COMPARISON MATRIX

Fortinet Solutions for CMMC

Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) is intended as a comprehensive framework for how cybersecurity solutions are implemented across more than 300,000 companies involved in the U.S. defense industrial base supply chain. CMMC v1.01 was released on January 31, 2020, and is the U.S. Department of Defense's (DoD) stepped-up requirement for keeping DoD information accessed by or housed in contractors' technology environments secure.

Previously, contractors supporting DoD had responsibility for assessing and self-certifying their success implementation, monitoring, and maintaining the security of any sensitive DoD information stored or accessible from their IT systems. The big change with CMMC is that the DoD will require third-party-governed assessments of how those contractors comply with best practices intended to protect data from cyber adversaries and prevent successful breaches. Details on how assessments will be conducted are still forthcoming as of July 2020, but all DoD contractors must understand the CMMC's technical requirements and prepare for certification, or risk eligibility to participate in DoD contracts, each of which will be tied to one or more CMMC levels.

Specifically, CMMC includes five certification levels intended to highlight a company's cybersecurity maturity and resilience levels—and therefore, a reflection of how effectively it can protect sensitive government information. Fortinet solutions for government are well-positioned to meet CMMC standards at all levels.

CMMC Capability	Practices	Fortinet Solution
MC01 Improve [DOMAIN NAME] activities	ML.2.998, ML.2.999, ML.3.997, ML.4.996, ML.5.995	**Fortinet Consulting Service** Fortinet consulting service team can help customers develop security plans to meet requirements as applicable to NIST 800-53, 800-171, and CSF.
C001 Establish system access requirements	AC.1.001, AC.2.005, AC.2.006	**FortiGate** FortiGates running FortiOS 6.4 now support Network access control (NAC) helps administrators implement policies to control the devices and users that have access to their networks. A NAC policy can use user or detected device information, such as device type or OS, to put traffic into a specific VLAN or apply specific port settings. FortiGate also supports a customizable captive portal per-interface and per-policy, which can be configured with custom disclaimers for privacy and security notices. **FortiNAC** FortiNAC assists with bring-your-own-device (BYOD) policies and a means to safely accommodate headless IoT devices in the network. FortiNAC enables three key capabilities to secure IoT devices: ■ Network visibility to see every device and user as they join the network. ■ Network control to limit where devices can go on the network. ■ Automated response to speed the reaction time to events from days to seconds.
C002 Control internal system access	AC.1.002, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.3.012, AC.3.017, AC.3.018, AC.3.019, AC.3.020, AC.4.023, AC.4.025, AC.5.024	**FortiGate** FortiGate identity and application aware policies limit activity between authorized users and applications to only permitted activity. FortiGate can also capture packets and other forensic data when a violation occurs. FortiGate device-based policies control how mobile device connect and where they can go on the network. **FortiGate/FortiWiFi/FortiAP** Fortinet wireless technologies can deploy DTLS to encrypt the data channel and EAP-TLS to provide PKI authentication between Wi-Fi clients and authentication server. FortiGate wireless technologies can perform monitoring of rogue APs and actively prevent users from connecting to them. When suppression is activated against an AP, the FortiGate WiFi controller sends deauthentication messages to the rogue AP's clients, posing as the rogue AP, and also sends deauthentication messages to the rogue AP, posing as its clients. **FortiNAC** FortiNAC assists with bring-your-own-device (BYOD) policies and limit where devices can go on the network. **FortiSIEM** FortiSIEM provides complete detail of user's access to resources from across all devices and applications. **FortiAuthenticator** FortiAuthenticator account policies can enable user account lockout for failed login attempts based on maximum number of allowed failed attempts. FortiAuthenticator account policies can terminate sessions after organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

CMMC Capability	Practices	Fortinet Solution
C003 Control remote system access	AC.2.013, AC.2.015, AC.3.014, AC.3.021, AC.4.032	**FortiGate** FortiGate as the remote access concentrator manages all sessions and can provide layer 7 inspection over all activity from remote access users to protected resources. The FortiGate operating system, FortiOS, undergoes FIPS validation for every minor release. Additionally, all FortiGate models are FIPS affirmed so customers have the ability to choose any model in the portfolio. The FIPS validated crypto is used in both management and data plane communications e.g. HTTPS, IPSec VPN, SSL VPN, etc. FortiGate as the remote access concentrator includes the ability to execute remote user posture validation and take into account users' risk factors from external threat intelligence sources. FortiGate supports AAA to strictly define the commands that users are authorized to access. FortiGate dynamic DNS allows customers to advertise remote access control points easily to remote users.
C004 Limit data access to authorized users and processes	AC.1.003, AC.1.004, AC.2.016	**FortiGate** FortiGate identity and application aware policies limit activity between authorized users and external applications to only permitted activity. FortiGate data leak prevention can ensure that CUI does not get transmitted in unauthorized flows.
C006 Manage asset inventory	AM.4.226	**FortiGate** FortiGate device inventory allows FortiOS to monitor networks and gather information about devices operating on those networks, including MAC and IP addresses, operating systems, hostnames, and usernames. **FortiSIEM** FortiGate device inventory allows FortiOS to monitor networks and gather information about devices operating on those networks, including MAC and IP addresses, operating systems, hostnames, and usernames.
C007 Define audit requirements	AU.2.041, AU.3.046	**FortiGate** FortiGate logs individual activities to the system event log. **FortiAuthenticator** FortiAuthenticator can identify network users, processes on systems to be used for non-repudiation accountability tasks. **FortiSIEM** FortiSIEM can alert if any systems report a failure on audit logging processes.
C008 Perform auditing	AU.2.042, AU.2.043, AU.3.048, AU.5.055	**FortiGate** FortiGate can leverage authenticated and trusted NTP servers to synchronize internal clocks for audit log time stamping. **FortiSIEM** FortiSIEM is a central repository of all audit logs for systems and endpoints allowing administrators to leverage the automated correlation of activity to determine unlawful or unauthorized activity. FortiSIEM can alert if any systems report a failure on audit logging processes
C009 Identify and protect audit information	AU.3.049, AU.3.050	**FortiGate** Audit tool configuration and files are not modifiable by system users. System users are only granted access to modify their view of the tools' outputs. **FortiSIEM** FortiSIEM role-based access control (RBAC) can granularly specify which users have access to which information.

CMMC Capability	Practices	Fortinet Solution
C010 Review and manage audit logs	AU.3.051, AU.3.052, AU.4.053, AU.4.054	**FortiGate** FortiGate can specify exact audit log generation to support on-demand. **FortiSIEM** FortiSIEM is a central repository of all audit logs for systems and endpoints allowing administrators to leverage the automated correlation of activity to determine unlawful or unauthorized activity. FortiSIEM provides an easy reporting interface that makes reviewing audit information from all systems on the network very easy.
C012 Conduct training	AT.2.057	**Fortinet ASE Training** Fortinet NSE Training enables personnel from novice to senior level to learn how to execute duties related to infosec daily operation, incident handling, and service enhancement.
C013 Establish configuration baselines	CM.2.061, CM.2.062, CM.2.063	**Fortinet Security Fabric Products** Fortinet products support role-based access that specifies exactly what each user can execute in order to enable a least-privilege posture. **FortiSIEM** FortiSIEM CMDB collects and maintains the baseline configurations and inventories of all endpoints. The CMDB can be used to provide real-time alerts to changes and report on changes throughout system lifecycles. **FortiClient/FortiClient EMS** FortiClient Software Inventory Management provides visibility into installed software applications and license management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.
C014 Perform configuration and change management	CM.2.064, CM.3.068, CM.3.069, CM.4.073	**FortiGate** Fortinet Security Rating and Department of Defense STIGs provide secure configuration guidance. **FortiClient/FortiClient EMS** FortiClient Software Inventory Management provides visibility into installed software applications and license management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface. **FortiEDR** FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to: ▪ Track applications and ratings ▪ Discover and mitigate system and application vulnerabilities with virtual patching
C015 Grant access to authenticated entities	IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.2.082, IA.3.083, IA.3.084, IA.3.085, IA.3.086	**FortiAuthenticator** FortiAuthenticator can identify users through a varied range of methods and integrate with third-party LDAP or Active Directory systems to apply group or role data to the user and communicate with FortiGate for use in Identity- based policies. Additionally, FortiAuthenticator could also be used for 802.1X implementations with Fortinet and 3rd party network devices. FortiAuthenticator extends two-factor authentication capability to multiple FortiGate appliances and to third party solutions that support RADIUS or LDAP authentication. FortiAuthenticator user account policies provide restrictions on password complexity and password reuse. FortiAuthenticator can discard stale authentication requests to prevent replay

CMMC Capability	Practices	Fortinet Solution
		attacks. FortiAuthenticator user database can allow for a temporary password requiring an immediate change to a permanent and confidential password. FortiAuthenticator stored password data is cryptographically hashed and salted. Transmitted password data can be protected by using the secure versions of authentication protocols e.g. LDAPS. **FortiToken** FortiToken combines user identity information from FortiAuthenticator and ensures that only authorized individuals are granted access to designated resources.
C016 Plan incident response	IR.2.092, IR.4.100, IR.5.106	**FortiSOAR** FortiSOAR facilitates efficient investigation of alerts through automated workflows, that can include manual intervention, allowing security analysts to neutralize threats quickly and gain visibility into the bigger picture and understand trends. FortiSOAR aggregates these alerts in one place while enriching them with added context to speed investigations. FortiSOAR streamlines simple SOC tasks such as alert ingestion, prioritization based on severity levels, assigning tasks, and subroutines and automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.
C017 Detect and report events	IR.2.093, IR.2.094	**Fortinet Security Fabric Products** Fortinet Security Fabric products provide advanced inspection capabilities to detect and report on interesting events. **FortiSOAR** FortiSOAR aggregates these alerts in one place while enriching them with added context to speed investigations. FortiSOAR streamlines simple SOC tasks such as alert ingestion, prioritization based on severity levels, assigning tasks, and subroutines and automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.
C018 Develop and implement a response to a declared incident	IR.2.096, IR.3.098, IR.4.101, IR.5.102	**FortiSOAR** FortiSOAR facilitates efficient investigation of alerts through automated workflows, that can include manual intervention, allowing security analysts to neutralize threats quickly and gain visibility into the bigger picture and understand trends. FortiSOAR aggregates incident alerts in one place while enriching them with added context to accelerate time to resolution. It also helps reduce the number of “false-positive” alerts and provides advanced case management functions that help to define, guide, and speed investigations. All activities can be reported to designated individuals or organizations. FortiSOAR simplifies SOC complexity by integrating disparate point security solutions into a centralized orchestration system that can be deployed in virtually any environment. This enables even the smallest of SOC teams to centralize their entire security process and to respond with all their current tools, which results in faster real-time response.
C019 Perform post incident reviews	IR.2.097	**FortiSOAR** FortiSOAR aggregates these alerts in one place while enriching them with added context to speed investigations. FortiSOAR streamlines simple SOC tasks such as alert ingestion, prioritization based on severity levels, assigning tasks, and subroutines and automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.

CMMC Capability	Practices	Fortinet Solution
C021 Manage maintenance	MA.2.111, MA.2.112, MA.2.113, MA.3.115	**Fortinet Security Fabric Products** Fortinet maintenance capabilities allow for direct or centrally managed maintenance operations. Fortinet devices support role-based access control to ensure that only authorized personnel can perform maintenance on Fortinet systems. Fortinet devices support deleting CUI data and defined overwrites to sanitize devices of CUI. **FortiGate** FortiGate remote access VPNs support native multifactor authentication to include but not limited to one-time password (OTP) tokens and user certificates with PKI, CAC, or PIV. FortiGate can also integrate with external authentication platforms that are integrated with additional authentication repositories. **FortiToken/Mobile/Service** The service encompasses everything needed to implement two-factor authentication in the FortiGate environment including the FortiToken Mobile app with push technology, simplifying the end-user two-factor experience to a swipe or click to accept.
C024 Sanitize media	MP.1.118	**FortiGate** Fortinet Secure RMA service supports customers that cannot return replaced hardware due to physical data protection requirements.
C029 Manage backups	RE.3.139	**FortiManager** FortiManager performs regular and incremental backups of FortiGate configurations allowing FortiGates to be restored with ease. **FortiAnalyzer** FortiAnalyzer performs regular backups of traffic logs and network audit data. These backups can also be rolled and archived to long-term storage over the network.
C030 Manage information security continuity	RE.5.140	**Fortinet Security Fabric Products** Fortinet Security Fabric Products support many configurations that enable high-availability and continuity.
C031 Identify and evaluate risk	RM.2.142, RM.4.149, RM.4.150, RM.4.151	**Fortinet Security Fabric** Fortinet security devices are designed to allow sharing of IOCs with each other and 3rd party tools, as well as leverage IOCs from external resources. **FortiSandbox** FortiSandbox displays malware techniques and tactics cross-referenced with the MITRE ATT&CK matrix to enable analysts to quickly familiarize with adversary methodologies. **FortiGuard Penetration Testing Service** FortiGuard Pentest Team offers assessments of external and internal vulnerabilities, and web and mobile applications penetration testing. The team also provide as a report of security shortfalls in the network and provides guidance on remediation procedures.
C032 Manage risk	RM.3.146, RM.5.155	**FortiGuard Penetration Testing Service** FortiGuard Pentest Team offers assessments of external and internal vulnerabilities, and web and mobile applications penetration testing. The team also provide as a report of security shortfalls in the network and provides guidance on remediation procedures.

CMMC Capability	Practices	Fortinet Solution
C034 Develop and manage a system security plan	CA.2.157, CA.4.163	**Fortinet Consulting Service** Fortinet consulting service team can help customers develop security plans to meet requirements as applicable to NIST 800-53, 800-171, and CSF.
C035 Define and manage controls	CA.2.158, CA.2.159, CA.3.161, CA.4.164, CA.4.227	**Fortinet Consulting Service** Fortinet consulting service team can help customers assess security control effectiveness in meeting requirements as applicable to NIST 800-53, 800-171, and CSF. **FortiGuard Penetration Testing Service** FortiGuard Pentest Team offers assessments of external and internal vulnerabilities, and web and mobile applications penetration testing. The team also provide as a report of security shortfalls in the network and provides guidance on remediation procedures.
C036 Perform code reviews	CA.3.162	**FortiGuard Penetration Testing Service** FortiGuard Pentest Team offers assessments of external and internal vulnerabilities, and web and mobile applications penetration testing. The team also provide as a report of security shortfalls in the network and provides guidance on remediation procedures.
C038 Define security requirements for systems and communications	SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.186, SC.3.187, SC.3.188, SC.3.189, SC.3.190, SC.3.191	**Fortinet Security Fabric Devices** Fortinet Security Fabric devices store CUI data on encrypted storage. **FortiGate** The FortiGate operating system, FortiOS, undergoes FIPS validation for every minor release. Additionally, all FortiGate models are FIPS affirmed so customers have the ability to choose any model in the portfolio. FortiGate can be deployed to provide isolation on any segment of the network. This flexibility is due to the FortiGate ability to operate as both a layer 2 and layer 3 segmentation firewall. FortiGate Security Rating audits the network configuration to ensure that CIS controls are adhered to in the design. The FortiGate layer 7 inspection can prohibit remote activation of collaborative applications to any device. FortiGate can record packets that trigger firewall rules or security inspection matches. The FortiGate VPN for site-to-site and remote-access users can provide the security required for management of network devices. FortiGate can prevent split tunneling and force all communication from remote SSL VPN users including traffic to the Internet uses an SSL VPN tunnel between the user's PC and the FortiGate unit. Connections to the Internet are routed back out the FortiGate unit to the Internet. Replies from the internet come back into the FortiGate unit before being routed back through the SSL VPN tunnel to the remote user. FortiGate enforces strict compliance with ports and protocols as both a layer 2 and layer 3 segmentation firewall. FortiGate can logically or physically isolate management plane and data plane functionality within the system with role-based access control and through the system with virtual domain (VDOM) technology. FortiGate Data Leak Prevention (DLP) can be used to define sensitive data patterns, and data matching these patterns will be blocked, or logged and allowed, when passing through the FortiGate unit. FortiGate session idle timers can be configured close communications after inactivity on a per port or application basis providing granular control of network behavior. The FortiGate allows for cryptographic key management from the central management system, FortiManager, and directly on the FortiGate via GUI, CLI, and API with automated 3rd party DevOps tools. FortiGate Mobile Security Service employs advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and gaining access to its invaluable information. FortiGate offers advanced VOIP protection and performs Deep SIP message inspection for SIP statements. FortiGate mechanisms such as strict-header checking for anti-spoofing protection and certificate inspection ensure that illegitimate entities are not communicated through the device.

CMMC Capability	Practices	Fortinet Solution
		FortiNAC FortiNAC device profiles can isolate collaborative computing devices at the access layer. **FortiEDR** FortiEDR can prevent collaborative processes from executing. **FortiClient** FortiClient thick client VPN enables SSL and IPsec VPN to manage network devices over the network. **FortiAnalyzer** FortiAnalyzer can archive recorded packets on long-term storage for examination by SOC personnel.
C037 Implement threat monitoring	SA.3.169, SA.4.171, SA.4.173	**Fortinet Security Fabric Products** Fortinet security devices are designed to allow sharing of IOCs with each other and 3rd party tools, as well as leverage IOCs from external resources. Fortinet security devices can also communicate to stakeholders when new IOCs are received. **FortiGate** FortiGate automation stitches can dynamically respond to IOCs received from external resources. **FortiSIEM with FortiInsight Subscription** Powered by its discovery capabilities, FortiSIEM can seamlessly collect a rich variety of performance and availability metrics to help the investigator hunt for threats from zero day malware. FortiSIEM can also alert when the metrics are outside of normal profile and can correlate such violations with security issues to create high fidelity alerts. FortiSIEM remediation scripts are out-of-the-box tools to automate response to IOCs with Fortinet or 3rd party security tools. FortiInsight provides rich access to the record of events that are streaming in from endpoints. Analysts are able to investigate events using broad search or summary tables to find more detailed information about events.
C039 Control communications at system boundaries	SC.1.175, SC.1.176, SC.3.192, SC.3.193, SC.4.199, SC.4.202, SC.4.229, SC.5.208	**FortiGate** FortiGates filter network traffic to protect an organization from external threats. Features include stateful packet filtering, network monitoring, IP mapping features, and deep inspection to identify attacks, malware, and other threats. FortiGate can be deployed to create subnetwork and isolate them from any segment of the network. This flexibility is due to the FortiGate ability to operate as both a layer 2 and layer 3 segmentation firewall. FortiOS Web Filtering solution utilizes FortiGuard Web Filtering Services with superior coverage of over 250 million rated websites. The FortiGate DNS filter can allow, block, or monitor access to web content according to FortiGuard categories. Once organizational policy is defined, FortiGate Data Leak Prevention (DLP) can be used to define sensitive data patterns, and data matching these patterns will be blocked, or logged and allowed, when passing through the FortiGate unit. The FortiGate natively uses the FortiGuard threat intelligence database containing a list of known malicious domains, botnet command and control (C&C) addresses. This database is updated dynamically and stored on the FortiGate. FortiGate can be used to protect internally defined boundaries and automation stitches to dynamically prevent threat identified by organizational personnel. FortiGate Mobile Security Service employs advanced detection engines to prevent both new and evolving threats. FortiGate can also leverage FortiSandbox for further analysis.

CMMC Capability	Practices	Fortinet Solution
		FortiSandbox FortiSandbox improves zero-day threat detection efficacy and performance by leveraging two machine learning models—patent-pending enhanced random forest with boost tree and least squares optimization applied to static and dynamic analysis of suspicious objects. It also accelerates threat investigation and management processes by adopting standards-based on the MITRE ATT&CK framework for malware reporting. The Fortinet automated breach protection strategy enables FortiSandbox to easily integrate across both Fortinet and non-Fortinet products to provide real-time threat intelligence and speed threat response. FortiSandbox analysis also includes malware that targets industrial control systems (ICS) so it can deliver the same sandbox benefits to organizations that manage both Information Technology (IT) and Operation Technology (OT) business segments.
C040 Identify and manage information system flaws	SI.2.214, SI.4.221	**Fortinet Consulting Service** Fortinet security devices are designed to allow sharing of IOCs with each other and 3rd party tools, as well as leverage IOCs from external resources. **FortiSIEM** FortiSIEM remediation scripts are out-of-the-box tools to automate response to IOCs with Fortinet or 3rd party security tools.
C041 Identify malicious content	SI.1.211, SI.1.212, SI.1.213, SI.5.222	**FortiGate** FortiGate Antivirus protects against the latest viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and accessing its invaluable content. FortiGate antivirus keeps protections up-to-date with hourly push updates. Updates may also be manually uploaded in air-gapped networks. FortiGate can apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions, and with SSL/SSH content scanning and inspection, FortiGate can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions. **FortiSIEM** Powered by its discovery capabilities, FortiSIEM can seamlessly collect a rich variety of performance and availability metrics to help the investigator hunt for threats from zero day malware. FortiSIEM can also alert when the metrics are outside of normal profile and can correlate such violations with security issues to create high fidelity alerts.
C042 Perform network and system monitoring	SI.2.216, SI.2.217, SI.3.218, SI.5.223	**FortiGate** FortiGate can be deployed to provide isolation on any segment of the network. FortiGate layer 7 inspection capabilities provide insight into payloads that allow detection potential attacks and indicators of compromise. FortiGate email filtering techniques use FortiGuard services to detect the presence of spam among your email. Capabilities include: ■ IP Address Check ■ URL Check ■ Detect Phishing URLs in Email ■ Email Checksum Check ■ Spam Submission

CMMC Capability	Practices	Fortinet Solution
		FortiMail FortiMail units can use various methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, Bayesian scanning, and heuristic scanning. **FortiSIEM** FortiSIEM provides ongoing monitoring and automated correlations of user and system activity to detect anomalous behavior. FortiSIEM alerts dashboard and emails quickly bring unauthorized attempts of system use to the attention of SOC personnel.
C043 Implement advanced email protections	SI.3.219, SI.3.220	**FortiMail** FortiMail provides numerous protections against email forgery to include inbound email marking and DMARC protections built on SPF and DKIM. **FortiSandbox** FortiSandbox can be utilized as an MTA to inspect malware in email or via security fabric connection, integrated with FortiGate or FortiMail to analyze malware in emails.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 9, 2021 11:45 AM

744564-0-0-EN

D:\Fortinet\2020 Old templates\Image Graphics\898628 - Typo in CMMC assets\FA-comparison-matrix-cmmc-assets-292021\FA-comparison-matrix-cmmc-assets-292021