TRUEFORT™

E-BOOK

How SERVICE ACCOUNT PROTECTION and MICROSEGMENTATION Help Your Business Meet CMMC 2.0 Requirements

+1 201 766 2023 | sales@truefort.com

TRUEFORT.COM

The US Department of Defense (DOD) recently announced an update to its existing Cybersecurity Maturity Model Certification (CMMC), which is a prerequisite in government contracts that may involve sensitive information. Companies competing for government contracts already need to demonstrate CMMC compliance as part of their proposals, and by 2025, 100% of all applicable federal contracts will require it. That leaves little time for organizations to transform security practices if they need to.

Regardless of how your security measures compare to CMMC 2.0 today, two key technologies can help you close the gap quickly. The first is microsegmentation, which helps secure an increasingly vulnerable and diffuse perimeter and minimize the attack surface for modern hybrid and cloud environments. Most organizations will need to implement microsegmentation to meet the CMMC 2.0 standards for Systems and Communications Protection.

And in accordance with the CMMC Identification and Authentication requirements for non-person entities, organizations will need automated processes for finding and protecting service accounts hidden deep in the technology stack. Service accounts are one of the most vulnerable elements of a modern network, and they're notoriously hard to secure and maintain manually. But federal contractors serious about CMMC 2.0 can't ignore them.

About CMMC 2.0

The CMMC model was created to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In response to the recent increase in cyberattacks on the defense industrial base (DIB), the DOD has created CMMC 2.0. It's designed to clarify federal standards for cybersecurity, ensure best-of-breed security practices for contractors on high-priority contracts, and make it easier to demonstrate compliance while maintaining accountability.

The new requirements align with cybersecurity standards set by the National Institute of Standards and Technology (NIST) and other government entities. While the 1.0 version stipulated five levels of compliance, the 2.0 model will utilize three. The first two levels have been published, but the third is still in development. Level 1 has not changed in the new model; still requiring DOD contractors to comply with regulations in the Federal Acquisition Regulation (DAR) document 48 CFR 52.204-1. In Level 2, contractors must comply with all standards described in NIST 800-171B plus 20 additional practices.

The requirements address 14 domains in the first two levels.

Access Control

Organizations must limit internal and external access to systems and information to authorized users and control any information posted for public use.

Awareness and Training

These requirements include training all users and administrators about typical security threats and best practices.

Audit and Accountability

Organizations must be able to log user and system events and generate reports, audits, and reviews to ensure all security systems are working properly and help remediate incidents.

Configuration Management

Security teams must build and maintain security configurations and inventories of organizational systems and implement the principle of least functionality – restricting nonessential programs, functions, ports, and services to minimum necessary operations.

Identification and Authentication

Enterprises meeting these criteria will identify all users, including non-person entities, such as service accounts, and authenticate them for the level of access they're requesting before granting permission.

Maintenance

Security teams will follow safe maintenance processes, including placing controls on tools and personnel, sanitizing equipment going off-site, inspecting media brought in, and supervising all maintenance activities.

Media Protection

Organizations will control and protect any media with secure information, including sanitizing or destroying devices, storage, or hardware no longer in use.

Personnel Security

Personnel should be screened before accessing CUI and prevented from taking or accessing information after transfers or terminations.

Incident Response

Security teams have the capability to detect, analyze, contain, and recover from incidents. The requirements also include reporting and documenting the processes.

Physical Protection

Organizations limit the physical access of systems, equipment, and operating environments to authorized individuals, and monitor the facilities and work sites for unapproved activity.

Risk Assessment

Risk management teams regularly scan for vulnerabilities and assess the risk from security incidents to an organization's mission, operations, and reputation.

Security Assessment

Security teams should periodically assess the effectiveness of controls, correct deficiencies, and monitor operations to ensure controls are working as designed.

System and Communications Protection

Organizations should monitor, control, and protect communications across internal and external network boundaries. Any publicly accessible subnets should be physically or logically separated from internal subnets.

System and Information Integrity

Organizations must protect systems from malicious code, install updates for such protection as needed, and scan any files from external sources for malware.

Many of the standards in each domain will be common practice for most organizations, but some requirements, such as those for System and Communications Protection and Identification and Authentication, present a challenge because of the evolving nature of enterprise networks and applications.

As networks shift to more hybrid, containerized applications relying on multiple microservices and shared resources, it becomes tricky to protect the perimeter with traditional security tools. With modern application deployment practices regularly spawning unmonitored service accounts, organizations have difficulty ensuring that only authorized entities have access to essential data. Faced with these challenges, contractors will find that microsegmentation and service account protection are essential in CMMC compliance.

Microsegmentation Supports the System and Communications Protection Requirements

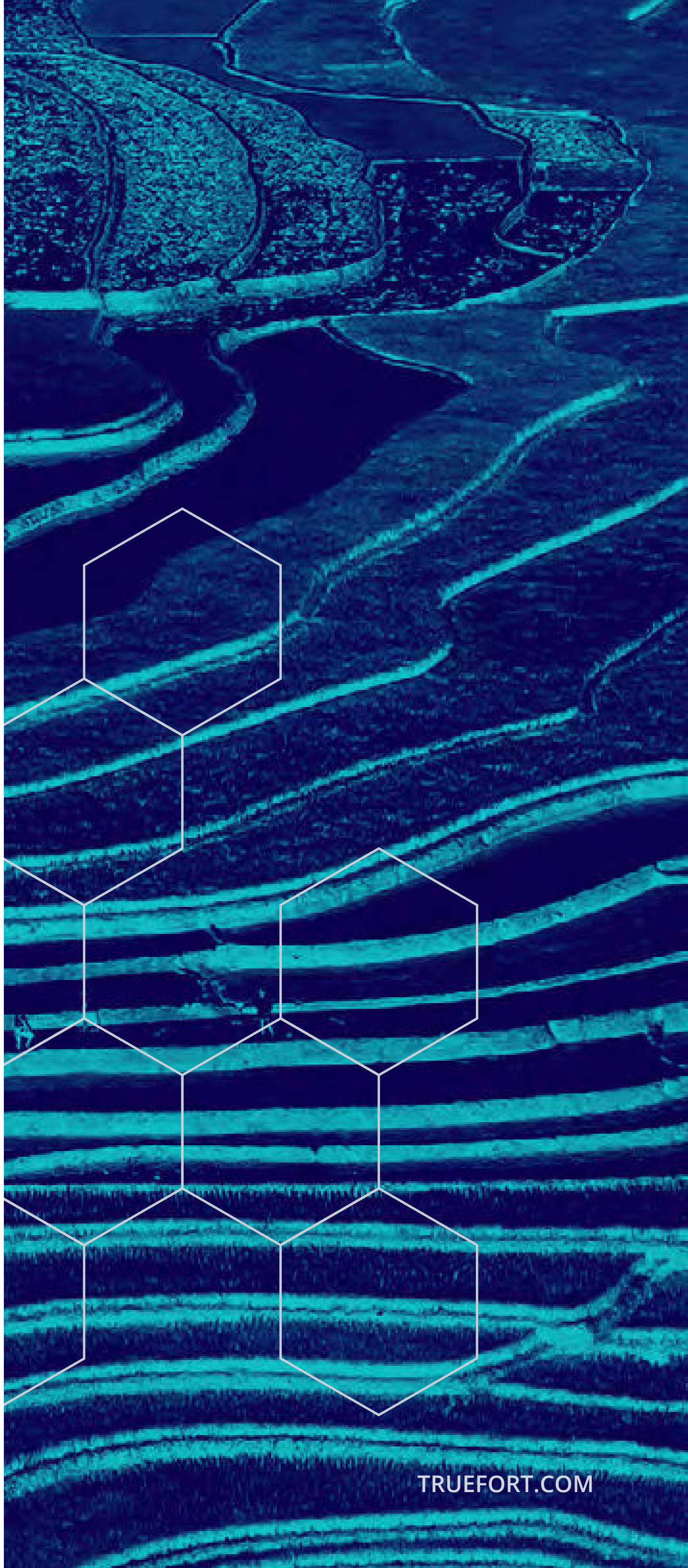
The CMMC requirements for the System and Communications Protection domain address boundary protection, separation of public and private systems, data in transit, and communications authenticity. Microsegmentation supports several of these capabilities by providing a granular level of protection and access control. For example, CMMC requires that organizations "implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks."

The CMMC regulation is designed to prevent malicious actors from getting inside a relatively open network, such as a consumer-facing website, and then moving laterally to other systems containing sensitive data. With the complexity of today's networks, it's extremely difficult to manage that kind of east-west traffic without granular security controls. Microsegmentation ensures that users (human or system) can access only workloads and data necessary and appropriate to their level of authentication and privilege. It logically separates any public workload from a private one, but it also controls data flow between systems as applications communicate with supporting services.

Microsegmentation picks up where traditional network segmentation falls short. Segmenting and protecting networks with gateways, firewalls, and routers no longer meets the demands of cloud and hybrid networks. Security teams need fluid and fine-grained control down to the workload level where policies can be customized by application and service. Acknowledging this new reality, reference architectures published by NIST and the DOD, which have informed the CMMC standard, identify microsegmentation as essential for effective network safety and Zero Trust security.

Microsegmentation Supports Additional CMMC Domains.

Microsegmentation also supports other CMMC requirements. For example, Level 2 standards for the Access Control domain demand implementation of least privilege access for users and devices. Workload-based security controls ensure that users who need to reach specific systems and data can do so, and all others are prevented from getting in, regardless of where the applications and data



reside in the network. As a result, organizations can meet Access Control requirements for remote and mobile device access as well.

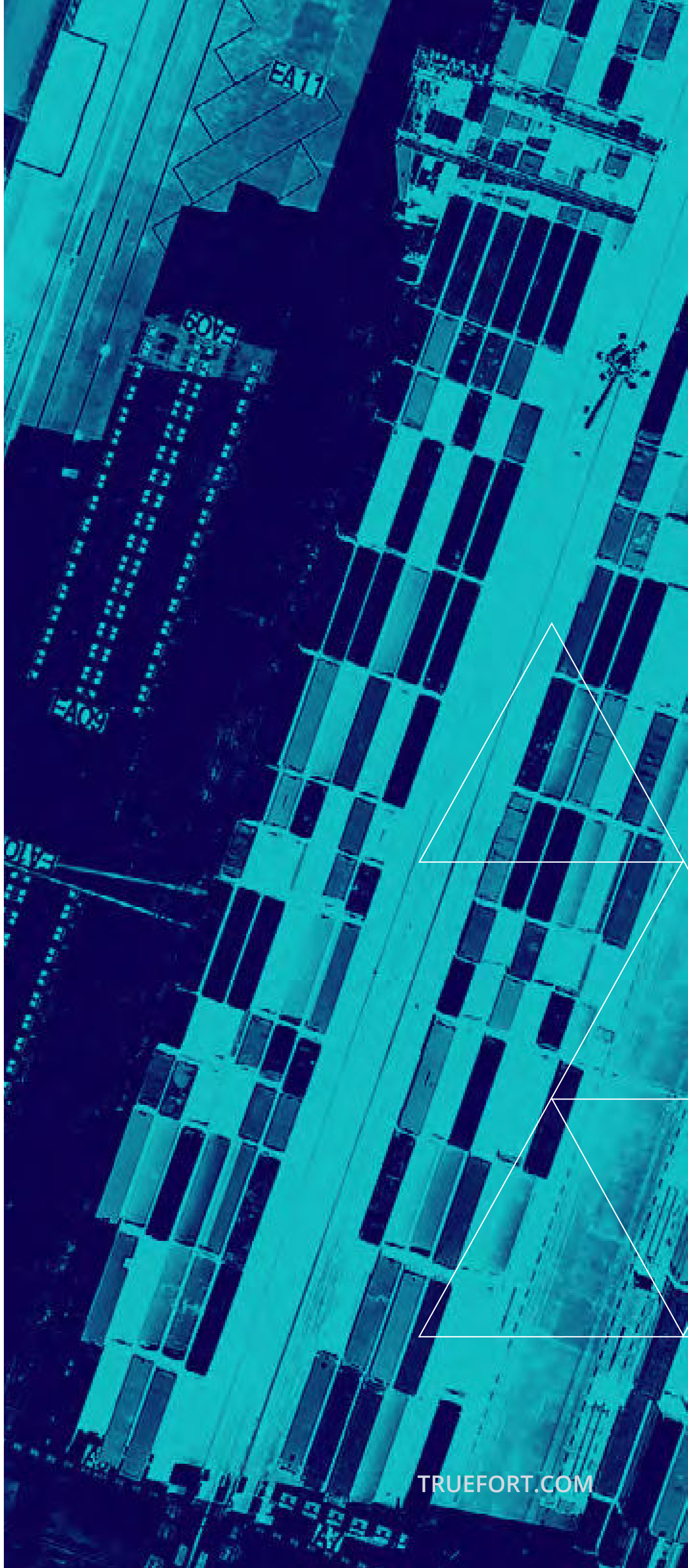
Microsegmentation provides the level of visibility needed for the Incident Response domain, which addresses the detection, analysis, containment, recovery, and reporting of incidents. Controls that monitor east-west traffic are also collecting data on each event which organizations can use for extremely detailed reporting and auditing as well as faster detection of incidents.

Security teams can use the network visibility of microsegmentation to monitor traffic real-time for suspicious behavior as required for Level 2 certification in the System and Information Integrity domain, which specifies that organizations must monitor communications for attacks. With workload-level communications data from microsegmentation, organizations can use machine learning to build a baseline of normal behavior and compare it to current activity, making anomalous behavior easy to identify and investigate.

Efficient Microsegmentation Relies on Intelligent Automation.

Implementing microsegmentation may entail major changes in security infrastructure, so organizations employing this technology to quickly become CMMC compliant should consider using intelligent automation to speed the process. As a first step to microsegmentation, security teams need to inventory all devices, applications, and workloads running in the network and map the dependencies between them so they can understand what resource each entity needs to access. An automated solution will speed up the laborious mapping process considerably.

With a complete dependency mapping, security teams can develop authorization and authentication controls and policies for individual workloads or groups of workloads to manage data access without hampering normal operations. Automation helps generate these policies and update them on the fly. Software agents installed on each workload can enforce security policies and provide visibility at the workload level.



Standards for Identification and Authentication Demand Service Account Discovery and Mapping

The CMMC domain Identification and Authentication requires control over all users accessing the system, including devices, and "processes acting on behalf of users." Those processes include service accounts, which are like user accounts for devices or applications instead of humans. They fall into NIST's category of non-person entity, and because they have the credentials to access systems, applications, and data, they must be identified and authenticated like any other user. If service accounts are left out of the identification and authentication process, it doesn't matter how good humans are at avoiding phishing attempts and maintaining strong passwords – adversaries will just use service accounts to get around them.

Service accounts are usually created during a product install or deployment. Modern applications use these accounts to automate access to data or systems they depend on to function properly. From a business point of view, they're extremely useful, and as applications rely more and more on microservices, these accounts will continue to proliferate.

Unfortunately, securing service accounts is challenging because they don't belong to a specific person, they're often created with a default password that isn't updated, and once they're in place, it's easy to forget about them. As TrueFort's co-founder Sameer Malhotra, explains for Forbes, "In short, service accounts are a hacker's dream. They're buried deep within technology stacks, aren't monitored, have non-expiring passwords, provide access to critical services and valuable data, and they're everywhere."

Automated service account protection speeds discovery and ensures compliance.

To meet the CMMC requirements for identification and authentication, organizations need to inventory and identify service accounts to control their access to systems and data. The difficulty is in finding them and mapping dependencies between operational applications and their associated service accounts.

Technology that can automatically discover, and map service accounts will make this task manageable. It will also support long-term maintenance by spotting unowned “orphaned” accounts, tracking the activity of specific accounts, and identifying account owners. Once organizations have visibility into service account dependencies and activity, they can use machine learning to create a baseline of normal traffic for each account and monitor for unusual patterns that could indicate a malicious attack.

Service account protection supports other CMMC domains.

Visibility and tracking of service accounts also help security teams meet other CMMC standards. For example, service account data can be used to meet Audit and Accountability domain requirements, both for reporting account activity, remediating any incidents involving service accounts, and identifying the owners of each account. Understanding how each account interacts with other systems and data sources will help risk experts’ complete vulnerability scans for the Risk Assessment domain requirements, especially when new systems or applications are deployed.

TrueFort Offers Essential CMMC Capabilities in One Solution

For contractors working toward CMMC 2.0 compliance, TrueFort solutions help satisfy standards in two of the most challenging domains, System and Communications Protections and Identification and Authentication.

TrueFort solutions simplify and expedite the implementation of microsegmentation and deliver results in just a few hours:

- Logical management of access at the workload level
- Application visibility
- Application mapping
- Traffic flows and dependencies between applications

With real-time behavioral data and traffic patterns, TrueFort automates policy generation, identifies suspicious activities, speeds investigations, enables automated policy enforcement, and provides detailed reporting for audits.

For the management of slippery service accounts, TrueFort provides

- Automatic discovery
- Automatic service account dependency mapping
- Service account owner identification
- Orphaned account identification
- Service account inventory by environment
- Visibility into how often service accounts are used

For both microsegmentation and service account management, TrueFort employs best-of-breed workload behavioral analysis, machine learning, and automation to help contractors meet the demanding CMMC 2.0 standards and secure their technical infrastructure in an efficient, flexible, and cost-effective manner.

FIND OUT how TrueFort can work for you.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM