TRUEFORT™

SOLUTION BRIEF

TrueFort™ Platform: Enhancing NIST Compliance

Easily comply with **National Institute of Standards and Technology (NIST)** guidance on best practices for protection, with a platform designed for adaptability, comprehensiveness, and scalability.

In response to a changing security landscape, the National Institute of Standards and Technology (NIST) continually refines guidelines like SP 800-53.

TrueFort, a truly comprehensive cybersecurity platform, provides the necessary tools to effectively and painlessly meet numerous controls for NIST compliance.

Supporting Federal Information Systems

NIST SP 800-53 is a National Institute of Standards and Technology publication that lists security and privacy controls to protect federal information systems and organizations. These controls aim to secure the confidentiality, integrity, and availability of federal data, and are mandatory for all federal entities under the Federal Information Security Modernization Act of 2014. The guidelines, divided into technical, operational, and management classes with 20 control families, are also voluntarily used by non-federal organizations to align with government standards.

The guidelines are also used voluntarily by non-federal organizations, such as private sector businesses, offering guidance to suppliers, vendors, and distributors wishing to work as partners with and approved suppliers for government and federal agencies.

- Overall, cyber security spending of the U.S. government on CFO Act and non-CFO Act agencies, excluding the Department of Defense, is projected to increase from **9.84 billion** U.S. dollars in FY 2022 to **10.89 billion** U.S. dollars in FY 2023. (Statistia)
- The number of cyberattacks targeting government agencies rose 95% in 2022, compared to 2021. (Sec. Int.)

Reinforcing Security Control Structure with TrueFort Platform

The NIST SP 800-53 document highlights six key principles in the promotion of effective information security where the TrueFort Platform can greatly support NIST compliance:

The following are paraphrased quotations emphasizing these principles:

Risk Assessment

"The organization conducts assessments of risk, and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information." (RA-3 Risk Assessment).

TrueFort Platform's capabilities align strongly with this by offering advanced risk assessment tools:

- **Real-time Behavior Analytics**
  TrueFort Platform leverages machine learning to understand normal behavior patterns of applications and users. By continually monitoring these patterns, it can identify and alert to anomalies that may signify a risk.
- **Comprehensive Visibility**
  TrueFort provides end-to-end visibility of applications, their interdependencies, and the underlying infrastructure. This detailed visibility allows for accurate risk assessment by identifying potential vulnerabilities.
- **Anomaly Detection**
  The platform provides alerting based on behavior and other parameters. This can help organizations prioritize remediation efforts based on the level of risk associated with different assets or activities.
- **Automated Policy Enforcement**
  TrueFort Platform can enforce policies based on behavioral anomalies. For example, if the behavior of a particular workload or application deviates by a certain amount, the platform can automatically limit access or perform other actions to mitigate the risk.
- **Continuous Monitoring and Updates**
  TrueFort's platform performs continuous monitoring and regularly updates its understanding of the environment, which allows it to adapt to changes in the risk landscape.

Access Control

"The information system enforces approved authorizations for logical access to information and system features in accordance with applicable access control policies." (AC-2 Access Control).

TrueFort Platform's granular access controls, through microsegmentation, enable organizations to manage access precisely and effectively.

- **Granular Application Controls**
  TrueFort Platform provides granular control over application behavior, network connectivity, and user interactions. It gives organizations the ability to control who can access what and under which circumstances, enforcing least privilege principles.
- **Dynamic Microsegmentation**
  TrueFort creates logical boundaries around each application or workload. This means that even if an attacker manages to gain access to one part of the network, they would be isolated and prevented from moving laterally to other parts of the network.
- **Policy-based Access Control**
  TrueFort Platform allows for the creation of detailed, policy-based access rules that control how data can move within these microsegments. This provides an additional layer of access control that is based on the specific requirements and risk profiles of individual applications and workloads.
- **Real-time Monitoring and Enforcement**
  TrueFort continuously monitors the network for policy violations and can automatically enforce access control policies when anomalous behavior is detected. This helps to prevent unauthorized access in real-time.
- **Integration with Existing Security Infrastructure**
  TrueFort Platform can integrate with existing security infrastructure such as Crowdstike or SentinelOne agents, enabling organizations to extend their existing access control policies to the application and network level.

System and Information Integrity

"The organization identifies, reports, and corrects information and information system flaws in a timely manner." (SI-2 Flaw Remediation).

The real-time data collection, analytics, and alert system offered by TrueFort allows for the rapid identification and correction of system flaws.

- **Real-time Data Collection**
  TrueFort Platform collects data in real-time from various sources across the network, including application behavior, user interactions, system logs, and network traffic. This provides a comprehensive view of the system's operation and potential vulnerabilities.
- **Advanced Analytics**
  The collected data is processed using advanced analytics, including machine learning algorithms, to detect anomalies and identify potential system flaws. For example, if an application starts behaving abnormally or a user starts accessing resources they typically don't, TrueFort's analytics engine can identify these as potential system flaws or security threats.
- **Alert System**
  When a potential flaw or threat is detected, TrueFort's system generates real-time alerts. These alerts provide detailed information about the detected anomaly, allowing security teams to understand and address the issue quickly. The alert system can be customized to prioritize alerts based on their severity or potential impact.
- **Automated Response**
  TrueFort can also automate responses to certain types of detected anomalies, further speeding up the process of addressing system flaws. For example, it could automatically restrict access or isolate a compromised application, preventing it from causing further damage while the issue is investigated.
- **Continuous Learning**
  TrueFort's machine learning algorithms continually learn from the collected data and the feedback from security teams, improving the accuracy and effectiveness of the analytics and alert system over time.

Audit and Accountability

"The organization develops, disseminates, and reviews/updates a formal, documented Audit and Accountability Policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities." (AU-1 Audit and Accountability Policy and Procedures).

TrueFort Platform supports audit and accountability through comprehensive data logging and visibility.

- **Comprehensive Data Logging**
  TrueFort collects and logs detailed data about application behavior, user activity, network traffic, and system events. This data can serve as an audit trail, providing a record of what has occurred within the system.
- **Real-Time Visibility**
  TrueFort provides real-time visibility into the entire IT environment, from applications and their interdependencies to underlying infrastructure. This allows organizations to quickly identify and investigate any unusual activity, enhancing accountability.
- **Centralized Reporting**
  TrueFort's platform offers centralized reporting capabilities, making it easy for organizations to access, analyze, and understand their logged data. This supports auditing efforts by simplifying the process of reviewing and interpreting the data. Automated - content missing?
- **Compliance Reports**
  The platform can automatically generate compliance reports based on the collected data, simplifying the compliance process and ensuring that organizations can demonstrate adherence to various regulatory requirements.
- **Advanced Analytics**
  TrueFort's advanced analytics capabilities help organizations to derive insights from their data, enabling them to identify patterns, spot anomalies, and understand the context of different events. This supports both accountability (by making it easier to identify when and where things have gone wrong) and auditing (by providing the data and insights needed to verify NIST compliance and regulatory requirements).

- **Integration with SIEM Systems**
  TrueFort can integrate with Security Information and Event Management (SIEM) systems, combining its log data with data from other sources for a more comprehensive view of the security posture.

Incident Response

"The organization establishes an operational incident handling capability for the information system that includes preparation, detection, analysis, containment, recovery, and user response activities." (IR-4 Incident Handling)

TrueFort's advanced behavioral analytics, anomaly detection, and incident response tools align well with this recommendation.

- **Preparation**
  TrueFort's comprehensive visibility into applications and their interdependencies aids in preparation by enabling a deep understanding of the operational landscape. Organizations can set baselines for normal behavior and develop appropriate response plans.
- **Detection**
  TrueFort's advanced behavioral analytics and anomaly detection play a crucial role in incident detection. By analyzing the behavior of applications, users, and the network, TrueFort can identify deviations from the norm that might signify a security incident.
- **Analysis**
  Once an incident is detected, TrueFort Platform provides detailed data and context to help security teams understand the nature of the incident. Its advanced analytics tools can help analyze the root cause and the potential impact of the incident.
- **Containment**
  TrueFort can automatically enforce security policies in response to detected anomalies. For instance, if a user or application's behavior suddenly changes, the platform could restrict their access to prevent potential damage while the incident is being investigated.
- **Recovery**
  By providing granular controls and visibility, TrueFort Platform allows for targeted recovery actions. Organizations can isolate affected elements, ensure the rest of the system remains operational, and then bring the isolated elements back online once the issue has been addressed.
- **User Response Activities**
  Through its real-time alert system, TrueFort Platform informs security teams about potential incidents and enables swift response. These alerts can be customized based on the severity of the incident and the organization's response plan.

Security Controls

"The organization applies security controls to protect the confidentiality, integrity, and availability of the information." (Summary of Control Families).

TrueFort Platform's comprehensive suite of controls comprehensively addresses these three key aspects of information security.

- **Confidentiality**
  TrueFort Platform offers advanced access controls, granular application behavior rules, and dynamic microsegmentation capabilities. These features help ensure that sensitive data is accessible only to authorized entities. Additionally, real-time monitoring and alerting prevent and notify of any unauthorized access attempts.
- **Integrity**
  The platform maintains the integrity of information by constantly monitoring application behavior and user activities. If any abnormal behavior or potential threat is detected, immediate alerts are sent to the security team. Furthermore, automated responses, such as access restrictions, help prevent unauthorized changes to data and applications.
- **Availability**
  TrueFort enhances system availability in compliance with NIST by providing real-time monitoring of system health and application behavior, enabling proactive issue identification and resolution. It bolsters security through anomaly detection and swift incident response, minimizing downtime. Its integration capabilities create a unified view of IT systems, while its microsegmentation strategy isolates applications to contain potential threats, preventing widespread system disruption.

Zero Trust and NIST SP 800-53: A Synergistic Approach

Implementing zero trust principles alongside NIST SP 800-53 guidelines, through the TrueFort Platform, can significantly bolster cybersecurity defense and resilience:

- Zero trust, which doesn't automatically trust anything inside or outside organizational perimeters, aligns with NIST SP 800-53's security control structure to create a potent cybersecurity defense strategy.
- "Least privilege access", a key principle of zero trust, matches with NIST SP 800-53's Access Control, creating a strong defense against unauthorized access.
- Both zero trust and NIST SP 800-53 emphasize detailed logging and system visibility, supporting real-time monitoring and swift incident response.
- Risk assessment, a component of both zero trust and NIST SP 800-53, enables constant evaluation of risk levels, complementing NIST's recommendations on periodic security risk assessments.
- Zero trust's focus on the integrity of systems and information aligns with NIST's System and Information Integrity control family.
- The importance of incident response in both zero trust and NIST SP 800-53 enhances the ability to rapidly detect, respond to, and recover from incidents.

By integrating Zero Trust principles into NIST SP 800-53 compliance efforts, organizations can achieve an optimal cybersecurity posture, ensuring both compliance and resilience in the face of evolving threats.

CONCLUSION

The TrueFort platform amplifies an organization's ability to adhere to and exceed NIST compliance standards. Its robust features allow for customization, enhanced visibility, advanced threat detection, and flexible controls, making it an indispensable tool for any CISO, CTO, or cybersecurity practitioner wanting to meet or exceed SP 800-53 or other NIST standards.

ABOUT TRUEFORT

TrueFort puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM