

# SecureGUARD

## Security Appliances für jeden Anwendungsbereich

ISP-Redundancy  
NAP-Support  
URL-Filtering  
SSTP (VPN over HTTPS)  
One-Time-Password  
SIP-Support  
Network Inspection System  
Multi-Engine AV  
Central Management  
Fast Recovery  
DirectAccess



art OF defence

HIKARUS  
security software



MICRODASYSTM

PointSharp



Microsoft®  
Forefront™  
Threat Management Gateway 2010

Integrierte und umfassende Lösung  
für den Schutz vor Angriffen aus dem  
Internet.



Microsoft®  
Forefront™  
Unified Access Gateway 2010

Vereinheitlichte Plattform, die alle  
Anforderungen an eine Remote  
Access Lösung erfüllt.

## SecureGUARD Operating System

Das SecureGUARD Operating System wird mit jeder Appliance ausgeliefert. Es stellt alle Funktionen für die Administration der Appliance zur Verfügung.

- **Intelligent Deployment**  
Das Appliance Management ermöglicht eine schnelle Inbetriebnahme und rasche Erstkonfiguration der SecureGUARD Appliance.
- **Intelligent Management**  
Die SecureGUARD Appliance kann durch das Appliance Management vollständig ohne die Nutzung einer Konsole administriert werden.
- **Intelligent Disaster Recovery**  
Das im SecureGUARD OS integrierte Disaster Recovery Tool ermöglicht es mit nur einem Klick das Gerät in den ursprünglichen Auslieferungszustand zurück zu setzen.
- **Support**  
Schnelle Hilfe und umfassende Unterstützung durch das erfahrene und kompetente Support-Team sind weitere Markenzeichen des SecureGUARD Teams.

*SecureGUARD steht für langjährige Erfahrung in der Entwicklung und Produktion von Security-Appliances. Entwickelt aus der Praxis für die Praxis und kombiniert mit Microsoft TMG 2010 oder UAG 2010 entstehen daraus anwenderfreundliche und praxisnahe Security-Lösungen für den Schutz von Unternehmensnetzwerken.*

## SecureGUARD Appliances ...

### Hardware, Software & Support aus einer Hand

Die SecureGUARD Appliances für Microsoft Forefront Threat Management Gateway 2010 und Unified Access Gateway 2010 kombinieren leistungsfähige Hardware, ausgereifte Security-Lösungen und umfassenden Support zu einer benutzerfreundlichen ready-to-use Gesamtlösung für Perimetersicherheit, Remote Zugriff, Anbindung von Zweigstellen, Webcaching oder Schutz von Server-Farmen.

### Schutz für jeden Anwendungsbedarf

Der modulare Aufbau der SecureGUARD Appliance gewährleistet die flexible Anpassung an die spezifischen Anforderungen Ihres Unternehmens. Von günstigen und geräuscharmen Modellen für den Mittelstand bis hin zu komplexen Enterprise-Lösungen mit höchster Performance.

### Einfache Bereitstellung und Verwaltung

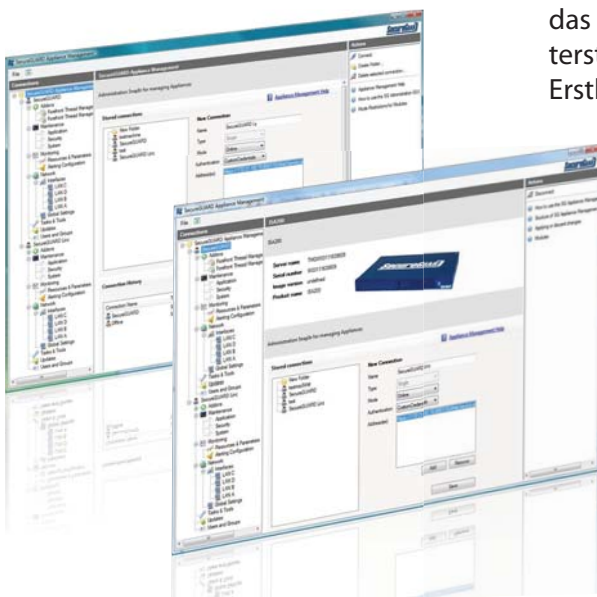
Die Inbetriebnahme wird durch das Appliance Management unterstützt, das sowohl die schnelle Erstkonfiguration als auch den weiteren einfachen Betrieb der SecureGUARD Appliances ermöglicht. Es gibt ein einheitliches Management Interface für alle Appliances, seien es TMG oder UAG Appliances. Auch die vorinstallierten Third-Party-Applikationen lassen sich über das Interface schnell und bequem aktivieren.



### Optimale Performance und persönliche Unterstützung

Durch ihre hohe Ethernet-Portdichte und der ausgereiften Hardware bilden die SecureGUARD Appliances komplexe Netzwerke mit unzähligen Subnetzen und DMZ's ohne Performanceeinbruch ab.

Weitere Markenzeichen der SecureGUARD Lösung: Schnelle Hilfe und umfassende Unterstützung durch unser erfahrenes und kompetentes Support-Team.



## Neue Features im Vergleich

Laufende sich ändernde Anforderungen an die IT im Bereich Sicherheit und Mobilität machen es notwendig vor allem Gateway Produkte ständig weiterzuentwickeln und zu erweitern.

Folgende Tabellen zeigen einen Überblick der neuen Features des Microsoft Forefront Threat Management Gateway 2010 und des Microsoft Forefront Unified Access Gateway 2010 im Vergleich zu ihren Vorgängerprodukten.

	ISA 2006	TMG 2010
Network and Application Firewall	✓	✓
Internet Access Protection (Proxy)	✓	✓
Basic OWA & SharePoint Publishing	✓	✓
VPN Endpoint (remote & site-to-site)	✓	✓
Windows Server 2008, native 64-Bit	✗	✓ Neu
Secure Web-Proxy (AV, Url-Filter)	mit 3 <sup>rd</sup> Party	✓ Neu *)
HTTPS-Inspection (Forward Proxy)	mit 3 <sup>rd</sup> Party	✓ Neu
SIP Filter, ISP Failover / LB, E-NAT	✗	✓ Neu
SSTP, NAP, Intrusion Prevention (NIS)	✗	✓ Neu
Static one-to-one NAT Support	✗	✓ Neu **)

\*) Client Access License (CAL) erforderlich; Realisierung durch 3rd Party möglich.

\*\*\*) Mit dem integrierten SecureGUARD NAT Filter.

	IAG 2007	UAG 2010
Application Intelligence and Publishing	✓	✓
End Point Security	✓	✓
SSL Tunneling	✓	✓
Information Leakage Prevention	✓	✓
NAP Integration, Terminal Service Integration	✗	✓ Neu
Array Management	✗	✓ Neu
Enhanced Management and Monitoring	✗	✓ Neu
Enhanced Mobile Solutions	✗	✓ Neu
Direct Access and SSTP Integration	✗	✓ Neu

### IKARUS

Der **IKARUS security.proxy** ist eine auf dem Gateway zusätzlich installierte Securityinstanz zur Absicherung des Webtraffic mittels URL-Filtering und Antivirus. Das Softwarepaket ist bereits vorinstalliert und enthält eine 5-User-Jahreslizenz.



### Art of Defence

**Hyperguard** ist eine softwarebasierte Enterprise Web Application Firewall, die innerhalb der HTTP-Ebene die Businesslogik der Web-Anwendungen gegen bekannte und unbekannte Angriffe schützt.



### Microdasys

**GeoShield** warnt vor oder blockt den Zugang zu Servern in geografisch riskanten Regionen und ermöglicht Sicherheitsvorgaben, die auf dem tatsächlichen Standort eines Servers basieren.



### PointSharp

**PointSharp ID** ist eine softwarebasierte Authentifizierungslösung, welche mit one-time-Passwörtern arbeitet.

**Secure ActiveSync** vereinfacht die Administration einer ActiveSync-Lösung bei gleichzeitiger Erhöhung der Sicherheit.

Diese Produkte sind bereits vorinstalliert und enthalten eine 10-User-Jahreslizenz.



## SecureGUARD UAG Appliance

SecureGUARD UAG steht für hochintegrierte, multifunktionale Security Appliance. Wir bieten eine kostengünstige ready-to-use Gesamtlösung mit umfassender Firewallfunktion auf Netzwerkebene, IPsec, SSTP, SSL-VPN Fähigkeiten, DirectAccess, robuster Anwendungsoptimierung und einem integrierten Disaster Recovery System für höchste Verfügbarkeit.

SecureGUARD stellt viele unterschiedliche Hardware Appliances zur Verfügung, um optimal auf Ihre individuellen Leistungsanforderungen einzugehen. Die Hardware skaliert vom Einsteigermodell bis hin zu einer High-End Lösung mit 8 CPU Kernen auf einer einzelnen Appliance im 1HE Format.

## Unified Access Gateway 2010

- **Sicherung von Inhalten**  
Differenzierter und policy-gesteuerter Zugriff auf Unternehmensdaten, Content Prüfung und Filterung sowie Management der Endpoint Security.
- **Sicherer Remote-Access**  
Zugriff für Mitarbeiter, Partner und Kunden auf Unternehmensressourcen – praktisch unabhängig vom Gerät und Standort.
- **Direct Access**  
UAG 2010 bietet die Möglichkeit Direct Access (Always-on-VPN) einfach schnell zu implementieren und zu skalieren.
- **Internet-Zugriffsschutz**  
Wirkungsvollere Abschirmung der IT-Infrastruktur gegen Gefahren aus dem Internet.

## Microsoft Forefront Unified Access Gateway 2010

### ... bring the good guys in

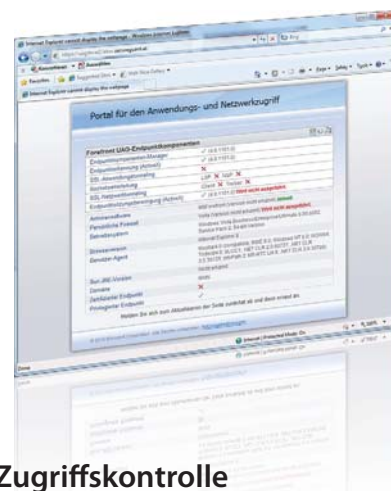
Durch die Integration des Unified Access Gateway 2010 (UAG 2010) bietet SecureGUARD eine Appliance, die sicheren Remote-Access, Sicherheit für Zweigniederlassungen und Internet Zugriffsschutz gewährleistet. Die Inbetriebnahme der SecureGUARD UAG 2010 Appliances wird durch das Appliance Management unterstützt, das sowohl die schnelle Erstkonfiguration als auch den weiteren einfachen Betrieb der SecureGUARD Appliances ermöglicht. Auch die vorinstallierten Third-Party-Applikationen lassen sich auf diese Weise schnell und bequem aktivieren.

### Umfassender, sicherer Zugriff

Das Unified Access Gateway (UAG) mit Application Optimizer-Modulen stellt ein SSL VPN, eine Web-Applikations-Firewall sowie Funktionalität für das Management der Endpoint-Security bereit und ermöglicht so Zugriffskontrolle, Autorisierung und Content-Prüfung für eine Vielzahl von Spartenanwendungen.



In ihrer Kombination bieten diese Technologien den Mobil- und Remote-Benutzern einfachen und flexiblen Zugriff von den unterschiedlichsten Orten und Geräten wie Kiosken, PCs und Mobil-Devices. Darüber hinaus ermöglicht das UAG den Administratoren, die Einhaltung von Richtlinien zur Nutzung von Anwendungen und Informationen mithilfe einer speziellen Remote-Zugriffs-Policy durchzusetzen, die sich nach dem Endgerät, dem Benutzer, der Anwendung richtet.



### Zugriffskontrolle

Sicherer, browserbasierter Zugriff auf Unternehmensanwendungen und Daten von Standorten und Endgeräten, ohne dass die Installation und Bereitstellung eines Clients erforderlich ist.

### UAG 2010 Service Pack 1

Mit dem Release von UAG 2010 Service Pack 1 wurde verstärkt auf Kundenanfragen eingegangen. Dies beinhaltet unter anderem eine Out-of-the-Box Unterstützung für Zwei-Faktor-Authentifizierung mittels RSA SecureID und eine Integration des DirectAccess Monitoring in den UAG Webmonitor. Ein erweiterter DirectAccess Connectivity Assistant sorgt für eine verbesserte Fehlersuche in DirectAccess Szenarien. Mit dem Service Pack 1 ist es ebenfalls möglich, DirectAccess in einem „Management Only“ Szenario zu betreiben.

## Microsoft Forefront Threat Management Gateway 2010

### ... keep the bad guys out

Das Threat Management Gateway 2010 (TMG 2010) beinhaltet Firewall Funktionalität mit Stateful Inspection Paketfilter, Application Layer Firewall, VPN Gateway Funktionalität, URL-Filtering und Web Proxy sowie Virenschutz. Der Einsatz ist besonders interessant in homogenen Microsoft Umgebungen mit zentraler Authentifizierung.

Durch die Integration in eine Backend-Anwendungsinfrastruktur wie beispielsweise Exchange Server und Windows SharePoint Services bietet TMG einen sicheren Mechanismus für Authentifizierung und Zugriff.



Tools wie Assistenten zur automatischen Veröffentlichung von Serverressourcen, formularbasierte Vorauthentifizierung, anpassbare Sicherheitseinstellungen für Exchange und Windows SharePoint Services sowie viele andere Verbesserungen zeichnen den Threat Management Gateway aus.

### Wo in meiner Umgebung sollte TMG 2010 bereitgestellt werden?

Threat Management Gateway 2010 kombiniert die Stärken einer Firewall auf der Anwendungsschicht mit VPN- sowie Proxy- und Caching-Funktionen. Die Lösung kann für folgende Aufgaben bereitgestellt werden:

- Als ein **Branchoffice-Gateway** zur Bereitstellung von Konnektivität und Sicherheit für Zweigstellen und Niederlassungen.
- Zum **Schutz der Anwendungsveröffentlichung**, um den Remotezugriff der Benutzer auf Unternehmensressourcen abzusichern.
- Als **Webzugriffsschutz**, gegen Bedrohungen aus dem Internet und ausgeklügelten Angriffen (AV, URL-Filtering).

Die SecureGUARD TMG 2010 Appliance überzeugt durch ein neues optimiertes und kostengünstiges Design, das zur Senkung der Betriebskosten beitragen kann und die Installation von mehreren Geräten verschiedener Anbieter für unterschiedliche Zugriffsmethoden überflüssig macht.

### Wer profitiert am meisten von den SecureGUARD TMG 2010 Appliances?

Unternehmen, die von einer Flut gezielter und ausgeklügelter Angriffe auf ihre Netzwerke betroffen sind. Unternehmen in vielfältigen Branchen, beispielsweise Finanzdienstleister, Wiederverkäufer oder Behörden und Verwaltungen, können große Vorteile aus einer Bereitstellung von TMG als Schutzmaßnahme für Internetclients und als Möglichkeit, interne Ressourcen für Remote Mitarbeiter verfügbar zu machen, ziehen.

## TMG Software Editionen

Die SecureGUARD Threat Management Gateway 2010 Appliances sind für die unterschiedlichen Anwendungsfälle in folgenden Versionen verfügbar. Die Basisfunktionalitäten sind bei allen Ausführungen identisch – nur die Clusterfähigkeit sowie zentrales Management unterscheiden die Versionen.

### Workgroup Edition

Für kleine und mittlere Unternehmen mit überwiegend einem Standort, welche neben URL-Filtering und Antivirus ein einfaches und funktionales Management benötigen. Oft nach dem all-in-one Konzept um weitere Third-Party-Applikationen erweitert. Die Workgroup 25 User Edition ist bereits ab dem TMG200 verfügbar.

### BranchOffice Edition

Zur Anbindung mehrerer Außenstellen an eine Zentrale (Enterprise Edition) mit den Vorteilen eines zentralen Managements. Die BranchOffice Edition ist die „Spezialversion“ der Enterprise Edition für die Außenstellen, welche von der zentralen Enterprise Edition verwaltet wird. Jede Ausführung der SecureGUARD Appliances kann mit der BranchOffice Edition ausgeliefert werden.

### Enterprise Edition

Ist für den Einsatz in großen Organisationen bestimmt, die flexible Verteilungsoptionen sowie ein höchstes Maß an Verwaltbarkeit und Verfügbarkeit benötigen. Das zentrale Management und die Clusterfähigkeit zeichnen diese Version aus. Wir empfehlen die Enterprise Edition in Kombination mit den SecureGUARD Appliances ab dem Modell TMG1000.

## SecureGUARD TMG200, UAG200

Die TMG200 mit ihrem kompakten Format wurde speziell für kleinere Büroumgebungen konzipiert.

### Standard-Spezifikationen:

**CPU:** Intel Dual Core 64-bit  
**Memory:** 2048 MB (UAG: 4096MB)  
**Hard Disk:** 1x SATA 24x7  
**Ethernet:** 4x 10/100/1000 NIC

### Optionale Erweiterungen:

Remote Management (shared NIC)  
Factory RAM Upgrade bis max. 4 GB (TMG-WG)



## SecureGUARD TMG1000, UAG1000

Diese Appliances kombinieren maximale Performance mit minimaler Höhe. Durch die Leistung der 4 CPU-Kerne gibt es auch bei hoher Benutzerlast keine Probleme.

### Standard-Spezifikationen:

**CPU:** Intel QuadCore XEON  
**Memory:** 4096 MB  
**Hard Disk:** 2x SATA2 RAID1 (kein Hotswap)  
**Ethernet:** 4x 10/100/1000 NIC  
**Formfaktor:** 19", 1HE  
**Features:** Remote Management

### Optionale Erweiterungen:

Factory RAM Upgrade bis max. 16 GB  
Factory NIC Upgrade bis max. 10 Interfaces



## SecureGUARD TMG1100, UAG1100

Das eingebaute LCD erlaubt einfache Basiskonfiguration und ein schnelles Rollout der Appliance, ohne einen Monitor oder eine Tastatur anzuschließen.

### Standard-Spezifikationen:

**CPU:** Intel QuadCore XEON  
**Memory:** mind. 4096 MB  
**Hard Disk:** 2x SATA2 HW RAID1  
**Ethernet:** 4x 10/100/1000 NIC  
**Formfaktor:** 19", 1HE  
**Features:** Remote Management

### Optionale Erweiterungen:

Factory RAM Upgrade bis max. 16 GB  
Factory NIC Upgrade bis max. 10 Interfaces  
Redundantes Netzteil



## SecureGUARD TMG1600, TMG1650, UAG1600, UAG1650

Die SecureGUARD TMG1650 Appliance ist eine der stärksten und leistungsfähigsten Appliances auf dem Markt. Der TMG1650 mit 12 CPU-Kernen erfüllt die höchsten Ansprüche im Security-Bereich.

### Standard-Spezifikationen 1600:

**CPU:** 2x Intel QuadCore XEON  
**Memory:** 8-16 GB  
**Hard Disk:** 2x SATA2 battery buffered HW RAID1  
**Ethernet:** 4-10x 10/100/1000 NIC  
**Formfaktor:** 19", 1HE  
**Features:** Remote Management,  
Redundantes Netzteil (optional)

### Standard-Spezifikationen 1650:

**CPU:** 2x Intel SixCore XEON Xtreme  
**Memory:** 16 GB  
**Hard Disk:** 2x SAS battery buffered HW RAID1  
**Ethernet:** 4-10x 10/100/1000 NIC  
**Formfaktor:** 19", 1HE  
**Features:** Remote Management,  
Redundantes Netzteil



## SecureGUARD Blade Edition

Die Blade Edition vereint die Kraft von 12TMG1000 Appliances mit ihren 48 CPU Kernen. Die 3+1 eingebauten Netzteile sorgen dabei für höchste Ausfallsicherheit. Ob Cloud-Computing-Security, maximale Performance für klassische Sicherheitssysteme oder mehrstufige Firewallkonzepte: Mit der Blade Edition lässt sich alles auf höchstem Niveau realisieren.

Die Oberfläche kann optisch und inhaltlich angepasst werden. Spezielle Images, auch im Hinblick auf 3rd Party Applikationen, können für Projekte erstellt werden.



Irrtümer und Druckfehler vorbehalten! Stand 01/2011. Produktabbildungen können vom tatsächlichen Produkt abweichen.



Salesinfo:  
office@secureguard.at  
www.secureguard.at  
Infohotline:  
+43 (0) 732 60 14 40



Salesinfo:  
sales@secureguard.de  
www.secureguard.de  
Infohotline:  
+49 (0) 89 570 880 25

Microsoft  
GOLD CERTIFIED  
Partner

SecureGUARD

All available products at  
[www.secureguard.at](http://www.secureguard.at)

Copyright (c) SecureGUARD GmbH 2010  
SecureGUARD is a registered trademark of SecureGUARD GmbH.  
All other trademarks and registered trademarks are the property of their respective companies.