Keys to the Kingdom: Guidance for Effective Zero Trust Architecture

This paper attempts to resolve the confusion surrounding Zero Trust Architecture (ZTA), and presents a strategy to fill in the gaps exploited by malicious insiders and credential-based attacks:

- **What ZTA is and is not**
- **Key concepts of ZTA**
- **Optimal strategies**
- **Difference in vendor approaches**
- **Importance of superior analytics to identify baseline behavior**

Sometimes it's good to make headlines, but not when you are the victim of a security breach. No matter what the cause of a breach, the cost to your organization can be tremendous in terms of both reputation and money. There are many things that delight CISOs and the cybersecurity teams they lead. Maintaining resilient environments, creating repeatable processes, satisfying audits, and establishing impactful training programs are just a few. While the role of the CISO is senior leadership in the organization, they tend to prefer to keep a low profile. While making the news is often good for the organization and other business leaders, for the CISO it could signal trouble.

The ransomware attack Colonial Pipeline suffered in 2021 was just such a case. During a U.S. Senate investigation into the breach, it was revealed that a single compromised password allowed hackers to breach its systems and disrupt fuel transport that impacted millions. In the aftermath, Colonial Pipeline admitted that the company used a legacy VPN that did not have multifactor authentication in place.

Colonial Pipeline is just one example of a high-profile breach that could have been prevented if the company had updated its user access policies to keep its networks and data secure.

"We noticed that while a number of these attacks exploited previously unknown implementation vulnerabilities, the vast majority actually were due to the exploitation of operational security principles," Christopher Roeser, assistant head of the Homeland Protection and Air Traffic Control Division, said in reports.

"That is, the gaining of individuals' credentials, and the movement within a well-connected network that allows users to gather a significant amount of information or have very widespread effects."

Traditional security access controls have fallen short, and a newer method, Zero Trust Architecture (ZTA), seeks to lock down access by moving defenses away from a perimeter focus with "some" trusted access, to an assumed breach, "trust no one, verify everyone" approach for users, assets, and resources. Instead of granting access to assets or user accounts based on a physical or network location, zero trust authenticates and authorizes both subjects and devices before allowing access to an enterprise resource. The concept has gained wide acceptance and as a result, vendors have attempted to create their own zero trust story, or force fit a connection to it. Unfortunately, the market is full of a wide array of zero trust products, stories, and vendor claims, leaving the whole area foggy for the security or network architect.

Zero trust is not a technology, but rather a model that seeks a shift in approach, first coined by Forrester Research. He asserted that the typical defense-in-depth approach was flawed due to the inherent-trust model, and instead recommended a new model that "allows us to build security into the DNA of the network itself." Essentially, in the zero-trust model, all traffic is deemed hostile.

Forrester suggested five concepts to make Zero Trust Architecture actionable:

1. All resources must be accessed in a secure manner.
2. Access control is on a need-to-know basis.
3. Do not trust people; verify what they are doing.
4. Inspect all log traffic coming in on the network for malicious activity.
5. Design networks from the inside out.

These five concepts were just the beginning; this initial thinking evolved significantly with contributions by governing bodies, such as NIST, CISA, and DISA, which we will incorporate later in this paper.

The Many Pieces of the **Zero Trust Architecture**

- **Access Management**
- **Identity Management**
- **MFA**
- **Persona Derivation**
- **Policy Enforcement Points**
- **Privilege Review**
- **SIEM**
- **SSO**
- **Trust Broker**
- **VPN**

Executive Order to Trust Nothing, Verify Everything

Zero trust, an enhanced security model for on-premises, cloud-based, and hybrid computer systems, is one part of a federally mandated Executive Order required of all U.S. government agencies (and contractors), and stipulates the need to prevent, detect, assess, and remediate cyber incidents is "a top priority and essential to national and economic security."

This likely will expand to state and local agencies, especially businesses contracting with those government entities. Given the frequency and severity of cyberattacks against infrastructure, commerce, and manufacturing, a shift to zero trust offers more than interoperability — it is a mandate for the future. A chain is only as strong as its weakest link, and as we've all seen attacks against smaller organizations servicing larger, more secure environments, it has become clear that any compromise matters.

Though many products and solutions are being labeled "zero trust," the concept should be considered independent of any particular technologies, security devices, or companies. There's a wide list: some vendors provide a health check for endpoints connecting to servers or services combined with single sign-on tools; others add policies, additional authentication, and privilege model review controls. Still more concentrate on virtual private networks (VPN) or desktops, brokering access between clients and servers as thirdparty secure environments.

In May 2021, President Joe Biden signed an Executive Order that enjoined departments to develop a plan to implement Zero Trust Architectures, using mitigations recommended by NIST. By January 2022, the Office of Management and Budget released their strategy memorandum for how to comply.

While many vendors may try to convince you that they check the box, be your own judge and consult the mitigation recommended by NIST and CISA to make sure you enjoy the full benefits of ZTA. NIST and CISA recognize that it is also necessary to add end-to-end monitoring, analytics, and response automation as additional capabilities to support detecting anomalies and incidents. These three capabilities are common characteristics of any Next-gen SIEM product.

As attacks have escalated on frontline security tools, platforms, and software supply chains used to protect organizational secrets and data, it's clear that "watching the watchers" in security terms is important. This is where the threat detection, investigation, and response (TDIR) capabilities of a SIEM focus, and why any security operations team needs to consider the visibility of their identity management, security log management, and threat detection tools across their on-premises and cloud attack surfaces.

The Pillars of Zero Trust

Zero Trust Architecture is an evolving way of constructing how users and entities, for example, people, devices, servers, and applications, are connected to organizational and agency resources. Even an authenticated user logged into a network needs to be verified when touching a new system, and must operate under least privilege in terms of authorization, keeping it appropriate to the role and function of the individual.

The Cybersecurity and Infrastructure Security Agency (CISA) defines the pillars of zero trust in the figure below, combining identity security, device health, network/ environment services, application workloads and data, and identifying the key areas in need of protection through a combination of architecture, processes, and tools.

The foundation of this zero trust maturity model incorporates visibility, logging, and analytics, along with automation and orchestration — core capabilities of a next-gen SIEM platform. Adding governance to the foundation provides an underlying principle for measuring and reporting on ZTA. Organizations need to do more than build ZTA; they need to demonstrate that zero trust is enforced automatically, operates effectively, and is monitored for anomalies and outliers that could represent a breach of trust.

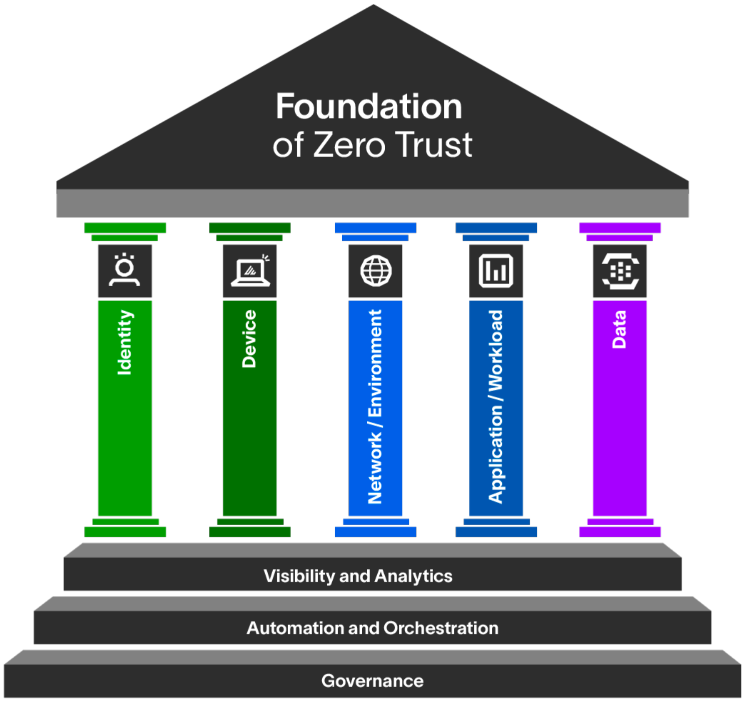


Figure 01 CISA's maturity model is a path to support the journey to zero trust.

According the CISA, the key concepts of ZTA include:

1. No implicit trust. All resources must be accessed securely, and resource access is confirmed by rules, policies, and role trust rather than network location.
2. Authentication and authorization must be confirmed for every credential and device with each session, and every connection — especially to guard against lateral movement, permission escalations, and unauthorized new account creation.
3. Verify what every credential and entity accessing resources is doing during the session. If an authenticated credential starts acting unusually, the anomaly will be recognized and identified automatically.
4. Inspect all ongoing log traffic for malicious activity, including local and cloud resources, and analyze for attacks and anomalies. A recent attack against Apache logging processes and resources (Log4j) proves that even this part of the zero trust operation requires scrutiny.
5. Automate and orchestrate responses. It's often a challenge to find sufficiently skilled security analysts, so every step that can be automated and coordinated across the security stack helps speed responses, control potential breaches, and ensure repeatability.

A zero trust security strategy includes answering tough questions:

- Who is monitoring the effectiveness of identity policies in real time?
- How do you know when something unusual is happening when the basic authentication and authorization steps are complete?

User Behavior Is Central to Zero Trust

A security stack averages between 17 and 50 tools, services, machines, and processes. Some are dedicated to monitoring or enforcing security on each pillar of the ZTA maturity model, from endpoints and network VPNs or proxies to identity protection, authentication, or cloud protections. But the truth is that few of the tools both understand normal user behavior relative to a baseline, and can use that to pinpoint new or unusual behavior.

The more mature an organization's security policies, processes, and tools are, the more prepared they are to deal with malicious actors. Security teams must be prepared to answer these types of questions:

- What is connected? Which entities, credentials, applications, and (native or cloud) services are used by the organization or agency? Can you see clearly which credentials are present on which devices, and see where every device and credential connect?
- Can security analysts observe the changing security posture of these entities and credentials as vulnerabilities and threats are discovered? Who is using the network? What users are part of the organization, or are external and allowed to access enterprise resources? This includes every identity from service accounts to privileged users and BYOD.
- What is happening right now? Security teams need insight into traffic patterns and messages with a clear vision of normal behavior for each to compare against new traffic, anomalous activity, and lateral movement.
- How is data protected? Outside of simple encryption solutions, organizations need fast visibility to detect abnormal data movement, file size changes, and more to be able to quickly identify risk.

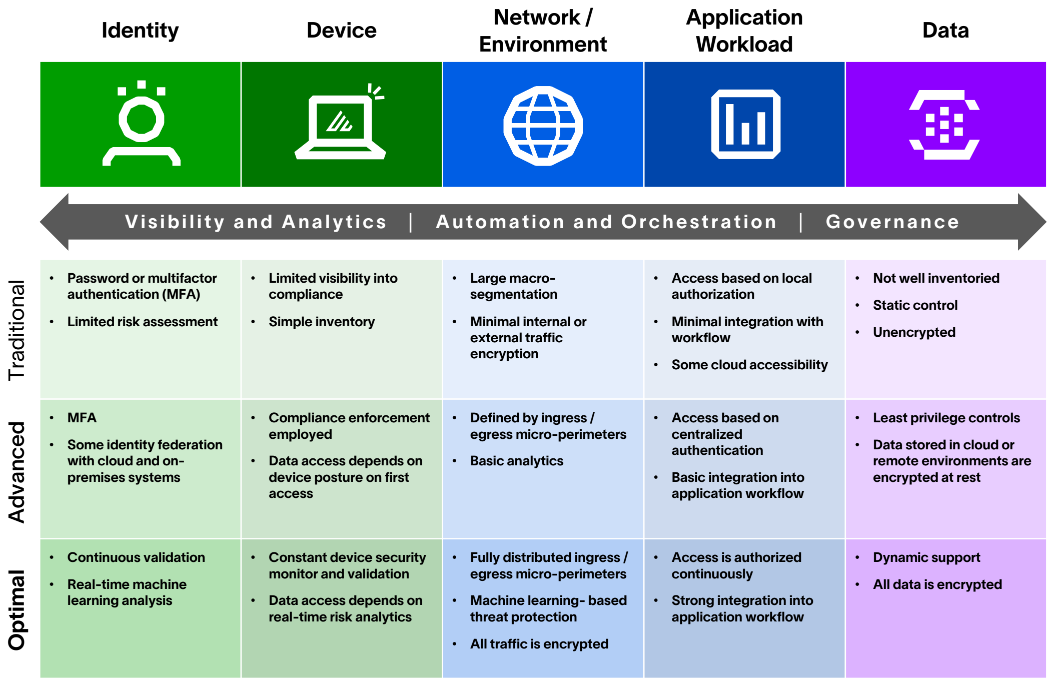
Pursuant to EO 14028, and relying on recommendations from CISA, OMB issued Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, to establish requirements for the retention and management of logs in cloud-hosted and agency-operated environments. M-21-31 focuses on ensuring centralized access and visibility for the highest-level security operations center (SOC) of each agency and on increasing information-sharing between agencies to accelerate incident response and investigative efforts.

- What automated responses are available, and are security teams clear on how to take the next investigation steps if anomalous behavior is discovered?
- Has anomalous lateral movement occurred? Can you answer when, where, and what?
- If an executive or manager asks on the fly, can security analysts identify every entity (credentials, devices, and resources) that may be involved?
- If a credential suddenly emerges or changes behavior and accesses new resources or sends out larger-than normal files to new destinations, did your security stack see and shut it down? Can you enforce data protection policies and cloud access — or were they bypassed?

Optimizing Zero Trust Architecture

Moving from traditional patchwork or tool-centric approaches into optimal security response requires end-to-end visibility across the security stack from a single point of reference. Rather than needing to manage logins for multiple tools and multiple UIs, a security analyst should have a single place to collect data, monitor risk for users and assets, and employ automated responses and playbooks for multiple attack types — from malware to malicious insiders, including compromised credentials.

All it takes is one employee's, contractor's, or partner's credentials to be compromised, and lateral movement may go unseen unless advanced or optimal zero trust is established.


Visibility and Analytics | Automation and Orchestration | Governance

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress / egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
Optimal	• Continuous validation • Real-time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress / egress micro-perimeters • Machine learning- based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted

Figure 02 CISA describes the different security maturity level approaches to a Zero Trust Architecture.

Creating a Foundation for ZTA, Security Operations, and Beyond

The capabilities of a Next-Gen SIEM are a force multiplier for any zero trust investment. By logging and analyzing the behavior of individual users and assets, and understanding what normal behavior for both looks like, the SIEM can maximize the power of the zero-trust components in place, even if the permissions and credentials appear legitimate. A careful review of the threat landscape will confirm that many (if not all) of the major breaches in recent months have come as a result of credential theft — rogue actors using valid credentials.

Modern platforms like Exabeam provide a holistic understanding of users and entities across organizational boundaries. These advanced SIEM capabilities can serve as an important ally against credential-focused attacks — which have no signatures or rules to detect them. With a focus on consuming alerts and context from as many systems, feeds, and APIs as possible, the SIEM is the best-suited platform to monitor, defend, and direct actions (within the SIEM or with third-party technologies) against identity/credential-based attacks.

Exabeam makes it easy to ingest security log events from every component within your Zero Trust Architecture. We store the data in a cost-effective way, run advanced analytics against it, and provide tools to quickly search and report on this data in real time or for historic purposes. This presents security analysts a framework for triage and investigation that allows even junior analysts to perform investigation tasks typically assigned to more senior analysts and sets in motion automated response workflows that streamline an otherwise cumbersome and time-consuming process: investigations.

Organizations can choose from flexible deployment options—cloud-delivered, self-hosted or hybrid—for easy integration with existing architecture and other security vendors.

Key benefits of the self-hosted LogRhythm SIEM Platform:

- **Comprehensive Threat Visibility:** Gain insight into critical threats with dynamic dashboards, advanced search capabilities, and simplified workflows.
- **Quickly Reduce Detection and Response Time:** Automate incident response and remediate security incidents using over 1,100 pre-built correlation rules, improving TDIR (threat detection, investigation, and response) effectiveness.
- **Flexible, Self-Hosted Platform:** Scale smoothly as your data requirements grow, with integration capabilities for both cloud services and on-premises applications.
- **Open Collection Architecture:** Collect data from over 1,000 log sources, including SaaS, self-hosted cloud, and on-prem sources, for immediate visibility across the environment.
- **Automated Data Enrichment and Normalization:** LogRhythm's patented Machine Data Intelligence (MDI) Fabric automatically normalizes and enriches log data to improve searchability and analytics.
- **Advanced Intelligence (AI) Engine:** Utilize over 1,100 actionable out-of-the-box correlation rules, including rules mapped to the MITRE ATT&CK® framework, with the option to build custom detections.
- **Enhanced Dashboards, Search, and Reporting:** Monitor the environment in real-time through dashboards, search common events across vendors, and generate scheduled reports.
- **Guided and Intuitive Workflows:** Consistent platform workflows help detect, investigate, and respond to threats more easily, reducing ramp-up time for analysts.
- **Automatic Alerts:** Risk-based alerts generated from analytics facilitate prompt incident response and reduce alert fatigue, with easy drill-down into evidence.
- **SOAR Capabilities:** Embedded Security Orchestration Automation and Response (SOAR) accelerates efficiency with automated incident response, case management, and integration with over 80 partner solutions.
- **Streamlined Compliance:** Pre-built content for 28 compliance frameworks, including lists, correlation rules, alerts, and reports, helps meet regulatory mandates more efficiently than manual processes.
- **Immediate ROI:** Gather, normalize, and interpret data from over 1,000 third-party products and cloud services, and instantly use pre-built correlation rules to detect and remediate security incidents.
- **Knowledge Base Access:** Regular bi-weekly updates offer actionable intelligence and advanced analytics to continuously improve the security posture.
- **Reduces Operational Burden:** Reduces the effort of managing SIEM, allowing security teams to prioritize tasks and focus on high-value activities.

Key benefits of the cloud-native Exabeam New-Scale Platform:

- **Pinpoint High-Risk Threats:** Uses AI-driven detection to learn normal user and entity behavior, prioritizing high-risk threats with context-aware risk scoring to identify and focus on critical security events.
- **Faster, More Accurate Investigations:** Automated investigations correlate disparate data to create threat timelines, streamlining the investigation process and allowing analysts to respond quickly and consistently.
- **Improve Threat Coverage:** Provides comprehensive coverage with pre-built integrations for over 650 third-party security products, 1,800 detection rules, and 800 behavioral models to detect a wide range of threats.
- **Maximize Security Investments:** Consolidates various security tools into a unified platform, allowing organizations to make the most of their existing investments and achieve strategic security outcomes.
- **Centralized Threat Management:** The Threat Center serves as a centralized workbench for threat management, automated evidence collection, and timeline creation, reducing alert fatigue and improving workflow efficiency.

- **Enhanced Productivity with AI Assistant:** Exabeam Copilot provides an AI-driven assistant that offers on-demand guidance, threat explanations, and suggested next steps, enhancing analyst productivity and effectiveness.
- **Automation for Streamlined Response:** Built-in Security Orchestration Automation and Response (SOAR) capabilities with pre-built playbooks and a no-code editor automate repetitive processes, reducing the time needed to resolve incidents.
- **Extensive Data Collection:** Securely collects data from on-premises, cloud, and context sources through a single interface, ensuring comprehensive coverage and ease of data transport.
- **Simplified Log Data Management:** Uses a Common Information Model (CIM) to normalize, categorize, and transform raw log data into actionable events, supporting threat detection, investigation, and response (TDIR).
- **Context Management:** Adds enrichment to event logs, including threat intelligence, geolocation, and user-host-IP mapping, enhancing detection and reporting on potentially suspicious activity.
- **Flexible, Scalable Log Ingestion:** Processes log data at a sustained rate of over 2 million events per second, with a central console for visualizing, managing, and monitoring log ingestion performance.
- **Outcomes Navigator:** Maps security log feeds against common security use cases and the ATT&CK framework, identifying gaps and improving threat coverage.
- **User-Friendly Search and Reporting:** Features a natural language processing (NLP) enhanced search experience for querying real-time and historical data, along with customizable dashboards and reports.
- **Long-Term Data Storage:** Offers options for extended log retention and archiving to meet compliance and long-term security requirements.

Exabeam offers superior analytics and insights that fuel the SIEM and strengthen Zero Trust Architecture.

Learn more about the cloud-native Exabeam Security Operations Platform and self-hosted LogRhythm SIEM Platform.

Ready to see Exabeam in action? Request a demo.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam™

Learn more at
www.exabeam.com →