

QTrust Server

Multilevel UTM-Appliance

STRATEGIE



We know the difference.

- Reduzierung von Komplexität erhöht die Sicherheit.
- Sicherheit versus Funktion – Ein Balance-Akt.
- Sicherheit ist kein kaufbares Feature sondern eine Reihe von aufeinander abgestimmten Prozessen und Lösungen.

QTRUST
SERVER

Der QTrust Server verfolgt eine simple Sicherheitsstrategie:

ANGRIFFSMÖGLICHKEITEN VERHINDERN BZW. REDUZIEREN UND BEI ERFOLGREICHEN ANGRIFFEN DIE NEGATIVEN AUSWIRKUNGEN MINIMIEREN

Inzwischen muss man bei der Komplexität der Anwendungen zwingend davon ausgehen, dass die eingesetzte Software nicht fehlerfrei, d.h. angreifbar ist. Auch gewünschte und notwendige Kommunikation kann für erfolgreiche Angriffe missbraucht werden.

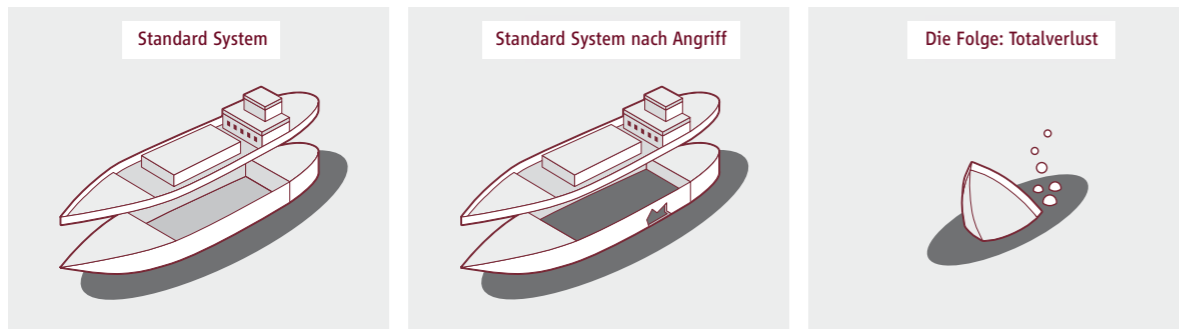
Dabei ist eines der Grundgesetze der Sicherheit nicht zu vernachlässigen:
JE EINFACHER, DESTO SICHERER.

Ziel der Entwicklung war es, ein Produkt zu schaffen, welches den höchsten Sicherheitsanforderungen entspricht, jedoch einfach einzusetzen und zu verwalten ist.

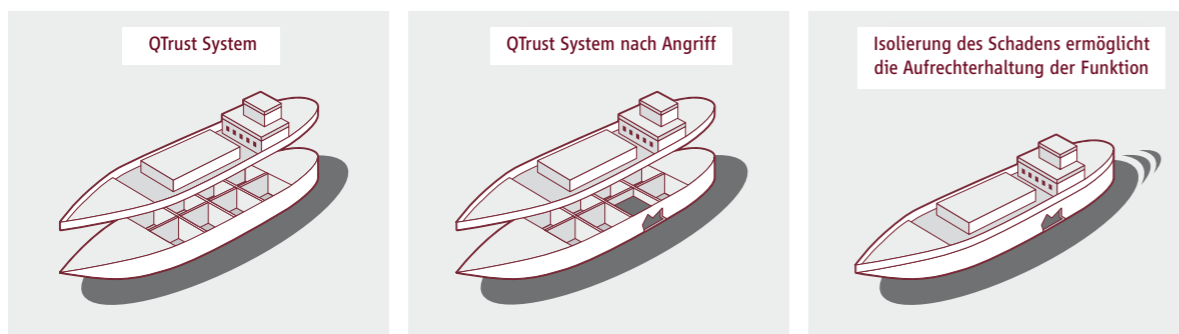
DAS QTRUST PRINZIP

Diese vollständig integrierte Lösung in Form einer Multilevel Security Appliance vereint die wichtigsten Netzwerk-Sicherheitsfunktionen in einem einzigen, leicht zu verwaltenden und hochsicheren System. Dabei wird in mehreren Schichten des ISO/OSI Modells gearbeitet, wobei auf jeder Ebene weitere Sicherheitseigenschaften hinzugewonnen werden.

Beispiel: Standard System



Beispiel: QTrust System



Der QTrust Server übernimmt als Stellvertreter der Zielapplikation die Kommunikation und schützt nach dem Sandboxprinzip die dahinterliegenden Systeme. Das Sandboxprinzip ist vergleichbar mit einem Sandsack, der eine Gewehrpatrone aufhält. Der Angreifer wird durch Absorption unschädlich gemacht. In Zusammenhang mit dem QTrust Server bedeutet dies, dass ein Angreifer, dem es gelingt, eine Applikation auf dem QTrust Server zu übernehmen, keinen unmittelbaren Zugriff auf die eigentlichen Server und die dort gespeicherten Daten erhält. Der QTrust Server übernimmt somit die Aufgaben einer kompletten DMZ (De-Militarisierte-Zone) komprimiert in einem einzigen System. Ermöglicht wird ein gleiches, wenn nicht sogar höheres Niveau an Sicherheit durch die Nutzung einer Technologie, die ein physikalisches System in eine Reihe von getrennten Applikations-Einheiten separiert.

Als Beispiel Mail:

Ein eingebauter Filter erkennt SPAM schon bevor unerwünschte Email auf dem eigentlichen Mail Server ankommt, so werden Mail Server und Anwender entlastet. Ein Virens Scanner erkennt Viren bereits an der Schnittstelle zum Internet, bevor diese in das interne Netzwerk gelangen. Dies schützt das ganze Netzwerk, nicht nur einzelne Rechner.

Im Unterschied zu gewöhnlichen Firewall Systemen verhindert der QTrust Server einen direkten Datenaustausch von außen nach innen – bei allen Konfigurationen ohne Ausnahme. Sämtliche internen Datendienste, die zur Kommunikation mit der Außenwelt vorhanden sind, werden durch den QTrust Server entkoppelt und geprüft. Eine Kommunikation erfolgt nur zwischen QTrust Server und der Außenwelt. Die eigentlichen Datendienste und -quellen, wie z.B. der Mail Server, liegen geschützt hinter dem QTrust Server versteckt.

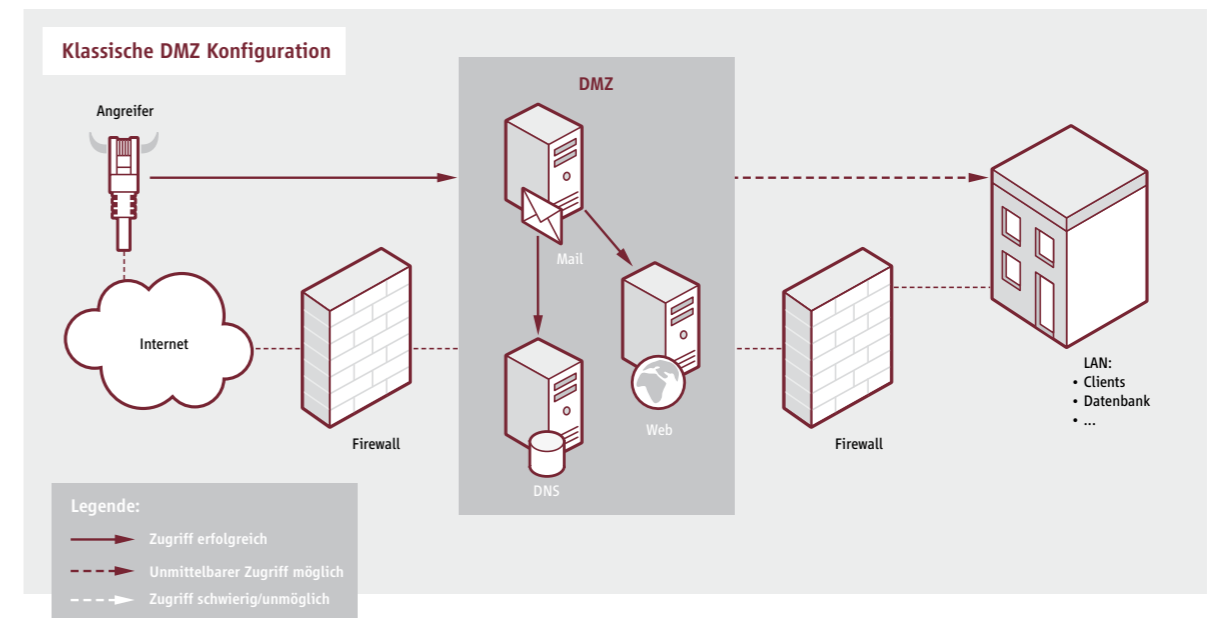
DER QTRUST SERVER

Der QTrust Server integriert eine Vielzahl von Sicherheitsmechanismen in einem System und bietet gleichzeitig verschiedene Mechanismen für mobile oder standortübergreifende Anbindung.

Über die klassische Firewall-Funktionalität (IP-Filter, VPN-Gateway) hinaus werden Daten auch auf Applikationsebene kontrolliert.

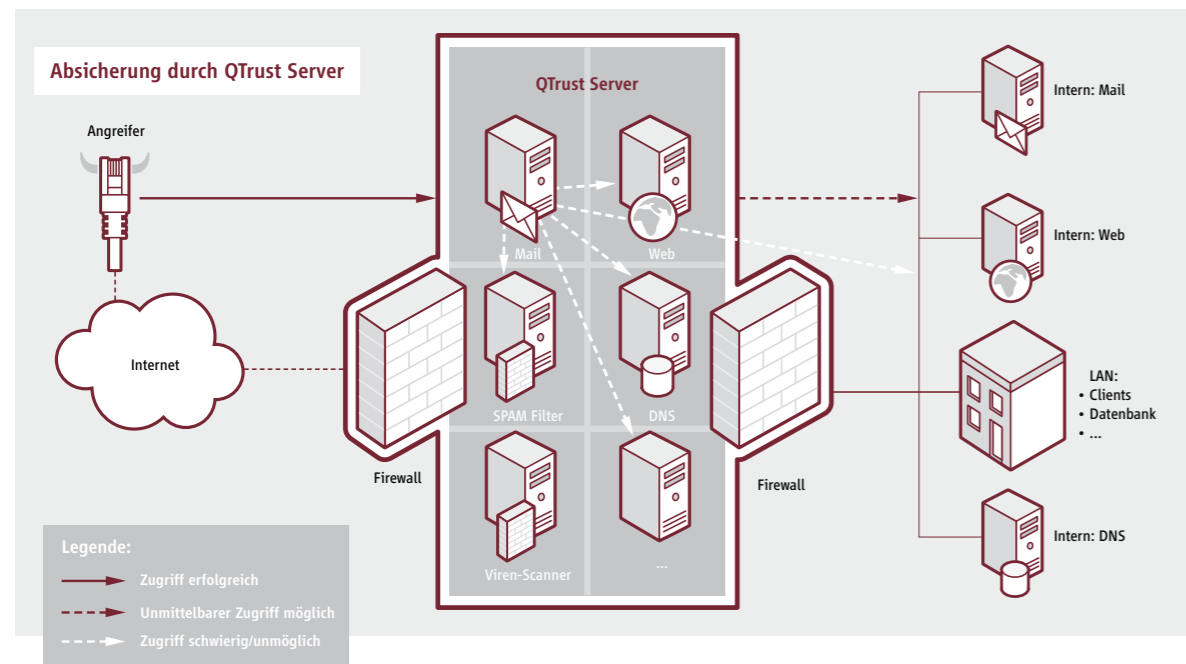
Hierzu wird der Datenfluss zwischen allen internen und externen Netzwerken unterbrochen, auf Berechtigung geprüft, gepuffert und auf Angriffe untersucht. Ein Application-Filter prüft ein- und ausgehende Datenpakete. Einbruchsversuche werden erkannt, geloggt und weitergemeldet.

Der QTrust Server wird intern durch die sichere Applikationsumgebung ‚PitBull‘ von der Argus Systems Group abgesichert. Basierend auf der Trusted Operating System (TOS) Technologie führt PitBull Prozesse der Firewall und Gateway



Anwendungen in einzelnen, voneinander getrennten Bereichen aus, die untereinander nur sehr eingeschränkt kommunizieren können. Innerhalb der Bereiche kann nur auf vordefinierte Ressourcen zugegriffen werden. Angriffe auf den QTrust Server selbst und die darauf laufenden Dienste können so unterbunden und kontrolliert werden. Dadurch kann ein Hacker maximal den angegriffenen Dienst beeinflussen, aber nicht andere Dienste übernehmen oder Zugriff auf die angeschlossenen Netzwerke erhalten.

Eine vergleichbare, hochsichere Konfiguration war bisher nur durch Verteilung der Dienste auf einzelne, unabhängige Server möglich. Teuer, komplex und aufwendig in der Administration kommen solche Lösungen meist nur bei sehr hohen und hochsicheren Anforderungen zum Einsatz, wie z.B. bei Banken und Versicherungen (u.a. bei Online-Banking).



Der QTrust Server vereint diese einzelnen Server auf einem integrierten System. Auf Basis der PitBull Technologie wurde die Linux Distribution ‚QLinx‘ entwickelt, die ebenso wie alle Sicherheits-Dienste über eine Webkonsole einfach und ohne Linux-Kenntnisse administriert werden kann. Eine eigene Paketverwaltung in QLinx erlaubt eine einfache, automatische und sichere Verwaltung und Installation von System- und Sicherheitsupdates.

Als Hardware-Plattform werden für die gesamte QTrust Produktfamilie Systeme von Hewlett Packard eingesetzt. Dies gewährleistet ein hohes Niveau an Ausfallsicherheit, Support und Service.

Für besonders hohe Anforderungen an die Verfügbarkeit stehen QTrust Server auf Plattform der Stratus ftServer zur Verfügung.

Als in der Anschaffung und Wartung günstige, einfach zu administrierende und skalierbare Appliance bietet der QTrust Server ein hohes Maß an Sicherheit für Unternehmen aller Größen.

QTRUST SERVER FUNKTIONALITÄT

Der QTrust Server unterbindet jede direkte Kommunikation zwischen externen und internen Netzwerken. Für jede ‚erlaubte‘ Verbindung werden die Datenpakete auf dem QTrust Server von Proxy-Diensten angenommen, untersucht, gepuffert und weitergeleitet. Dienste in internen Netzwerken oder in DMZs (Demilitarised Zones) werden so über den QTrust Server nach ‚außen‘ gespiegelt oder abgebildet.

• DNS:

Die internen primären DNS Server werden auf dem QTrust Server gespiegelt und nach außen publiziert. Für das Internet agiert der QTrust Server als virtueller Primary DNS Server (VPDNS).

• SMTP (mit SPAM-Filter und Virenschanner):

Die MX-Einträge der Domänen, für die Email empfangen wird, zeigen auf den QTrust Server, der die eingehenden Emails verifiziert, auf SPAM und Viren untersucht und dann an die internen Mailserver weiterleitet. Ausgehende Emails werden genauso behandelt. Die Integration von DNS Blacklisten sorgt für eine deutliche Reduzierung von Spam-Mails, welche rechtlich korrekt gar nicht erst angenommen werden.

• HTTP/HTTPS Webdefense Funktionalität:

Der QTrust Server agiert als virtueller HTTP/HTTPS Server (Proxy), der die Daten der internen Webserver nach außen zur Verfügung stellt. Geschützt werden können alle Formen von Web-Applikationen. Dabei wird jeder Zugriff auf die Web-Applikation geprüft. Angriffe werden anhand des IDS/IPS Systems erkannt und falls gewünscht geblockt. Mod-Security und spezielle QTrust Technologien verhindern erfolgreiche Angriffe wie SQL-Injections und Buffer Overflows.

• HTTP - HTTPS Umsetzung:

Ein interner HTTP Server kann nach außen als HTTPS Server gespiegelt werden und so eine sichere Verbindung erlauben, ohne dass der interne Server HTTPS können muss. Diese Funktionalität macht es leichter, die Struktur der Infrastruktur einfacher zu halten und entlastet die eigentlichen Systeme.

• FTP:

Für interne FTP Server agiert der QTrust Server ebenfalls als transparenter Proxy. Datei-Inhalte werden nach schädlichem Code durchsucht und gefiltert.

• IDS / IPS:

Auf Basis des Intrusion Detection Systems Snort ermöglicht der QTrust Server das dauerhafte oder temporäre Blocken von Angreifern. Eine Honeypot Konfiguration hilft hier erheblich, Angreifer frühzeitig zu erkennen und auszuschließen.

SCHUTZ DER INTERNEN NETZE

Für die Kommunikation aus den internen Netzen heraus werden folgende Protokolle transparent, d.h. ohne Änderung an den internen Clients, unterstützt. Der QTrust Server nimmt erlaubte Datenverbindungen an, untersucht die Daten auf Viren und leitet sie dann weiter.

• HTTP / Web-Proy

Das Surfen im Internet birgt viele und immer neue Gefahren: Trojaner, Viren, Keyboard-Logger und vieles mehr. Der QTrust Server als transparenter Proxy mit integrierter TrendMicro™ Viruswall verhindert diese Angriffe, ohne dass irgendeine Einstellung auf den Clients verändert werden muss. Gleichzeitig wird der Wartungsaufwand auf den Clients verringert.

• FTP:

Besonders öffentliche FTP Server können schnell infizierte Dateien zur Verfügung stellen. Auch hier scannt der QTrust Server alle übertragenen Dateien, ohne dass der Anwender dies umgehen kann. Darüber hinaus übernimmt der QTrust Server noch weitere Funktionen, welche die Geschäftsprozesse eines Unternehmens effizienter gestalten:

• Schutz vor SPAM und Viren:

Alle ein- und ausgehenden Emails werden ohne Ausnahme auf SPAM und Viren untersucht. Der SPAM Filter ist lernfähig und erkennt auch neue SPAM-Techniken automatisch. Als SPAM erkannte Emails werden entsprechend gekennzeichnet und können dann vom internen Mailserver entsprechend weiterverarbeitet werden.

• Paketfilter (Firewall):

Einzelne Verbindungen können IP Protokoll basiert gefiltert und/oder protokolliert werden.

• IPSec / VPN Gateway:

Mit dem QTrust Server können stark verschlüsselte VPNs zwischen verschiedenen Firmenstandorten oder Partnerunternehmen aufgebaut werden. Gleichzeitig dient er als VPN Gateway für Mitarbeiter, die auf Dienstreise oder von Zuhause aus autorisierten Zugriff auf firmeninterne Daten und Ressourcen brauchen. Es werden die am weitesten verbreiteten Standards unterstützt: IPSec, VTUN, openVPN und PPTP.

• QTrust 2go:

Zusätzlich zu den vorhandenen VPN Protokollen beinhaltet jeder QTrust die volle QTrust 2go Funktionalität. QTrust 2go verbindet dabei die Sicherheitsmerkmale des AXSionics Internet Passports mit einer auf einem Trusted OS laufenden Authentifizierungsplattform – dem QTrust Server – mit dem Ziel, User aus dem Internet sicher auf das Unternehmensnetzwerk zugreifen zu lassen.

• DHCP Server:

Der QTrust Server kann als DHCP Server für die internen Netzwerke eingesetzt werden.

• Load Balancer:

Werden in den internen Netzwerken aus Verfügbarkeitsgründen oder zur Lastverteilung mehrere Webserver eingesetzt, agiert der QTrust Server als Load Balancer. Die externen Anfragen werden automatisch an die internen Server verteilt.

Alle Systeme der QTrust Produktfamilie basieren auf Server-Hardware von Hewlett Packard, der ProLiant Serie. Entsprechend den Anforderungen kann zwischen vier Ausbaustufen mit entsprechenden Serviceverträgen und Garantieleistungen des Herstellers gewählt werden. Der Service und Support ist somit weltweit verfügbar, vorhandene Investitionen in HP Hardware können berücksichtigt werden.

QTRUST SERVER – EINFACHE ADMINISTRATION UND SINNVOLLE PROZESSE

Die Konfigurations-Parameter des QTrust Server und aller Dienste werden in einer internen Datenbank gespeichert. Über ein komfortables Web-Interface mit verschiedenen Berechtigungsstufen wird das System administriert. Bei der Erstinstallation hilft ein Einrichtungsassistent. Über das Web-Interface können Log-Dateien angesehen und zur Auswertung heruntergeladen werden. Verschiedene Statistiken geben Auskunft über den aktuellen Systemstatus. Zur automatischen Weiterverarbeitung von Protokoll-Dateien kann ein Netzlaufwerk angegeben werden auf das die täglichen Dateien gesichert werden.

Wichtige Sicherheitsupdates werden vom QTrust Server automatisch installiert ohne dass Administrationsaufwand notwendig ist.

Die Konfiguration lässt sich jederzeit bequem auf einen USB Stick sichern und von diesem auch wiederherstellen – so kann problemlos auf andere Hardware gewechselt werden.

Aufgrund der Schutzmaßnahmen, welche die PitBull Technologie ermöglicht, kann zudem sicher gestellt werden, dass keine kritischen Konfigurationsdaten von nicht-authorisierten Personen verändert werden, so dass nach einem Ausfall des Systems das System mit minimalem Aufwand wieder in Betrieb genommen werden kann.

Für häufige Fragen kann kostenlos über das QLine Portal eine Knowledge-Base genutzt werden.

ERWEITERTER SERVICE

QGROUPE bietet für den QTrust Server einen erweiterten Supportvertrag mit der Möglichkeit an, Problemtickets über das QLine Portal online zu eröffnen (eTicket).

Durch den Abschluss eines umfangreichen Service Vertrags kann die gesamte Administration des QTrust Servers an QGROUPE ausgelagert werden. Dies reicht von der Erstkonfiguration über die regelmäßige Wartung bis hin zur Echtzeitüberprüfung der Erreichbarkeit einzelner Dienste.

