SOLUTION BRIEF

Fortinet and METTCARE Integrated Security Solutions

Broad, integrated and automated joint solution for digital ID management & transactional processing

Challenges

Digital transformation is forging the way for corporate data to be accessed from any location and any device at any time. Controlling the access, management and storage of enterprise assets has never been more critical.

Application layer security encompasses a holistic approach to cyber asset protection. Controlling the privacy and security of externally-facing applications in ecommerce, banking, bill payments, eHealth, and from additive manufacturing to government operations and enforcement, each shapes the fabric of everyday activities that cannot afford system disruptions or breaches.

Together, the joint Fortinet Security Fabric and METTCARE solution combines application layer with network security in network, application or mobile environments and cloud, virtualized or physical environments for advanced threat protection, assurance and intelligence.

Joint Solution Description

Fortinet and METTCARE technology partnership brings together the METTCARE Trustus application layer security services with FortiGate enterprise firewall, FortiAuthenticator and FortiToken Mobile to address the cyber challenges of digital identity needs.

How Does It Work?

Trustus Suite of Products (TrustusSP) provides secure storage for digital assets and crypto keys used in all application based cryptographic events. A weakness of many certificate authorities and password vaults is the inability to prevent theft of crypto keys and passwords by rogue actors (internal and external). Trustus provides a next-generation repository that safely secures these vulnerabilities by providing an untouchable, secure database for storing all authentication data, irrespective of the source and purpose.

The integrated solution leverages the METTCARE Trustus certificate authority (CA), virtual tokens (VT), multi-factor authentication (MFA) and end-user single-sign-on (SSO) application layer products for preventing infiltration malicious attempts on protected assets. In the absence of consent of use, Trustus blocks access to protected critical data and FortiGate firewalls block access to network assets.

TrustusSP compliments Fortinet products with pioneering cryptographic FIPS 140-2 certified software, quantum and 5G ready, with SS7 flaw vulnerabilities removed. Digital certificates, VT, and MFA are applied to every component of digital identify profiles; comprised of users' attributes (names, date of birth, SSN, network login, passwords, PINs), server and machine attributes, mobile devices' attributes, routines, programs, events, etc.

Privacy is embedded into the Trustus framework as the default setting for all Trustus application layer cybersecurity; anticipating the risks and resolving privacy invasive events before they occur: (1) proactive design, not reactive response, (2) preventative actions not remediation, and (3) audit and privacy compliance under GDPR, SOX, Cloud Act (2018), HIPAA, PCI, as well as local regulations.

Solution Components

Fortinet Security Fabric – FortiGate, FortiAuthenticator, FortiClient, FortiToken Mobile

METTCARE - TrustusCA, TrustusDI, TrustusMFA, TrustusSSO, TrustusVT, TrustusE2EP, TrustusEDS

Joint Benefits

- Organizations gain from one-stop all-in product and service provisioning
- Enterprise assets and data protected against elusive cyberattacks, including malwares and intrusions
- Sensitive data is concealed in randomized repositories to prevent information leaks of metadata, transactions and document information
- Unified digital certificates and virtual tokens for devices, programs, events and persons
- Leveraged third party risk mitigation minimizes exposure of shared sensitive data. Data owner inherent rights protected and data territoriality preserved
- Application security and firewalls protect and extend the lifecycle of legacy systems

FORTINET Fabric-Ready

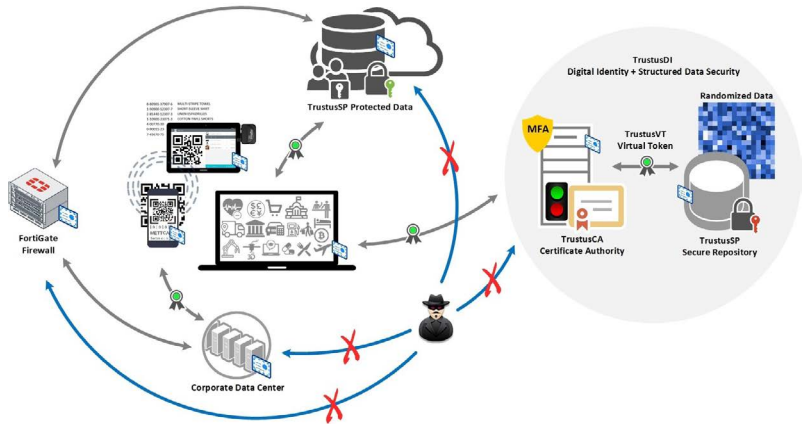

Figure 1: Structured Application Layer Defense for Secure Transactional Data.

Use Case 1: Beyond Bot Attacks and Vulnerability Exploits

Events, actions, programs, and records on the application layer are locked and hidden from intruders by TrustusSP. Once access to critical data is legitimately granted (Trustus knows who, what, where, when and how), TrustusCA digital certificates and TrustusVT virtual tokens secure the data from edge to storage, permitting business as usual irrespective of the growing threat landscape. Under attack, FortiGate firewalls block network access and TrustusEDS renders critical assets impermeable.

Use Case 2: Secure Access Controls

VPN, MFA and SSO secure access credentials need protection. TrustusCA and TrustusEDS provide additional layers of security with FortiClient. TrustusCA digital certificates add functionality to FortiAuthenticator remote-location VPN, for more secure and flexible user connectivity. TrustusCA certificate deployments offer impermeable security with MFA and SSO, with PKI managed by Trustus.

METTCARE Product Description

METTCARE TrustusSP structured products comprise TrustusCA (certificate authority), TrustusDI (digital identity), TrustusMFA (multi-factor authentication), TrustusSSO (single-sign-on), TrustusVT (virtual token), TrustusE2EP (end-to-end protection) and TrustusEDS (enterprise data store). For optimal security and data protection, TrustusSP API and enterprise centric integration with FortiGate, FortiAuthenticator and FortiToken Mobile is recommended.

TrustusCA ensures user digital certificates issued by TrustusCA are not compromised. TrustusDI grants identified parties (individuals, organizations, hardware, and software) reliable multi-faceted digital identities. TrustusMFA authentication protects against fake cyber logins. TrustusSSO online/mobile come-back logins deliver complete trust and integrity. TrustusVT one-time use software tokens return absolute user session security and privacy. TrustusE2EP communication between parties (senders and receivers) permit access and data movement without security or privacy risk. TrustusEDS pioneering hybrid-cloud-storage protects transactional and content data rendering it meaningless to the unintended and unauthorized.

FortiGate: Next-Generation Firewall

FortiGate enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the cloud. FortiGate enterprise firewalls leverages purpose-built security processors (SPUs) that delivers scalable performance of advanced security services like Threat Protection, SSL inspection, and ultra-low latency for protecting internal segments and mission critical environments.

FortiGate NGFW provides automated visibility into cloud applications, IoT devices and automatically discovers end to end topology view of the enterprise network. FortiGate is a core part of security fabric and validated security protect the enterprise network from known and unknown attacks.

About METTCARE

METTCARE digital identity, data security, application layer protection and vulnerability management bring a new level of trust to our users by authenticating people, machines, and transactions from devices to the cloud, across industries as diverse as payment processing, eHealth, and manufacturing to government services. We create value with every transaction and asset we protect, up-ending how cybersecurity and privacy should be delivered in a connected world for maximum effect. Learn more at www.mettcare.com.

FORTINET

www.fortinet.com

October 16, 2019 1:00 AM

513323-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Mettcare\sb-FA-fortinet-and-mettcare-integrated-security-solutions