Software zur Sicherung und Verwaltung von BYOD
Bring your own Device

SECURITY- UND MANAGEMENT-SOFTWARE FÜR BYOD

HERSTELLER	AIRWATCH	AMAGU	BMC SOFTWARE	BOXTONE	CISCO SYSTEMS	CISCO SYSTEMS	CISCO SYSTEMS	CITRIX SYSTEMS	DELL
URL	www.air-watch.com	www.amagu.eu	www.bmc.com	www.boxtone.com	www.cisco.com	www.cisco.com	www.cisco.com	www.citrix.ch	www.dell.ch
Software-Name	AirWatch	Amagu MDM Portal Services	BMC BladeLogic Client Automation (BCA)	BoxTone 7.0	Cisco AnyConnect Security Client	Cisco Jabber Collaboration Client	Cisco WebEx Client	XenDesktop	Dell MDM 12.1
Software-Kategorie									
Security	■	■	■	■	■	❑	❑	■	■
Management (Software zur Verwaltung und Organisation der Geräte)	■	■	■	■	❑	❑	❑	■	■
Weiteres									
Unterstützte Notebook-Plattformen	Mac OS X Lion	❑	Mac OS, Windows XP, Vista, 7, Linux (Redhat, Suse etc.)	❑	Mac OS, Windows, Android	Mac OS, Windows	Mac OS, Windows, Linux	Mac OS X, Windows, etc.	k.A.
Unterstützte Tablet-Plattformen	iOS, Android	iOS, Android	iOS 4 und 5, Android 2.3 und 4; Windows	iOS, Android, Blackberry	iOS, Android, Symbian, Palm, WebOS	k.A.	Mac, Windows, Linux[1]	iOS, Android, etc.	iOS, Android
Unterstützte Smartphone-Plattformen	iOS, Android, Windows Mobile, Windows Phone, Blackberry, Symbian	iOS, Android, Windows Mobile, Windows Phone 7, Windows CE, Blackberry, Symbian, WebOS	iOS 4 und 5, Android 2.3 und 4, Windows Mobile, Windows Phone, Blackberry	iOS, Android, Windows Phone, Blackberry, Symbian	iOS, Android, Symbian, Palm, WebOS	iOS, Android, Blackberry, Symbian	iOS, Android, Windows Phone, Blackberry, Symbian	iOS, Android, Blackberry etc.	iOS, Android, Windows Phone 7, Blackberry, Symbian S60, Qualcomm Gobi
Was kann die Software in Bezug auf BYOD?	Die Lösung ermöglicht die rasche Inbetriebnahme von Geräten in der Unternehmensumgebung, die Konfiguration und Aktualisierung von Geräteeinstellungen «over the air», die Einhaltung von Sicherheitsrichtlinien und Compliance, den sicheren mobilen Zugang zu Firmenressourcen und die Remote-Löschung von Geräten.	Die Lösung unterstützt selektive, kontextsensitive Unternehmensregeln. Abhängig von Ort, Zeit, Zustand des Gerätes und/oder der Einhaltung der Policies werden die Rechte des Gerätes oder innerhalb von Applikationen beeinflusst. Die Regeln können sowohl statisch als auch über Variablen gesteuert werden.	Verwaltung, Inventarisierung, OS- und Software-Verteilung, Patching, automatisierte Konfiguration sowie Compliance-Kontrolle für Client Devices.	Die Unified-Enterprise-Mobility-Management (EMM)-Plattform von Boxtone bietet eine patentierte Echtzeit-Automation-Technologie, die den gesamten Mobile-Lifecycle adressiert – inklusive Mobile Device Management (MDM), Applikations-Management (MAM), Support- und Operations-Management.	Cisco AnyConnect stellt zuverlässige sowie einfach einzusetzende, verschlüsselte Netzwerk-Verbindung von Notebooks, Tablets und Smartphones bereit, damit mobile Anwender konstanten und sicheren Zugang zu Unternehmensdaten haben.	Mit Cisco Jabber erhalten Anwender Zugang zu Präsenzinformationen, Instant Messaging, Voice, Video, Desktop Sharing und Conferencing.	Teams können in einem Virtual Meeting, das Audio, HD-Video und Echtzeit-Inhaltsaustausch beinhaltet, effektiver zusammenarbeiten. WebEx Meetings ist eine Software-as-a-Service-Lösung. Die hochverfügbare und sichere Service-Delivery-Plattform bietet Performance, Integrationsflexibilität und Sicherheit.	Citrix XenDesktop ist eine Virtualisierungslösung, mit der Windows-Desktops bereitgestellt werden können. Sie liefert virtuelle Desktops und Anwendungen schnell, sicher und benutzerfreundlich an PCs, Macs, Tablets, Smartphones etc.	MDM ermöglicht es, durch die Implementierung von Regeln und Strategien die mobilen Geräte im Griff zu behalten.
Zielgruppe (Anzahl verwaltete/geschützte Geräte)	1 bis unbegrenzt	10 bis 10'000	300 bis 100'000	skalierbar bis über 100'000	k.A.	k.A.	k.A.	1 bis unbegrenzt	100 und mehr
Anzahl Kunden in der Schweiz	10	derzeit im Marktaufbau	9	1	tausende	einige 100	tausende	843	1
Wichtigste Implementierungspartner in der Schweiz	IT Concepts (www.itconcepts.ch)	derzeit im Marktaufbau	Frox (www.frox.com), IT Concepts (www.itconcepts.ch)	Codalis (www.codalis.ch), CSC (www.csc.com/ch), Dell (www.dell.ch), HP (www.hp.com/ch), Xerox/ACS (www.xerox.ch)	alle zertifizierten Cisco-Partner	alle zertifizierten Cisco-Partner	alle zertifizierten Cisco-Partner	Axacom (www.axacom.ch), Bechtle (www.bechtle.ch), Conapro (www.conapro.net), Inserto (www.inserto.ch), Itivity (www.itivity.ch) u.a.	Dell Channel Partner

■ = ja, ❑ = nein; k.A. = keine Angaben; 1) Cross-Plattform-Support

Quelle: Swiss IT Magazine

Software zur Sicherung und Verwaltung von BYOD
Bring your own Device

SECURITY- UND MANAGEMENT-SOFTWARE FÜR BYOD

HERSTELLER	DELL	ERGON INFORMATIK	ERGON INFORMATIK	GOOD TECHNOLOGY	IBM	KASPERSKY LAB	LAN DESK SOFTWARE	MCAFEE
URL	www.kace.com	www.ergon.ch	www.ergon.ch	www.good.com	www.ibm.com	www.kaspersky.ch	www.landesk.de	www.mcafee.com/de
Software-Name	KACE	Airlock	Medusa	Good for Enterprise	IBM Endpoint Manager Produkt-Familie	Kaspersky Open Space Security	LANDesk Management Suite	McAfee Enterprise Mobility Management (McAfee EMM)
Software-Kategorie								
Security	❑	■	■	■	■	■	■	■
Management (Software zur Verwaltung und Organisation der Geräte)	■	❑	❑	■	■	❑[2]	■	■
Weiteres								
Unterstützte Notebook-Plattformen	Mac OS X, Windows, Red Hat Linux	alle	alle	❑	Mac OS X, Windows, Linux etc.	Mac OS X, Windows, Linux, Unix	Mac OS, Windows, Linux	Mac OS X, Windows
Unterstützte Tablet-Plattformen	k.A.	alle	alle	iOS, Android	iOS, Android, Windows Mobile, Symbian	Android	iOS, Android, Windows Phone, Blackberry etc.	iOS, Android
Unterstützte Smartphone-Plattformen	k.A.	alle	alle	iOS, Android, Windows Phone 7.5	iOS, Android, Windows Mobile, Symbian	Android, Windows, Blackberry, Symbian	iOS, Android, Blackberry	iOS, Android, Windows Phone, Blackberry[3]
Beschreibung darüber, was die Software in Bezug auf ByoD kann	KACE ermöglicht es, durch Systems-Management die Sicherheit der Geräte zu gewährleisten.	Zugangssicherung für beliebige mobile Endgeräte auf unternehmenskritische Dienste (z.B. via Active Sync) von aussen wie auch von innen.	Sichere Authentifizierung beliebiger Endgeräte, insbesondere mit X.509 Zertifikaten. NAC/EAP TLS 802.1X für den sicheren Zugriff auf das Firmen- oder Gastnetzwerk für unbekannte Benutzer/Devices. NAC-fähige Router interpretieren über RADIUS das entsprechende Protokoll zur Absicherung des Netzwerkzugangs richtig.	Good for Enterprise ist eine Sandbox-Lösung (auch Container-Lösung genannt). Dadurch werden die geschäftlichen Daten von den privaten Daten vollständig getrennt. Daher besonders gut geeignet als BYOD-Lösung für alle wichtigen mobilen Plattformen.	Einheitliches Management von mobilen Endgeräten, Laptops, Desktops und Servern. Umfassende Funktionalität mit Lifecycle-, Compliance, Power-, Lizenz- und mobiles Endgerätemanagement aus einer Plattform. Echtzeit-Kontrolle und Reporting. Kontinuierliche Richtlinienüberwachung und Wiederherstellung	Mit dem Kaspersky Security Center können der Schutz auf allen Geräten im Firmennetzwerk zentral administriert und kontrolliert werden. Von Desktops über Notebooks und Smartphones bis zu virtualisierten Maschinen sind alle Einstellungen, Policies und Berichte hier schnell erreichbar.	Vereint Erkennung, Software-Verteilung, Mobilgeräteverwaltung, Betriebssystem-Migration, Remote-Steuerung und Berichterstattung in einer Konsole. Verwaltung, Steuerung und Aktualisierung von PCs, Macs, Laptops und mobilen Geräten – von jedem Ort aus. Innerhalb und ausserhalb der IT-Infrastruktur.	McAfee EMM bietet Sicherheit und Kontrolle für mobile Geräte, einschliesslich Identifizierung, Kennzeichnung und Zuweisung von Richtlinien. Es kombiniert sicheren Zugang zu mobilen Anwendungen, Malware-Schutz, starke Authentifizierung, hohe Verfügbarkeit, skalierbare Architektur und Compliance-Berichte.
Zielgruppe der Software (Anzahl verwaltete/geschützte Geräte)	10 bis 10'000[1]	unbegrenzt	unbegrenzt	ab 50	ab 100	je nach Kunden-Anforderung	1 bis 100'000	unbegrenzt
Anzahl Kunden in der Schweiz	> 30	150	70	150	k.A.	k.A.	34	k.A.
Wichtigste Implementierungspartner in der Schweiz	Cosus (www.cosus.de), Frey + Cie Telecom (www.freytelecom.ch), Inginia (www.inginia.ch) u.a.	grosse Outsourcing-Partner (T-Systems, Swisscom), Security-Integratoren, E-Commerce- und E-Banking-Hersteller	Integrationspartner für spezifische Projekte	Comdirect (www.comdirect.ch)	k.A.	LAN Expert (www.lanexpert.ch), SITC Services for IT & Communications (www.sitcag.ch), Softwareone (www.softwareone.ch)	Axept (www.axept.ch), Binary (www.binary.ag), Insight Technology Solutions (www.ch.insight.com)	BW Digitronik (www.bwdigitronik.ch), E-secure (www.e-secure.ch), Go4mobile (www.go4mobile.ch), Omicron (www.omicron.ch), Softwareone (www.softwareone.com)

■ = ja, ❑ = nein; k.A. = keine Angaben; 1) je nach Konfiguration der Appliances; 2) zentrale Verwaltung der Schutzprogramme auf allen Geräten möglich; 3) Blackberry: Reports werden in den ePO importiert, um dem Kunden eine ganzheitliche Sicht zu geben. Aber kein Management von Blackberry.

Quelle: Swiss IT Magazine

Software zur Sicherung und Verwaltung von BYOD
Bring your own Device

SECURITY- UND MANAGEMENT-SOFTWARE FÜR BYOD

HERSTELLER	MICROSOFT	MOBILEIRON	NORMAN DATA DEFENSE SYSTEMS	NORMAN DATA DEFENSE SYSTEMS	SAP	SAGE SCHWEIZ	SOPHOS	SYMANTEC	TREND MICRO
URL	www.microsoft.ch	www.mobileiron.com	www.norman.ch	www.norman.ch	www.sap.ch	www.sageschweiz.ch	www.sophos.de	www.symantec.ch	www.trendmicro.de
Software-Name	Windows Intune	MobileIron Virtual Smartphone Platform (VSP)	Norman Device Control	Norman Application Control	SAP Afaria	Sage Cockpit Mobile	Sophos Mobile Control	Mobile Management 7.2	Mobile Security
Software-Kategorie									
Security	■	■	■	■	■	■	■	■	■
Management (Software zur Verwaltung und Organisation der Geräte)	■	■	■	■	■	❑	■	■	■
Weiteres									
Unterstützte Notebook-Plattformen	Windows 7 Enterprise, Ultimate und Professional; Windows Vista Enterprise, Ultimate und Business; Windows XP Professional mit Service Pack 2[1]	❑	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	alle	Mac OS X, Windows, Linux	❑	❑	Mac OS, Windows
Unterstützte Tablet-Plattformen	ab iOS 4.0, ab Android 2.1	iOS, Android, Windows Phone, WebOs	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	iOS, Android, Blackberry etc.	iOS, Windows	iOS, Android	iOS, Android, Windows 7	iOS, Android
Unterstützte Smartphone-Plattformen	ab iOS 4.0, ab Android 2.1, ab Windows Phone 7 (7.0)	Android, iOS, Windows Phone, Blackberry, Symbian, WebOS	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	Agent wird auf Windows installiert, zu überwachende Devices sind unabhängig vom Betriebssystem.	iOS, Android, Blackberry etc.	iOS, Windows	iOS, Android, Windows Phone, Blackberry	iOS, Android, Windows Mobile, Windows Phone, Blackberry, Symbian	iOS, Android, Windows Phone, Blackberry etc.
Beschreibung darüber, was die Software in Bezug auf ByoD kann	Integriert mit Hilfe von Active Directory und Microsoft Exchange die Verwaltung mobiler Geräte. Unterstützt wird u.a. das Erstellen von Sicherheitskonzepten für mobile Geräte: Passwortschutz, Verschlüsselung, Fernsperrung, Löschen der Daten, Definieren von Regeln zur Kontrolle des Zugriffs mobiler Geräte.	Schutz vor gefährlichen Apps, Management von Apps, granulare Policies, Integration in IT-Security-Infrastruktur, Zugriffssperre auf Firmennetzwerk für nicht konforme Geräte, Trennung von dienstlichen und privaten Apps und Daten. Bei Ausscheiden eines Mitarbeiters werden nur Firmendaten und Apps gelöscht.	Norman Device Control ermöglicht das Erstellen und Überwachen von Richtlinien für die Nutzung von Wechseldatenträgern, erlaubt die Verwaltung von Geräten und Daten mit Whitelist/Default Deny-Methode, sowie die Implementation von Kopier-Beschränkungen, Dateityp-Filterungen und Verschlüsselungsrichtlinien.	Norman Application Control verwaltet, überwacht und kontrolliert Anwendungen zentral mit Hilfe einer Whitelist-Strategie, die nur die Ausführung von autorisierten Anwendungen ermöglicht und sicherstellt, dass weder Malware noch unerwünschte und nicht lizenzierte Software im Netzwerk ausgeführt wird.	Umfassende Verwaltung von mobilen Geräten: Durchsetzung von Sicherheitsanforderungen (z.B. Remote-Wipe-Funktion, minimale Passwort-Anforderungen), Verwaltung von Geschäftsapplikationen ohne Beeinträchtigung von persönlichen Daten, Self-Service Portal, Telecom Expense Management, volle Skalierbarkeit.	Sage Cockpit Mobile ist eine Web-basierte Business-Intelligence-Anwendung, welche für das iPhone optimiert ist. Sie dient als Management-Cockpit und ermöglicht, gekoppelt an eine Sage-Lösung, die Abfrage und Darstellung von Statistikdaten (Verkauf, Umsatz etc.) auf mobilen Endgeräten.	Sophos Mobile Control (momentan Version 2.0) beinhaltet ein Self-Service Portal, womit sich Nutzer selbständig anmelden können, um danach z.B. Firmen-E-Mail auf dem Privatgerät zu lesen und Schutzfunktionen wie remote lock und remote wipe bei Verlust/Diebstahl abzubilden.	Mobile Geräte lassen sich sicher ins Firmennetz einbinden, und die darauf gespeicherten Daten werden geschützt. Es lassen sich plattformübergreifende Richtlinien definieren, Sicherheitskonfigurationen durchsetzen, private App-Stores einrichten und private von geschäftlichen Daten auf dem Gerät trennen.	Mit Trend Micro Mobile Security können die Verwendung von Kennwörtern auf mobilen Geräten durchgesetzt, Daten verschlüsselt und von verloren gegangenen oder gestohlenen Geräten per Fernzugriff gelöscht werden. Zudem kann Plattformabhängig der Schutz durch das Scannen nach Malware erweitert werden.
Zielgruppe der Software (Anzahl verwaltete/geschützte Geräte)	1 bis 20'000	50 bis mehrere 1000	10 bis unbegrenzt	10 bis unbegrenzt	1 bis 100'000	k.A.	ab 10	>10	ab 26
Anzahl Kunden in der Schweiz	k.A.	rund 75	k.A.	k.A.	k.A.	1	30	k.A.	k.A.
Wichtigste Implementierungspartner in der Schweiz	Microsoft Partner	Getronics (www.getronics.ch), Nomasis (www.nomasis.ch), Swisscom (www.swisscom.ch)	Reseller-Netzwerk	Reseller-Netzwerk	16 Schweizer SAP-Partner	Elvadata (www.elvadata.ch)	k.A.	Ontrex (www.ontrex.ch)	k.A.

■ = ja, ❑ = nein; k.A. = keine Angaben; 1) SP3 wird empfohlen

Quelle: Swiss IT Magazine

SECURITY- UND MANAGEMENT-SOFTWARE FÜR BYOD

HERSTELLER	T-SYSTEMS	UNITED SECURITY PROVIDERS	UNITED SECURITY PROVIDERS	WEBSENSE
URL	www.t-systems.ch	www.united-security-providers.ch	www.united-security-providers.ch	www.websense.de
Software-Name	Sichere Mobile Kommunikation (SiMKo)	USP Network Authentication System	USP Secure Entry Server	Triton Mobile Security
Software-Kategorie				
Security	■	■	■	■
Management (Software zur Verwaltung und Organisation der Geräte)	■	■	❑	■ 4)
Weiteres				
Unterstützte Notebook-Plattformen	Windows XP, 7, 8 1)	Herstellerunabhängig 2)	Herstellerunabhängig 2)	Mac OS X, Windows
Unterstützte Tablet-Plattformen	Android	Herstellerunabhängig 3)	Herstellerunabhängig 3)	iOS
Unterstützte Smartphone-Plattformen	Android, Windows Mobile	Herstellerunabhängig 3)	Herstellerunabhängig 3)	iOS
Beschreibung darüber, was die Software in Bezug auf ByoD kann	SiMKo ist derzeit die einzige Lösung für den mobilen Groupware-Zugriff und die Datensynchronisation nach dem Sicherheitsstandard VS-NfD mit Einsatzempfehlung des BSI und wurde für den Einsatz im öffentlichen Bereich und für Unternehmungen mit höchsten Anforderungen an mobile Sicherheit konzipiert.	Beim Zugriff mit einem mobilen Endgerät auf einen firmeninternen Dienst wie CRM etc. wird das Gerät identifiziert und je nach Bestimmung in das passende Netzwerk verbunden. Die Lösung authentisiert das mobile Gerät und holt sich die für den Zugangsentscheid nötigen Zustandsinformationen aus einem MDM-System.	Beim Zugriff mit einem mobilen Endgerät auf eine Webanwendung via Internet identifiziert die Lösung Anwender und Gerät und verbindet je nach Bestimmung des Geräts auf die Zielsysteme. Die Lösung authentisiert den Anwender und holt sich die für den Zugangsentscheid nötigen Zustandsinformationen aus einem MDM-System.	Websense Triton Mobile Security ermöglicht es Unternehmen, mobile Endgeräte im Arbeitsumfeld sicher einzusetzen. Mit datensensitiven Verteidigungsmassnahmen und mobiler DLP für E-Mail können Unternehmen Datenverlust und den Diebstahl geistigen Eigentums verhindern.
Zielgruppe der Software (Anzahl verwaltete/geschützte Geräte)	10 bis 10'000	100'000	unbegrenzt	ab 10
Anzahl Kunden in der Schweiz	0	20	80	50 in Mitteleuropa
Wichtigste Implementierungspartner in der Schweiz	Compass Security (Beratung, Prüfung, Konzeption; www.csnc.ch)	BNC Business Network Communications (www.bnc.ch), Connectis (www.connectis.ch), Terreactive (www.terreactive.ch)	Clounet (www.clounet.ch), Everyware (www.everyware.ch), In4U (www.in4u.ch), Open Systems (www.open.ch)	Infoguard (www.infoguard.ch)

■ = ja, ❑ = nein; k.A. = keine Angaben; 1) weitere auf Anfrage; 2) IEEE 802.3, IEEE 802.1X; 3) IEEE 802.1X; 4) vollständig Cloud-basiert

Quelle: Swiss IT Magazine