protections)	Agency threat protections have minimal integration with application workflows, applying general-purpose protections for known threats.	Agency integrates threat protections into mission-critical application workflows, applying protections against known threats and some application-specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.
Contrast support: Contrast ensures that both known (CVE/Common Vulnerability and Exposure) and unknown vulnerabilities in applications cannot be exploited by attackers. This applies to both libraries (such as Log4j) and custom application and API code. Contrast provides complete threat visibility at the application layer.				
3. Accessible Applications (Formerly Accessibility)	Agency makes some mission-critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission-critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission-critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
Contrast support: Contrast is widely used to protect applications and APIs on the public internet. Many organizations add Contrast to their platform as part of a cloud or zero-trust transformation effort, so that all applications and APIs are protected.				

Contrast SECURITY

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
4. Secure Application Development and Deployment Workflow (New Function)	Agency has ad hoc development, testing and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing and production environments (including automation) with formal code deployment mechanisms through continuous integration/ continuous deployment (CI/ CD) pipelines and requisite access controls in support of least-privilege principles.	Agency uses distinct and coordinated teams for development, security and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.
Contrast support: Contrast provides instant, accurate, and comprehensive library analysis and vulnerability testing that naturally integrates into CI/CD pipelines, along with integrations, to provide instant feedback.				
5. Application Security Testing (Formerly Application Security)	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the Software Development Life Cycle (SDLC) across the enterprise with routine automated testing of deployed applications.
Contrast support: Contrast provides unparalleled application security testing that runs continuously during development and quality testing. Contrast's results are reported instantly, are far more accurate than traditional Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools, and can scale to many thousands of applications in parallel.				
6. Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission-critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health and performance) and security monitoring for improved log collection, aggregation and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprisewide comprehensive visibility.
Contrast support: Contrast provides extensive analytics around application security telemetry gathered from development, testing and production environments. Contrast enables policy enforcement across an application portfolio and metrics to ensure compliance and continuous improvement.				

Contrast SECURITY

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
7. Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize security and performance.
Contrast support: Contrast is fully automated and can be run continuously on many thousands of applications in parallel. Every project will have real-time dashboards, notifications and integrations into tools already being used. All data is accessible via a fully supported REST API.				
8. Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching and tracking software dependencies based upon mission needs (for example, with Software Bills of Materials [SBOMs]).	Agency implements tiered, tailored policies enterprisewide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.
Contrast support: Contrast enables full policy control over an entire portfolio of applications and APIs. Contrast includes numerous dashboards and reports that can be used to govern application security at scale and drive improvement.				

CONTRAST SECURE CODE PLATFORM AND ZERO TRUST

With government agencies and enterprises adopting the zero-trust philosophy when designing their security architecture, how does the Contrast Secure Code Platform support their efforts to build and deploy secure applications?

1. **Instrumentation and interactive security testing:** The Contrast platform continuously detects and prioritizes vulnerabilities and guides developers on how to eliminate risks.

2. **Third-party code:** Test and protect third-party, open-source code moving through your software supply chain.

3. **Production runtime protection:** Harden underlying runtime environments where applications run and block runtime attacks on known and unknown code vulnerabilities with greater precision.

While zero trust spans many technology areas, Contrast Security can help secure your applications with a complete platform. To schedule a demo and see how this works, contact us here: https://www.contrastsecurity.com/request-demo.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333

Contrast SECURITY

contrastsecurity.com