INFOBRIEF

# IGEL OS SECURITY

## Umfassender Endgeräteschutz für ein sicheres Unternehmen

Viele Unternehmen, die Remote-Desktop-Technologie, virtuelle Desktops und Desktop-as-a-Service-Modelle einsetzen, wollen damit auch die Sicherheitsrisiken am Endpoint reduzieren. Wenn Windows-Betriebssysteme nicht auf Endgeräten, sondern in Rechenzentren oder Cloud-Umgebungen ausgeführt werden, kommen Unternehmen diesem Ziel einen großen Schritt näher. Allerdings ist auch auf dem Endpoint ein Betriebssystem erforderlich, um den Remote-Zugriff auf Anwendungen und Desktops zu ermöglichen und lokale Schnittstellen, Displays und Peripherigeräte zu unterstützen.

IGEL OS ist das Edge-Betriebssystem der nächsten Generation für Cloud Workspaces, das speziell für diesen Zweck entwickelt wurde. Basierend auf Linux und strukturiert als modulare, schreibgeschützte Firmware verfügt IGEL OS über eine extrem kleine Angriffsfläche und eine breite Palette von Sicherheitsfunktionen. Diese sind darauf ausgelegt, Risiken zu minimieren und zu verhindern, dass Angreifer über den beliebtesten Einstiegspunkt – den Netzwerkrand – in Ihr Unternehmen eindringen.

Die Endpoint Security steht bei der Entwicklung und Weiterentwicklung von IGEL OS im Mittelpunkt.
In den folgen-den Tabellen sind die wichtigsten Sicherheitsfunktionen des Betriebssystems zusammengefasst.

| SICHERHEITS-FEATURE, VORINSTALLIERT | FUNKTION |
|---|---|
| Modulare Partitionen | Ermöglichen das Ein- und Ausschalten bestimmter Funktionen (z.B. Cirix Workspace, Browser, ThinPrint, etc.) am Endpoint. Sensible Partitionen werden verschlüsselt, um kritische Daten und andere Funktionen zusätzlich zu schützen. |
| Automatische Abmeldung | Durch die Kombination eines Sitzungstyps mit einem Auto-Logoff-Befehl wird der Benutzer automatisch aus der letzten Sitzung abgemeldet In Kombination mit Kerberos ist das Gerät abgemeldet und sicher. Benutzer-name und Passwort sind erforderlich, um sich erneut anzumelden. |
| Vorinstallierte Sicherheitsfunktionen | Reines Kerberos-Ticket-Handling, basierend auf Benutzername und Passwort, mit ausgeklügelten Zwei-Faktor-Smartcard-Lösungen (Smartcard und PIN) durch eine “Dreierkonstellation”.<br>• IGEL OS-powered Endpoint<br>• Active Directory-Infrastruktur<br>• Kerberos-fähiger Dienst (z.B. Citrix Virtual Apps and Desktops)<br>Ausgefeiltes Regel- und Rechte-Rollout-Management im gesamten Netzwerk auf Anwendungsebene und für Services.<br>Kein lokales “Fake-Active-Directory”. |

| SICHRHEITS-FEATURE, VORINSTALLIERT | FUNKTION |
|---|---|
| VNC Secure Mode | Unterstützt die Einhaltung von Compliance-Standards in Unternehmen – unter anderem durch folgende Kontrollmöglichkeiten:<br>• Protokollierung von Session Shadowing<br>• Zuweisung unterschiedlicher Shadowing-Berechtigungen<br>• Definition von Shadowing-Gruppen und Sicherheitsstufen<br>• Verbot von VNC-Sitzungen zwischen Client und Client (wenn sie in den Client-Desktop integriert sind).<br>• Ausschließliche Zulassung von IGEL-Shadowing oder VNC-Client eines Drittanbieters in der UMS-Konsole<br>• Sperren von externen/unbekannten VNC-Clients von Drittanbietern im gesamten Netzwerk<br>• Verschlüsselung mit TLSv1.2 |
| Papierkorb | Gelöschte Objekte werden in den Papierkorb verschoben, wo Sie Objekte am Ursprungspunkt wiederherstellen oder Objekte dauerhaft löschen können. Versehentlich gelöschte Objekte können wiederhergestellt werden. |
| High Availability Erweiterung | HA ermöglicht den Betrieb von zwei oder mehr UMS-Servern innerhalb des Netzwerks mit einem automatischen Ausfallmechanismus – sowohl für Redundanz als auch für bessere Skalierbarkeit. Ein integrierter Load Balancer unterstützt einen unabhängigen gleichzeitigen Bootvorgang, was besonders für größere Umgebungen nützlich ist. Mehr Infos auf Knowledge Base |
| USB Management | Das USB-Management ist für den Schutz vor Sicherheitsrisiken ganz entscheidend. USB-Geräte wie Eingabestifte, drahtlose Steuerungen oder Drucker können zum Datendiebstahl, zur Ausführung nicht autorisierter Software oder sogar zur Verbreitung von Malware genutzt werden.<br>Um die Verwendung von USB-Geräten zu kontrollieren und die Angriffsfläche von IGEL UD Endpoints zu minimieren, Deaktivierung von USB-Geräten ist im IGEL Setup möglich. Sie können Regeln konfigurieren, um den Zugriff durch unerwünschte USB-Geräte zu blockieren.<br>Eine Schritt-für-Schritt-Anleitung ist in der Knowledge Base verfügbar<br>Das IGEL USB-Management (Basisfunktion) basiert auf der USB-Klasse, der Hersteller-/Produkt-ID oder der Geräte-UUID mit einem stark vereinfachten Zugriffs- und Ablehnungsmechanismus.<br>FabulaTech (erweiterte Funktion, erfordert optionale Serverkomponenten vom Drittanbieter) basiert auf Protokollen (RDP, Horizon, Citrix) und unterstützt je nach Protokoll unterschiedliche Funktionen.<br>Die DriveLock Thin Client Suite basiert auf virtuellen Protokollen, die protokollübergreifend mit benutzerabhängigem USB-Management einen sehr hohen Sicherheitsstandard ermöglichen. |

## IGEL Chain of Trust

Die IGEL Chain of Trust stellt sicher, dass alle Komponenten eines VDI/Cloud-Arbeitsbereichsszenarios sicher und vertrauenswürdig sind. Jede startende Komponente prüft die kryptographische Signatur der nächsten und startet sie nur, wenn sie von einer vertrauenswürdigen Partei wie IGEL oder dem UEFI-Forum signiert ist.

Bei Endgeräten mit IGEL OS beginnt die Kette beim UEFI, das den Bootloader auf eine UEFI Secure Boot-Signatur überprüft. Der Loader wiederum überprüft den Linux-Kernel von IGEL OS. Wenn die Signaturen der Betriebssystempartitionen auf der Festplatte korrekt sind, wird IGEL OS gestartet und die Partitionen werden eingebunden.

Bei IGEL UD3 und UD7-Geräten beginnt dies bereits auf der AMD-Hardwareplattform. Ein spezieller Sicherheitsprozessor überprüft die kryptographische Signatur des UEFI (ab Dezember 2019).

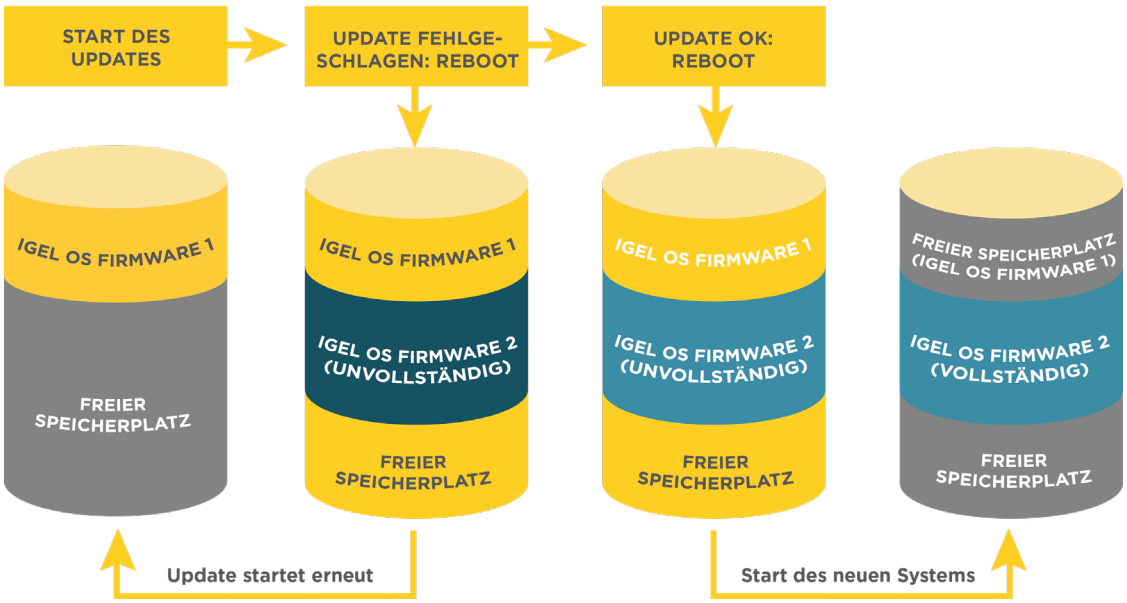
Wenn Benutzer eine Verbindung zu einer VDI- oder Cloud-Umgebung herstellen, überprüft eine Zugangssoftware wie Citrix Workspace App oder VMware Horizon das Zertifikat des Servers, mit dem sie sich verbinden.

Diese Kette stellt sicher, dass keine der Komponenten in Ihrer Umgebung manipuliert wurde - eine hervorragende Grundlage für sicheres Endbenutzer-Computing.

| SYSTEMINTEGRITÄT | FUNKTION |
|---|---|
| Bestätigungsprüfungen von Partitionen | Hashwert-Prüfungen sowohl bei Update- als auch bei Boot-Prozessen für System- und Benutzerpartitionen erkennen Manipulationen. Bei einem positiven Befund wird das System nicht gestartet. Wenn eine andere Partition betroffen ist, deaktiviert das System die betroffenen Module vor dem Start. |
| Flash-Medien können nicht in einem anderen Gerät gemountet werden | IGEL verwendet ein eigenes Partitionierungssystem mit komprimierten Partitionen, die Daten verschlüsseln. Prüfsummen von IGEL-Partitionen verhindern das Laden von modifiziertem Code. |
| Geschützte Konfiguration | Die Konfiguration wird auf eine dedizierte und verschlüsselte Partition geschrieben. |
| Ausfallsichere Firmware-Updates | Firmware-Updates werden immer vollständig abgeschlossen, während das Gerät läuft und bootfähig bleibt. Kritische Updates werden grundsätzlich in zwei Phasen bearbeitet, um den Erfolg zu sichern. |
| UEFI Secure Boot | Der IGEL OS Bootloader wurde von Microsoft (im Namen des UEFI-Forums) validiert. IGEL OS bootet auf Systemen mit aktiviertem UEFI Secure Boot.<br>• Nur Bootloader, die mit IGEL-Schlüsseln oder von IGEL zugelassenen Microsoft-Schlüsseln signiert sind, können das Betriebssystem laden<br>• IGEL generiert und verwaltet die Austauschschlüssel der kryptographischen Plattform, die in den entsprechenden UEFI-Versionen enthalten sind<br>• Derzeit auf IGEL UD2, UD3, UD7 Thin Client Endpoints<br>• Auf IGEL OS 11 der Modus “Secure Boot” ist als Standardwert im UEFI (BIOS) aktiviert |

| SYSTEMINTEGRITÄT | FUNKTION |
|---|---|
| Sicherer Browser über AppArmor | Sicherer Browser mit eingeschränktem Zugriff auf sensible Daten mit folgenden Eigenschaften:<br>• SSH-Schlüssel kann nicht gelesen werden<br>• Neue Schlüssel können nicht hinzugefügt werden<br>• IGEL-Konfigurations- und Firmware-Update-Skripte sind nicht zugänglich<br>• Keine Ansicht der Konfigurationsdateien<br>• Java ist vollständig deaktiviert<br>• Keine Downloads<br>• Zugriff auf Yubikey: Zwei-Faktor-Authentifizierung |
| Verifizierung durch das Center of Internet Security (CIS) | Erfolgreich absolvierte Benchmark-Tests des CIS zum Schutz vor Cyber-Bedrohungen. |

## AUSFALLSICHERER FIRMWARE UPDATE PROZESS




| INTEGRIERTE TECHNOLOGIEN | FUNKTION |
|---|---|
| Vorinstallierte VPN-Lösungen | OpenVPN wird über VPN-basiertes IGEL Client Management der IGEL UMS unterstützt. Der NCP-e VPN-Client (optionale NCP-e Lizenzierung) verwendet den universellen IPsec-Client.<br>Der Genua GenuCard-Support umfasst die vollständige Verwaltung über die IGEL UMS mit Verbindungsaufbau über den IGEL Managed Client und Unterstützung für ADSL-, LAN-, EDGE-, 3G- und 4G-Verbindungen. VS-NfD, NATO RESTRICTED und RESTREINT UE sind autorisiert und zertifiziert. |
| Keyboard Encryption | Die Keyboard Encryption über das Cherry Secure Board garantiert eine unmittelbare Verschlüsselung der Tastatureigaben. |
| IP-based cryptosytem | IGEL OS unterstützt SINA Workstation von secunet, die für die Verarbeitung von Verschlusssachen bis einschließlich GEHEIM, NATO SECRET und SECRET UE/EU SECRET zugelassen sind. |

| INTEGRIERTE TECHNOLOGIEN | FUNKTION |
|---|---|
| Vorinstallierte SSO-Lösungen | Der Smartcard-Support ist über IGEL-Partitionen individuell anpassbar. Unterstützt werden<br>• IGEL Smartcard<br>• **SecMaker** NetID<br>• **SafeNet** Aladdin eToken<br>• **Gemalto SafeNet** Middleware für Gemalto/SafeNet eToken, IDPrime Smartcards und Token<br>• **cryptovision sc/interface** Middleware für cryptovision Smartcards<br>• **Gemalto IDPrime** Smartcards<br>• **Athena IDProtect** Middleware für Athena IDProtect Smartcards<br>• **A.E.T. SafeSign** Middleware für SafeSign Smartcards<br>• **Secmaker Net iD** Middleware für Net iD Smartcards<br>• **Coolkey** Middleware Coolkey<br>• **OpenSC** Middleware OpenSC<br>• **90meter** Middleware<br><br>Die Unterstützung von Smartcard-Lesegeräten ist über IGEL-Partitionen individuell anpassbar und unterstützt folgende Funktionen<br>• Elatec TWN4 CCID<br>• PC/SC Lite<br>• M.U.S.C.L.E.<br>• HID OMNIKEY<br>• REINER SCT cyberjack<br><br>In IGEL OS integrierte Autorisierungssoftware<br>• **Imprivata** OneSign ProveID Embedded<br>• **Evidian** AuthMgr |
| Contextualizing | Zur Einhaltung von Governance-Anforderungen unterstützt IGEL OS DeviceTrust. Der Zugriff auf Apps und Verzeichnisse wird abhängig vom Zugriffsort gewährt. |
| Vorinstallierte biometrische Technologien | IGEL OS unterstützt biometrische Peripheriegeräte wie<br>• Crossmatch Fingerabdruck-Leser<br>• Fujitsu Handvenen-Scanner |

IGELs Fokus liegt auf der Bereitstellung des ultimativen Endpoint-Betriebssystems für Cloud Workspaces. Sicherheit und Datenschutz haben beim Design und bei der Entwicklung von IGEL OS höchste Priorität. Die oben aufgeführten Informationen geben einen Überblick über das laufend wachsende Angebot an Sicherheitsfunktionen. Diese tragen alle dazu bei, den bestmöglichen Endpoint-Schutz zu bieten und die Angriffsfläche am Netzwerkrand zu reduzieren.

Besuchen Sie igel.de und erfahren Sie mehr über neue Entwicklungen von IGEL für höhere Endpoint Security und einen einfachen und **sicheren** Übergang in die Cloud.

Besuchen Sie uns online: **igel.de/security-at-the-edge**

Revolutionary in its
**Simplicity**

IGEL is a registered trademark of IGEL Technology GmbH. All hardware and software names are registered trademarks of the respective manufacturers.
Errors and omissions excepted. Subject to change without notice. © 07/2021 IGEL Technology I 85-EN-24-1 I WEEE-Reg.-Nr. DE 79295479 I WEEE-Reg.-No. UK 5613471