Cal-Secure Alignment with Tanium

Version 1.0

PUBLIC

USE ONLY

The information in this document is subject to change without notice. Further, the information provided in this document is provided “as is” and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium’s customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://docs.tanium.com for the most current Tanium product documentation.

Version history

Version	Date	Pages	Change Agent	Changes
1.0	05/11/2022	all	TMT	initial document

Reviewer	Date
Z. Nandapurkar	5/10/2022

Contents

Executive summary

Cal-Secure is a five-year roadmap for California agencies to mature their information security practices so they may deliver digital services in an effective and secure manner. The plan partially focuses on improving the security posture and governance to enhance defenses in the face of rising information security risk. Cal-Secure has directives for each California agency across three major categories: people, processes, and technology. With the thousands of cybersecurity vendors on the market, it can be tough to know where to start, especially when organizations are often already using multiple tools to manage their information security practices.

Departments and Agencies within the State of California know first-hand about the tool proliferation that cybercriminals can take advantage of daily. And point tools aimed at anything from patching to software management to threat hunting can multiply quickly. This leads to unpatched systems, a lack of a single source of truth for security data, and management challenges that burden agency resources.

That is why when procuring solutions that can address the requirements of the Cal-Secure plan, a platform approach is imperative. Instead of cobbling together numerous new tools for each requirement, and hoping they communicate with each other seamlessly, Information Technology (IT) teams need to be able to work from one data source, and pivot from threat detection to remediation to ongoing compliance.

Tanium's Converged Endpoint Management platform was built to address federated information security operations across teams, at scale, with accuracy and through a single source of truth for security data. Used by the world's most demanding organizations to include over half of the Fortune 100, and five branches of the U.S. Armed Services, the Tanium platform is the tool of choice for California agencies to satisfy more than half of the technical requirements in the Cal-Secure Plan.

Tanium customers within the State of California are already using the platform approach to answer important questions such as:

- How many of your endpoints have critical vulnerabilities?
- What critical patches are outstanding?
- How long does it take to resolve a threat once you have identified it?
- What is the status of disk encryption, antivirus, and host firewalls?

Without quick and accurate answers to these questions, California organizations could be left in the dark in the event of a major breach, leaving constituent data, reputation, and security maturity at risk.

Phased order of priority of cybersecurity capabilities

The California Homeland Security Strategy (HHS) lays out the priority to implement and maintain procedures to detect malicious activity, and conduct technical and investigative-based countermeasures, mitigation, and operations against existing and emerging cyber-based threats. As such, the state of California has defined the phased order of priority of cybersecurity capabilities. These include:

Phase one

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Anti-Malware Protection	The automated technical capability to detect and block malicious activity from trusted and untrusted applications, and dynamically respond to security incidents and alerts.
Anti-Phishing Program	A collection of security controls, including technological capabilities to detect and prevent email-based phishing attacks, as well as the process of training employees to identify and deal with potential phishing email threats.
Multi-Factor Authentication	Authentication is based on two or more of the following: something you know (i.e., password), something you have (i.e., token or smartcard), or something you are (i.e., a biometric).
Continuous Vulnerability Management	Vulnerability scanning is an inspection of potential points of exploitation and weakness on a network or system including outdated software versions, missing patches, or misconfiguration and flawed programming.

Phase two

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Asset Management	The effective tracking and managing of IT assets for an entity's program and enterprise IT infrastructure and production systems, including the ability to identify and classify entity owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g., state staff, vendor support), and the ongoing refresh activities necessary to maintain the entity's IT assets.
Incident Response	An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is a six-step process that includes: 1) preparation, 2) identification, 3) containment, 4) eradication, 5) recovery, and 6) lessons learned.
Continuous Patch Management	Systematic notification, identification, deployment, installation, and verification of operating system, firmware, and application software patches.
Privileged Access Management	Secure provisioning of privileged access to critical assets, and effective monitoring and maintenance of privileged accounts and access. Privileged access spans a wide range of systems and infrastructure components, such as operating systems, databases, middleware, applications, and network devices.
Security and Privacy Awareness Training	Creating awareness and educating employees and other users of information systems on the information security risks associated with the activities related to their job roles, as well as their responsibilities in complying with an organization's security policies and procedures designed to reduce these risks.
Security Continuous Monitoring 24x7	Information Security Continuous Monitoring is the ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems and networks by assessing security control implementation and organizational security status in accordance with organizational risk tolerance and within a reporting structure designed to make real-time, data-driven risk management decisions.
Cloud Security Monitoring	The continuous security monitoring of cloud infrastructure for potential security vulnerabilities and threats, as well as assuring optimal functioning of the cloud platform while minimizing security risks including costly data breaches.

Phase three

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Data Loss Prevention	The ability to identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) from unauthorized use and disclosure. Data loss prevention (DLP) includes deep packet inspection and analyzing the contextual security of transactions.
Log Management	The process for generating, transmitting, storing, analyzing, and disposing of log data. Log management is essential to ensure computer security records are stored in sufficient detail for an appropriate duration. Sources of log entries include network devices, authentication servers, operating systems, applications, etc.
Network Threat Detection	Effective monitoring and analyzing of network or system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.
Network Threat Protection	Effective protection against network security threats attempting to harm organizational assets and thwarting attempts to proliferate on an organization's network.
Threat Intelligence Platform	Automated mechanism to aggregate, transform, analyze, interpret, or enrich threat information to provide the necessary context for decision-making processes.
Application Security	Application security incorporates specific security measures, policies, processes, and controls into all phases of the application lifecycle including design, development, testing, implementation, upgrade, and maintenance.
Operational Technology (OT) Security	Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. OT is common critical infrastructure in Industrial Control Systems (ICS) such as a SCADA System.

Phase four

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Disaster Recovery	The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
Enterprise Sign-On	Enterprise sign-on eliminates the need to separately authenticate and sign-on to individual applications and systems. It allows the user to authenticate once, and then be subsequently and automatically authenticated when accessing other specified systems.
Mobile Device Management	The fundamental visibility and security controls needed to secure, manage, and monitor any entity or employee-owned mobile device, such as smartphones or tablets that access an organization's sensitive or confidential information.
Application Development Security	Security as part of the software development lifecycle to ensure application confidentiality, integrity, and availability. It includes the people, processes, policies, and practices to build security into application development and is the responsibility of all stakeholders and project staff, not just the software developers.
Application Whitelisting	The use of whitelists (a list of explicitly allowed applications) to control the applications permitted to execute on a host, thereby preventing the execution of malware, unlicensed software, and other unauthorized software.
Software Supply Chain Management	Supply-chain-management software (SCMS) is the software tools or modules used in executing supply chain transactions, managing supplier relationships, and controlling associated business processes.

Phase five

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Identity Lifecycle Management	The collection of technologies and practices that provisions and deprovisions users to appropriate levels of access to organizational resources.
Insider Threat Detection	A coordinated collection of security capabilities designed to detect the unauthorized disclosure of sensitive information by an entity with authorized access.

CAL-SECURE TECHNICAL CAPABILITY	DEFINITION
Network Access Control	Examining incoming connections to an organization's network from remote users and allow or disallow access based on those checks.
Enterprise Encryption	Enterprise encryption applies security and access controls directly to structured and unstructured data wherever it exists in the enterprise including on premises, virtual, in the cloud or in a hybrid environment, and at rest, in transit and in motion.
Mobile Threat Defense	Threat detection and protection technologies that are designed for the requirements and vulnerabilities of mobile platforms, such as smart phones and tablets.
Unified Integrated Risk Management	Implement a statewide Unified Integrated Risk Management Platform for integrated risk management and automation of information security programs and oversight.

Mapping Tanium solutions to technical capabilities across each phase

The Technical Capabilities outlined in the Cal-Secure Plan are mapped across five phases to help departments prioritize which capabilities to focus on first and help plan across the five phases. With the Tanium Platform, departments can leverage Tanium's pre-existing solution areas, to strategically satisfy the technical capabilities across all five phases. Each solution area is made up of modules – which are outlined in further depth in this document.

What to implement, and when?

Each Tanium solution area (listed below) comes with a collection of modules that will help California departments address specific aspects of their endpoint security and operations management. The solution areas can be implemented as-is or can be broken up into modules in an ad-hoc way.

The Tanium platform is deployed as a fully-managed, cloud-based service, with zero customer infrastructure required. It is available in the cloud through a number of cloud providers. On-premise deployment options are also supported.

TANIUM SOLUTION AREA	INCLUDED MODULES
Asset Discovery & Inventory *See everything on every endpoint*	Discover, Asset
Client Management *Control your IT assets with confidence*	Discover, Asset, Enforce, Deploy, Patch, Performance, Provision
Risk & Compliance Management *Stay ahead of exploits*	Discover, Enforce, Deploy, Patch, Risk, Impact, Comply, Reveal
Sensitive Data Monitoring *Gain complete control of all your data*	Discover, Integrity Monitor, Reveal
Threat Hunting *Shut down attackers*	Discover, Enforce, Impact, Threat Response

For entities within the State of California to get the most benefit from the Tanium platform, and to satisfy the Cal-Secure Technical Capabilities most efficiently across each phase, we recommend departments implement Tanium Solution areas in the following order:

PHASES	TANIUM SOLUTION AREAS / MODULES RECOMMENDED
1& 2	Asset Discovery & Inventory Solution Area Risk & Compliance Management Solution Area + Threat Response Module
3	Sensitive Data Monitoring Solution Area
4 & 5	Technical Capabilities already covered with previously implemented Solutions

This Solutions-based approach may help departments establish a foundation of certainty with visibility and control starting in phases one and two, and with just one additional solution area for phase three, satisfy the technical requirements for future phases as well.

However, if a department should prefer procuring Tanium in an ad-hoc approach by module, that is also an option.

The remainder of this document will outline the specific Technical Capabilities listed in the Cal-Secure Plan and outline how Tanium *modules* meet each requirement.

Phase one of cybersecurity capabilities

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Anti-Malware Protection	• Tanium Threat Response continuously monitors endpoints for suspicious activity whether they are on or off the network or VPN. Real-time alerting gives security teams immediate notice when anomalies occur so they can investigate using the Tanium platform. Users can also create custom alert definitions for tailored detection depending on their unique needs. Deep Instinct Integration Deep Instinct prevents and classifies threats for the Security Operations Center to triage with Tanium alerts to stop multi-stage attacks faster. • Tanium Enforce integrates with Windows Defender native antivirus (AV) capabilities allowing security operators to manage and configure Windows Defender across the organization. Enforce Anti-malware policies using the Microsoft Anti-malware engine to protect endpoints from viruses. These policies are configured using machine administrative templates, and Windows Defender Antivirus Active Directory administrative group policy objects on Windows systems. • Tanium Threat Response integrates with Deep Instinct's Deep Learning Cybersecurity Platform to further enable SecOps to see the status of prevented events and alerts in one single source of truth console. Learn more about Deep Instinct integration with Tanium here: Tanium + Deep Instinct Relevant Tanium Modules: • Tanium Threat Response • Tanium Enforce	Tanium Fully Meets This Requirement
Anti-Phishing Program	Tanium does not address this requirement at this time.	Tanium Does Not Currently Meet This Requirement
Mult-Factor Authentication	Tanium does not address this requirement. Tanium does play into a Zero Trust practice by validating endpoint security posture alongside an IdAM or other identity or application validation.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Continuous Vulnerability Management	• Tanium Comply provides unified vulnerability management built to assess modern endpoint environments. With Tanium Comply, organizations can continuously scan their endpoints for vulnerabilities, misconfigurations, and incidents of noncompliance with internal standards or external regulations. With this real-time data, organizations can prioritize the problems they find, drive remediation, and validate whether they have addressed their risks. Tanium Comply helps meet internal standards and provides continuous compliance management for regulations such as PCI (Payment Card Industry), HIPAA (Health Insurance Portability and Accountability), and SOX (Sarbanes-Oxley Act). Tanium Comply supports the Security Content Automation Protocol (SCAP), can use any Open Vulnerability and Assessment Language (OVAL) content, and uses its own content library updated daily with vulnerability, compliance, and CIS (Center for Internet Security) definitions and benchmarks. • With Tanium Deploy, IT operations teams can detect and update outdated software versions across large organizations with minimal infrastructure requirements. Tanium Deploy can evaluate environments of any size and return real-time and accurate results on software versioning and other granular information in minutes, giving teams a single source of truth for patch status, and the ability to deploy patches or make other changes as needed as quickly as possible. • Tanium Risk helps organizations prioritize remediation by evaluating the potential impact of a vulnerability or compliance gap in their environment —whether lateral movement or sensitive data exposure. Relevant Tanium Modules: • Tanium Comply • Tanium Deploy • Tanium Risk	Tanium Fully Meets This Requirement

Phase two of cybersecurity capabilities

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Asset Man-agement	• Tanium Asset allows users to automate asset reporting with speed and accuracy. Quickly and easily find, inventory, and maintain IT assets from one platform. Tanium's unique approach to endpoint visibility and control allows IT teams to take a real-time inventory of hardware and software assets across the entire organization. Utilize predefined (or custom) reports and dashboards with details by department, location, user group, and more to gain insights around software utilization. Built-in automation allows team members to create reports, and have them automatically update, get emailed to stakeholders, or get notified with set parameters. Organizations often make important decisions based on their Configuration Management Database (CMDB) information, and if that data is not accurate, misalignment can occur. Tanium Asset feeds real-time data into common CMDBs, such as ServiceNow, allowing organizations to have the freshest and most accurate information possible. For offline devices, Tanium Asset provides reporting on the last known state of the device. • IT Service Management (ITSM) through Tanium's partnership with Salesforce combines the comprehensive, real-time data provided from the Tanium platform with ease of use, familiar user interface, built-in artificial intelligence (AI) features, and automation of the Salesforce platform. The IT Service Center (ITSC) CMDB is integrated with the endpoint management features of the Tanium platform. Tanium's endpoint management solution helps ensure teams have accurate, real-time data that is comprehensive. Learn more about integration here: Configuration Management Database (CMDB). Relevant Tanium Modules: • Tanium Asset • Salesforce IT Service Center (powered by Tanium)	Tanium Fully Meets This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Incident Response	With Tanium Threat Response, organizations can deploy a set of incident response tools to each endpoint. With these tools on the endpoints, organizations can: • Scope and hunt for incidents across the enterprise by searching for evidence from live system activity and data at rest with simple natural language queries. • Examine and parse dozens of forensic artifacts on Windows, Mac, and Linux systems. • Identify outliers and anomalies by collecting and comparing data across systems in real time. • Build saved queries and dashboards to continuously monitor endpoints for malicious activity aligned to key phases of the intrusion lifecycle. Relevant Tanium Modules: • Tanium Threat Response	Tanium Fully Meets This Requirement
Continuous Patch Man-agement	• With Tanium Patch, IT operations teams can keep systems up to date with automated patching for Windows, Linux and MacOS endpoints across the enterprise, at speed and scale. This helps organizations reduce complexity and increase business resilience. • With Tanium Deploy, IT operations teams can rapidly install, update, and remove software across large organizations with minimal infrastructure requirements. Tanium Deploy includes templates for importing and deploying third-party software. The Tanium platform offers speed and scale to help ensure application software patches deploy quickly on endpoints without fail. Relevant Tanium Modules: • Tanium Patch • Tanium Deploy	Tanium Fully Meets This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Privileged Access Management	Tanium Impact allows operators to identify and quantify the user accounts that have administrative access to key systems, such as high-profile workstations or Active Directory domain controllers. Operators can determine the potential lateral movement of an attack and take action to prevent additional compromise. Tanium Impact gives actionable information on how an organization can make their IT environment more resilient by reducing the risk and impact of security incidents and IT outages. Tanium Impact users can: • Visualize complex access rights, dependencies, and relationships across enterprise assets. • Leverage automated tools to measure, prioritize and remediate risks caused by complex access rights. • Determine the impact of vulnerable systems on the overall enterprise security posture. Learn more about Tanium Impact here: Why Tanium Impact is Important to IT Organizations Relevant Tanium Modules: • Tanium Impact	Tanium can partially address this requirement, by auditing and revealing user access to different systems
Security and Privacy Awareness Training	Tanium does not address this, aside from providing Tanium specific training.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Security Continuous Monitoring (24 x 7)	Tanium Interact leverages Tanium features to ensure AV and other security tools are installed, configured, and running properly. • Tanium Enforce allows organizations to simplify, centralize, and unify policy management of end-user devices. This includes auditing and assessing several security controls such as Windows Defender AV management, as well as Local Firewall Policy Management, BitLocker, and more. Tanium Threat Response continuously monitors endpoints for suspicious activity whether they are online or offline, and on or off VPN. Real-time alerting out-of-the-box signals give security teams immediate notice when anomalies occur so they can investigate. Users can also create custom signals for tailored detection. • Tanium Trends gives insight into key security metrics and operational health by creating visualizations of current and historical endpoint data. • Tanium Comply and Tanium Discover remote authenticated scanning within the modules look for endpoints that do not have the Tanium client installed. This scan type is useful for getting information from endpoints within subnets that do not support having the Tanium Client installed. This provides for a better view of risk and security posture across the entire organization. • Tanium Risk helps organizations prioritize remediation by evaluating the potential impact of a vulnerability or compliance gap in their environment, whether lateral movement or sensitive data exposure. Relevant Tanium Modules: • Tanium Interact • Tanium Trends • Tanium Enforce • Tanium Comply • Tanium Discover • Tanium Threat Response • Tanium Risk	Tanium Fully Meets This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Cloud Security Monitoring	• The wide array of capabilities provided with the Tanium platform allows organizations to replace siloed point tools that either will not scale in the cloud or will not work in the cloud environment. Organizations can also simplify their management stack and realize cost savings while increasing security, speed, and agility with a single agent for cloud, virtual, or physical endpoints. Discover and remediate vulnerabilities and configuration compliance issues in seconds. The platform also provides full visibility and control of running applications, containers, and virtual machines. • With Tanium Discover, organizations can quickly gather inventory of all cloud endpoints and proactively gain management control over unmanaged instances. • With Tanium Patch and Tanium Deploy, organizations can distribute, manage, and report on operating system patches and software updates for cloud hosted systems reliably and quickly. • With Tanium Threat Response, organizations can hunt, detect, investigate, contain, and remediate threats and vulnerabilities within the cloud infrastructure. Relevant Tanium Modules: • Tanium Discover • Tanium Patch • Tanium Deploy • Tanium Threat Response	Tanium Fully Meets This Requirement

Phase three of cybersecurity capabilities

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS REQUIREMENT?
Data Loss Prevention	Traditional DLP products typically require a complex architecture of indexing servers and databases that result in slow performance and poor scalability. Tanium Reveal can efficiently identify, search, and monitor sensitive data across hundreds of thousands of endpoints with the same single management server and client with no need for any additional infrastructure. Tanium Reveal provides out-of-the-box rules to help organizations identify sensitive data governed by regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), PCI, and HIPAA. Users can also define their own rules to detect any type of sensitive or proprietary data, specifying the types of files to match against, the patterns to detect, and how to tag and alert on matches. Tanium can also look inside of files, and not just in file names, for keywords or general criteria that indicate sensitive data. Many traditional DLP solutions aggregate indices of potentially sensitive data onto centralized storage, which can introduce additional risks of data exposure. Tanium Reveal preserves sensitive data at its origin, which can reduce these risks and simplify regulatory compliance. Relevant Tanium Modules: • Tanium Reveal	Tanium Reveal can partially address this requirement, but it is not a full DLP solution. It can, however, supplement many of the features of a DLP solution. In many cases, such as Log4j, Tanium Reveal can provide a unique capability other DLP solutions cannot
Log Management	Tanium Connect is not a log management tool but can integrate with Security Information and Event Management (SIEM), log analytics tools, threat feeds, or send email notifications based on collected endpoint data. Through the adoption of the Tanium Platform and replacement of point products, entities can reduce log data transmissions to originate from Tanium, for easy storage and data realization.	Tanium can export data to logs, but currently does not offer log management
Network Threat Detection	Tanium does not address this capability. However, we can query your environment for all devices connected to your network that may pose a threat due to poor device posture.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS REQUIREMENT?
Network Threat Protection	Tanium does not address this capability. However, we can query your environment for all devices connected to your network that may pose a threat due to poor device posture, and allow you to take action to secure those devices.	Tanium Does Not Currently Meet This Requirement
Threat Intelligence Platform	Tanium Threat Response can leverage multiple sources of intel to identify and alert on potential threats in an environment. In addition to supporting third-party intelligence sources, Tanium provides threat intelligence called Signals. Intel documents and Signals, referred to as intel, interact with the engine to provide comprehensive monitoring and alerting. With the Tanium's reputation feature within the Tanium Threat Response module, organizations can build a repository of reputation data pulled into the Tanium platform from various sources, such as Palo Alto WildFire, Recorded Future, ReversingLabs, and VirusTotal. These sources determine threat levels for file hashes. Tanium Threat Response can use this data to give an indication of potentially malicious files. Organizations can also send reputation data to other tools used alongside Tanium to import reputation data to Tanium trends boards. The reputation database is a cache that consists of reputation items. When configured, reputation items are scanned by a reputation source, which is a service that determines whether a reputation item is considered malicious, non-malicious, suspicious, or has an unknown status. This functionality allows operators and organizational leaders to get a more holistic view of their risk posture all from one tool. Relevant Tanium Module: • Tanium Threat Response	Tanium can address this need end-to-end for endpoints in conjunction with our partners, or even stand alone for some entities depending on the level of maturity they need out of a Threat intelligence management solution
Application Security	Tanium does not provide application code security capabilities for software application security. Tanium can scan your application libraries for vulnerabilities and threats.	Tanium Does Not Currently Meet This Requirement
Operational	Tanium does not address specific change control monitoring for ICS Infrastructure.	Tanium Does Not Currently Meet This Requirement

Phase four of cybersecurity capabilities

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Disaster Recovery	Tanium Deploy can be used in a disaster recovery scenario to rapidly install, update, and remove software across large organizations with minimal infrastructure requirements. You can create deployments to run during a maintenance window that is convenient for your IT operations. Tanium Provision provides bare-metal provisioning of Microsoft Windows to on-premises and Internet-connected devices. It also enables imaging of outdated or broken devices in a disaster recovery scenario. For more information, see: Introducing: Bare Metal Provisioning with Tanium Provision Relevant Tanium Modules: • Tanium Deploy • Tanium Provision	Tanium can partially address this requirement, to help organizations quickly image devices whether they are on-premises or remote.
Enterprise Sign-On	Tanium does not address this capability.	Tanium Does Not Currently Meet This Requirement
Mobile Device Management	Tanium does no address this capability.	Tanium Does Not Currently Meet This Requirement
Application Development Security	Tanium does not address this capability.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Application Whitelisting	With Tanium Enforce, organizations can use and set AppLocker policies environment-wide to prevent unwanted executables from running on endpoints (deny rules) or to allow only certain applications to run on endpoints (allow rules). Use a Software Restriction Policy (SRP) to block the execution of applications that are created using the Windows SRP component. Relevant Tanium Module: • Tanium Enforce	Tanium currently addresses this end-to-end on AppLocker supported systems
Software Supply Chain Management	Tanium does not address this capability. Tanium can scan your environmet for vulnerabilities introduced by third party software supply chain risks and allow you to take action to remediate those vulnerabilities.	Tanium Does Not Currently Meet This Requirement

Phase five of cybersecurity capabilities

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Identity Life-cycle Man-agement	Tanium does not yet address this capability.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Insider Threat Detection	• With Tanium features plus Tanium Threat Response, organizations can use Tanium out-of-the-box sensors to perform the following: ◦ Identify unauthorized processes sending data out of the network ◦ Validate findings from hits or alerts coming from various security and operational teams such as: ▪ Identifying the last logged-in user to a machine or, ▪ If the file still exists and/or has been renamed. ◦ Conduct a forensic review of events leading to a data leak incident. Learn more about mitigating insider threat here: Seven Tanium Use Cases for Mitigating Insider Threat. • Tanium Discover identifies and allows organizations to classify unmanaged, Bring Your Own Device (BYOD), and shadow IT in an organization's environment in real-time. • Tanium Reveal can locate, categorize, and manage personally identifiable information (PII), personal health information (PHI), and sensitive project keywords in a wide variety of common file formats on Windows, Mac, and Linux endpoints. • Tanium Integrity Monitor allows organizations to monitor and record registry and file events across operating systems, applications, and log files. The Client Recorder Extension monitors the endpoint kernel and other low-level subsystems to capture a variety of events. As events occur, the Tanium Recorder captures a comprehensive, easy-to-interpret history of the who, what, when, where, and how. Which, can in turn, be monitored with Tanium Integrity Monitor as required. Relevant Tanium Modules: • Tanium Interact • Tanium Discover • Tanium Reveal • Tanium Integrity Monitor • Tanium Threat Response	Tanium Fully Meets This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Network Access Control	With Tanium Risk and Tanium Comply, organizations can integrate Tanium with Cloud Access Security Brokers and Zero Trust Network Access providers such as Cloudflare, Okta, and Google BeyondCorp, to verify that devices connecting to cloud applications and zero trust networks are managed and secure. Relevant Tanium Modules: • Tanium Risk • Tanium Comply	Tanium can address this capability end-to-end with existing partnerships and integrations with companies like Cloudflare, Okta, and BeyondCorp
Enterprise Encryption	• Tanium Enforce (Drive Encryption) utilizes BitLocker policies to encrypt drives on endpoints using Windows BitLocker Drive Encryption and FileVault policies to encrypt drives on endpoints using macOS FileVault Encryption. • With Tanium features plus Tanium Risk, organizations can use Tanium sensors to check for insecure SSL or TLS certificates in use on the endpoint. Relevant Tanium Modules: • Tanium Enforce • Tanium Risk	Tanium can partially address this requirement for drive encryption
Mobile Threat Defense	Tanium does not offer this capability at this time.	Tanium Does Not Currently Meet This Requirement

CAL-SECURE TECHNICAL CAPABILITY	TANIUM FUNCTIONALITY	MEETS CAPABILITY?
Unified Integrated Risk Management	Tanium Risk can provide California State Agencies with a data-driven process to objectively assess and score IT risk statewide and at the agency and department level, reduce it to an acceptable level and demonstrate progress to the State CIO and Governor's Office. The Tanium Risk module provides the following features and benefits: • Continuously scans all endpoints and compares them with up-to-the-minute risk intelligence. • Averages the endpoint risk scores into a single score between 0 - 1,000 for the entire environment. The risk score gives a logical, transparent picture of the organization's total risk at all times. • Prioritizes the issues it finds and outlines the next 10 - 20 actions to take to address the biggest threats. • Guides organizations through resolving identified problems and remediating multiple threats in one console. Relevant Tanium Modules: • Tanium Risk	Tanium Fully Meets This Requirement