

Vertrauen schaffen in mobile Zugänge™

Wie die iPass Policy Orchestration die Durchsetzung von Sicherheitslösungen für Endgeräte und Netze garantiert

- **Schließen Sie Lücken in der mobilen Sicherheit, indem Sie diverse iPass-Zugangsservices und führende Tools für die Unternehmenssicherheit koordinieren.**
- **Schützen Sie Nutzeridentitäten, mobile Ende-zu-Ende-Systeme, Sitzungsdaten und Ihr Unternehmensnetz.**
- **Koordinieren Sie die Nutzung von führenden VPNs, Personal Firewalls, Anti-Virus-Paketen und Patch-Management-Systemen.**
- **Setzen Sie Sicherheits- und Zugangsrichtlinien universell durch, indem Sie sicherstellen, dass die Nutzer beim Zugriff auf Ihr Netz sämtliche Prüfpunkte passieren.**



ERKENNEN VON LÜCKEN IN DER SICHERUNG MOBILER ENDGERÄTE

Die Tatsache, dass viele Mitarbeiter über mobile und Remote-Netzgänge arbeiten, stellt eine der größten Sicherheitsrisiken für betriebliche Assets und Abläufe dar. Sicherheitslücken durch ungeschützte Endgeräte mit Internetzugang können erhebliche geschäftliche, finanzielle und rechtliche Risiken mit sich bringen. Aus diesem Grund steht die Sicherung der mobilen und Remote-Zugriffe auf Platz Eins der Prioritätenliste heutiger Unternehmen.

Am schwierigsten lassen sich Remote- und mobile Computer sichern, die fernab des Unternehmens eingesetzt werden. Die Bedrohung durch Viren und andere über das Internet verbreitete Gefahren, die Sicherheitslücken aufgrund von veralteter oder fehlerhaft konfigurierter Security Software nutzen, ist für diese Systeme am größten. Wenn derartige Attacken erfolgreich sind, kommt es nicht nur zu einem dramatischen Verlust an Produktivität der Endnutzer, sondern es besteht auch eine handfeste Gefahr für persönliche und Unternehmensdaten, die Funktionsfähigkeit von Laptops und das Unternehmensnetz selbst. Die Wiederherstellung der Systeme ist notwendig, jedoch kompliziert, da mobile und Remote-Endgeräte unter Umständen nur gelegentlich eine Verbindung zum Unternehmensnetz herstellen. Dies macht den Einsatz von Desktop-basierten Systemen zur Fehlerbehebung wenig wirksam.

Um die Sicherheit von Endgeräten und Firmennetz zu stärken, setzen die Unternehmen in der Vergangenheit auf eine Vielzahl von Endpoint-Sicherheitsprodukten für den Schutz der immer wieder auftretenden Schwachstellen. Angesichts der heutigen Bedrohungslage kann auf derartige Maßnahmen nicht verzichtet werden. Gleichzeitig arbeiten diese Sicherheitsprodukte in der Regel jedoch isoliert voneinander, erschweren den Nutzerzugang und sind nicht in der Lage, eine konsistente Durchsetzung der Sicherheitsrichtlinien des Unternehmens zu gewährleisten. Diese Tatsache verstärkt noch die Gefahr, die von Remote- und mobilen Mitarbeitern ausgeht, wenn sie über das Internet eine Verbindung zum Unternehmensnetz herstellen.

“TRUSTED MOBILITY” – SICHERE VERBINDUNGEN FÜR EINEN EFFEKTIVEN SCHUTZ DES UNTERNEHMENS

Damit wichtige Unternehmensassets wirksam gegen diese zugangsbasierten Bedrohungen geschützt sind, entwickelte iPass unter der Bezeichnung „Policy Orchestration“ ein eigenes Sicherheitskonzept. Mit einer Fülle von Funktionen zentraler iPass-Services und einer nahtlosen Technologie-Integration versetzt die Policy Orchestration Unternehmen in die Lage, einen globalen Zugang zu ihrem Netz zu schaffen und dabei ein Höchstmaß an Kontrolle und Richtlinienkonformität sicherzustellen. Dies beinhaltet die konsequente Anwendung von Sicherheitsprodukten bei sämtlichen mobilen und Remote-Internetverbindungen.

Mit dem Policy Orchestration-Konzept beschreibt iPass neue Wege vom grundlegenden Schutz von Authentifizierungsprozessen und Sitzungsdaten (sicherer Remote-Zugang) zur so genannten „Trusted Mobility“, die sich durch eine leistungsfähige, lückenlose Richtlinienumsetzung auszeichnet, mit der sowohl Endgeräte als auch Unternehmensnetze wirksam geschützt werden. Mit eigens konzipierten Services, die an zentralen Stellen des Verbindungsprozesses ansetzen, sorgt iPass für die Integration, Koordination und Durchsetzung von Richtlinien und schließt so Sicherheitslücken mit Blick auf Endgeräte und Netze.

Die vertrauenswürdige mobile Kommunikation stützt sich auf die folgenden Kernelemente:

iPass Corporate Access™: Dieser Service garantiert Ihren Mitarbeitern den weltweiten Netzzugang durch analoge oder ISDN- Einwahl, über Mobilfunknetze, per mobilen Breitbanddienst Connexion by BoeingSM für den Internetzugang im Flugzeug oder mehr als 20.000 Wi-Fi-Zugangspunkten, darunter eine Vielzahl von T-Mobile® HotSpot-Standorten in den USA.

iPassConnect™-Client: Stellt eine übersichtliche, konsistente Benutzeroberfläche für sämtliche Zugangsoptionen innerhalb und außerhalb des iPass-Netzes zur Verfügung. Der Client dient außerdem als zentraler Koordinationspunkt für die



intelligente Anwendung Ihrer Sicherheitsrichtlinien auf alle Verbindungsarten.

Policy Orchestration: Dieses Konzept beinhaltet Services, die Schwachstellen in der Sicherung der mobilen Zugänge beheben, und koordiniert hierzu diverse iPass-Zugangsservices und führende Tools für die Unternehmenssicherheit.

LÜCKENLOSE SICHERHEIT DURCH DIE IPASS POLICY ORCHESTRATION

Wenn Sicherheitstools isoliert vom Zugangsdienst des Unternehmens arbeiten, entstehen leicht Lücken bei der Richtliniendurchsetzung. Unabhängig davon, ob sich die Nutzer über einen DSL-Anschluss ohne Personal Firewall anmelden oder auf ungesicherte Wi-Fi-Netze zugreifen – der Verzicht auf wichtige Sicherheitspatches macht sie stets zu idealen Ziele für Wurm- und Virentacken oder sogar noch schlimmeren Bedrohungen.

Die iPass Policy Orchestration schließt diese gefährlichen Lücken, indem Sicherheits- und Zugangstechnologien intensiv miteinander verwoben werden. Möglich wird dies durch die nahtlose Integration des iPassConnect-Client mit einer ganzen Palette von Sicherheitsservices. Durch das Zusammenspiel führender Tools für die Authentifizierung, Autorisierung und Patchverwaltung sorgt die Policy Orchestration für einen wirksamen Schutz von Nutzeridentität, mobilen und Remote-Systemen und Unternehmensnetz gleichermaßen.

Dieser einmalige, herstellerübergreifende Ansatz ermöglicht IT-Experten die gezielte Durchsetzung von Sicherheitsrichtlinien für den Internet- und VPN-Zugang unabhängig davon, welches Verbindungsverfahren die Nutzer im Einzelnen verwenden. Dies gilt sogar für nicht von iPass bereitgestellte Netze. Zugriff erhalten nur Nutzer und Endgeräte, die die entsprechenden Endpoint-Sicherheitsrichtlinien einhalten. Wenn die Sicherheitssoftware eines Endgeräts nicht ausgeführt wird oder veraltet ist, werden entweder Sofortmaßnahmen zur Behebung der Sicherheitslücke eingeleitet, oder der Zugang wird gesperrt.

Zur praktischen Umsetzung dieser Vorgaben nutzt die iPass Policy Orchestration einen sicheren Verbindungsprozess, mit dem IT-Abteilungen die Kontrolle über den Netzzugang behalten, während gleichzeitig die Sicherheit und Produktivität der Nutzer gewährleistet ist. Dieser Prozess besteht aus insgesamt sechs Komponenten, die für einen maximalen Nutzen als Einheit, bei Bedarf jedoch auch in einzelnen Phasen implementiert werden können.



Die Funktionsweise der Policy Orchestration Beim Versuch eines Internetzugriffs wird das Endgerät gesperrt. Der VPN-Zugang wird nur gewährt, nachdem eine Reihe von Prüfpunkten erfolgreich passiert wurden; dazu zählt auch die Sofortbehebung von Sicherheitsproblemen. Außerdem wird durch das Zusammenwirken mit führenden Lösungen für die Netzsicherheit ein zuverlässiger Schutz der Unternehmensnetze gewährleistet.

VERTRAUENSWÜRDIGE NETZE

Das globale, virtuelle iPass-Netz hebt die Netzsicherheit auf eine völlig neue Stufe. Jeder Netzanbieter muss über eine „Enterprise Ready“-Zertifizierung verfügen und wird strengsten Tests hinsichtlich Dienstqualität und Kompatibilität mit Unternehmenssystemen unterzogen.

Mit den folgenden Maßnahmen sorgt das iPass-Netz für eine hundertprozentig zuverlässige Authentifizierung:

iPass Secure End-to-End Encrypted Login (ISEEL): Mittels modernster „Public Key“-Verschlüsselung werden Passwörter gegen Diebstahl und Replay-Attacken geschützt. Mit Hilfe von iSEEL bleiben Passwörter auf ihrem gesamten Weg durch die Netze von Zugangsanbietern und das Internet vollständig verschlüsselt, so dass eine sichere Übertragung gewährleistet ist.

Austausch digitaler Zertifikate: In jeder Phase des Authentifizierungsprozesses, d.h. im gesamten iPass-Netz aus vertrauenswürdigen Zugangsanbietern, findet ein gegenseitiger Austausch digitaler Zertifikate statt. Indem bei jeder Transaktion die Identität der beteiligten Systeme bekannt ist, kann verhindert werden, dass sich Endgeräte mit betrügerischer Absicht in die Authentifizierungsschleife einklinken.

SSL-geschützte Authentifizierung: Zu jedem Zeitpunkt des iPass-Authentifizierungsprozesses werden 128-Bit-SSL-Tunnel verwendet. So ist sichergestellt, dass keine persönlichen Nutzerdaten entwendet oder in einer Replay-Attacke genutzt werden, um unbefugten Zugang zum Unternehmensnetz zu erhalten.

Kunden, die ihre firmeneigenen oder öffentlichen Netze breiter zugänglich machen wollen, können auch für Netze anderer Anbieter auf Funktionen der Policy Orchestration zurückgreifen. Auf diese Weise werden Endgeräte und Netze direkt geschützt, während die Authentifizierungssicherheit beim jeweiligen Netzanbieter liegt.

LOCKDOWN DER ENDGERÄTEUMGEBUNG

iPass bietet die einzigartige Möglichkeit, einzelne Endgeräte zu sperren und vom Internetzugang auszuschließen, während sie sich in einem nicht überprüften und somit nicht vertrauenswürdigen Zustand befinden. Mit dieser Funktion können Endgeräte während der Nutzerauthentifizierung und der Fehlerbehebung vor einer Attacke aus dem Internet geschützt werden.

Endgeräte-Eigenquarantäne: iPassConnect wendet je nach Zugangsstatus unterschiedliche Firewallregeln an. Dies begrenzt den Zugang von Endgeräten auf die iPassConnect-Kommunikation, wobei iPass-Server zur Durchsetzung der Richtlinien verwendet werden; erst nachdem die Konformität des Endgeräts bestätigt wurde, wird die Firewall wieder geöffnet. Diese Vorgehensweise schützt das Endgerät während des Durchsetzungsprozesses vor Angriffen aus dem Internet und verhindert gleichzeitig, dass nicht konforme Endgeräte auf das Internet zugreifen.

DeviceID: Dieser besondere Service stellt die Vertrauenswürdigkeit von Endgeräten sicher, indem die Geräteeigenschaften überprüft, einmal verwendbare Passwörter ausgegeben und beide Faktoren mit der VPN-Authentifizierung verbunden werden. Durch die Authentifizierung auf Endgerätebasis kann die Nutzeridentität mit Endgeräten, die vom Unternehmen genehmigt wurden, sowie mit Anforderungen an spezifische Endgeräte-Security-Software verknüpft werden. So erhalten Sie die notwendige Flexibilität, um strengere Zugangskontrollen anzuwenden und die Einhaltung von Sicherheitsrichtlinien durch die Endgeräte erzwingen zu können, bevor ein VPN-Zugang erteilt wird.

Endgeräte-Eigenquarantäne*: Der iPassConnect-Client wendet je nach Zugangsstatus unterschiedliche Firewallregeln an. Auf diese Weise bleibt die Kommunikation des Endgeräts auf spezifische iPass-Server, die zur Richtlinien-durchsetzung dienen, beschränkt. Nachdem die Endgerätekonformität bestätigt ist, wird die Firewall wieder geöffnet und gestattet dann auch anderweitige Datenübertragungen. Diese Vorgehensweise schützt das Endgerät während des Durchsetzungsprozesses vor Angriffen aus dem Internet und verhindert gleichzeitig, dass nicht konforme Endgeräte auf das Internet zugreifen.

DeviceID™: Dieser besondere Service stellt die Vertrauenswürdigkeit von Endgeräten sicher, indem er die Geräteeigenschaften überprüft, einmal verwendbare Passwörter ausgibt und beide Faktoren mit der VPN-Authentifizierung verbindet. Durch die Authentifizierung auf Endgeräteeigenschaften kann die Nutzeridentität mit Endgeräten, die vom Unternehmen genehmigt wurden, sowie mit Anforderungen an spezifische Endgeräte-Security-Software verknüpft werden. So erhalten Sie die notwendige Flexibilität, um strengere Zugangskontrollen anzuwenden und die Behebung von Sicherheitslücken erzwingen zu können, bevor ein VPN-Zugang erteilt wird.

SICHERE NETZZUGÄNGE

Die Schaffung und Aufrechterhaltung sicherer Zugänge erfordert mehrere, voneinander unabhängige Technologien und Prozesse. Der iPassConnect-Client koordiniert das Zusammenspiel von Personal Firewall, Anti-Virus- und VPN-Software, ohne dass Nutzer oder IT-Mitarbeiter hierfür eingreifen müssen.

SecureConnect: iPassConnect ruft automatisch Firewall-, Anti-Virus- und VPN-Software auf und stellt so sicher, dass das Endgerät zuverlässig geschützt ist, bevor die Authentifizierung des Nutzers für den Zugang zum Internet erfolgt. Bei Kombination mit DeviceID ist - abhängig von der Ausführung anderer Sicherheitstools - auch ein optionaler Start der VPN-Software möglich.

Auto-Teardown: Diese Funktion ergänzt SecureConnect, indem Internetsitzungen beendet werden, falls ein Sicherheitstool nicht mehr ausgeführt wird. Dabei ist es unerheblich, aus welchem Grund die Ausführung beendet wurde. Auf diese Weise ist ein durchgehender Schutz des Endgeräts sichergestellt.

DYNAMISCHE RICHTLINIENANFORDERUNG

Der IT-Administrator kann Richtlinien für die Zugangskontrolle und Sicherheit von einer zentralen Konsole aus implementieren und modifizieren. Nachdem die Identität des Nutzers überprüft und eine Verbindung mit dem Internet hergestellt wurde, werden die betreffenden Richtlinien über den iPassConnect-Client automatisch auf das Endgerät angewendet. Updates können nach den Kriterien Standort, Zugangstyp, Nutzer oder Nutzergruppe aufgespielt werden, so dass für bestimmte Länder Zugriffsbeschränkungen definiert oder einzelne Nutzer von bestimmten Zugangsmodalitäten ausgeschlossen werden können.

Die Sicherheitseinstellungen für sämtliche unterstützten Produkte und Zugangsmethoden können mittels Remote-Zugriff festgelegt werden, ohne dass ein direkter Eingriff am Endgerät notwendig oder der Nutzer bei seiner Arbeit beeinträchtigt wird. Die Änderungen lassen sich jederzeit vornehmen und werden auf die Endgeräte der Nutzer aufgespielt, sobald diese eine Verbindung zum Internet herstellen.

REMOTE-SCHWACHSTELLENANALYSE UND-BEHEBUNG

Das simple Sperren von Nutzern, die nicht den Sicherheitsrichtlinien entsprechen, bringt erhebliche Einbußen bei der Produktivität

mit sich. Aus diesem Grund ist ein Mechanismus notwendig, der bei einer Richtlinienverletzung korrigierend eingreift.

Endpoint Policy Management™: Dieser iPass-Service ermöglicht die automatische Schwachstellenanalyse und -behebung bei mobilen Systemen über eine beliebige Internetverbindung. Nach der dynamischen Richtlinienanforderung ruft der iPassConnect-Client den Endpoint Policy Management-Service auf und überprüft, ob das Endgerät die aktuellen, auf einem zentralen Server gespeicherten Sicherheitsrichtlinien erfüllt. Der Service lädt und installiert die notwendigen Sicherheitspatches und Virensignaturen, um so die Richtlinienkonformität des Endgeräts herzustellen. Endpoint Policy Management ist als Ergänzung zu Standardprodukten für die Softwareverteilung gedacht und sorgt dafür, dass auch Endgeräte, die nur von Zeit zu Zeit auf das Firmen-LAN zugreifen, stets auf dem neuen Sicherheitsstand sind.

Universelle Richtlinien-durchsetzung: Durch die Kombination der drei hier vorgestellten, leistungsstarken iPass-Sicherheitslösungen können Sie sich darauf verlassen, dass Ihre Sicherheits- und Zugangsrichtlinien universell

DIE VORTEILE DER POLICY ORCHESTRATION AUF EINEN BLICK

Verlässliche Richtlinien-durchsetzung durch effiziente Koordination: Mit dem iPassConnect-Client sichern Sie sich die Kontrolle über den VPN-Zugriff auf Ihr Unternehmensnetz. So können Sie sich darauf verlassen, dass Zugangs- und Sicherheitsrichtlinien bis ins Detail eingehalten werden und nur konformen Endgeräten der Zugang erteilt wird.

Integrierte Schwachstellenanalyse und -behebung: Bringen Sie die Endgerätesoftware über das Internet auf den neuesten Stand, und stellen Sie so sicher, dass die Endgeräte bei jedem Verbindungsversuch geschützt sind, ohne dass den Nutzern grundlos der Zugang verwehrt wird.

Höchstmaß an mobiler Produktivität: Unterstützen Sie Ihre mobilen und Remote-Nutzer durch eine sichere Zugangslösung, die für ein Plus an Produktivität sorgt, indem die Einhaltung von Richtlinien ohne großen Aufwand jederzeit gewährleistet ist.

Unterstützung beliebiger Internetverbindungen: Setzen Sie VPN-Zugangsrichtlinien konsequent durch, und sichern Sie sich eine umfassende, richtlinienbasierte Kontrolle über den Netzzugang Ihrer Nutzer - unabhängig davon, ob dies über das globale, virtuelle iPass-Netz oder über Netze anderer Anbieter geschieht.

Komfortable, zentralisierte Kontrolle: Nutzen Sie das iPass-Portal, um Ihre Zugangsrichtlinien bequem von einer zentralen Stelle aus durchzusetzen.

Flexible, offene Architektur: Holen Sie das Maximum aus Ihrer Investition durch die reibungslose Integration der iPass-Services in führende Sicherheitsprodukte, die auf Ihre Anforderungen zugeschnitten sind.



Anwendung finden. iPass Connect stellt sicher, dass die Nutzer beim Zugriff auf das Internet sämtliche Prüfpunkte passieren, DeviceID sorgt für einen sicheren VPN-Zugang, und Endpoint Policy Management erhöht die Sicherheit durch eine obligatorische Schwachstellenanalyse und -behebung. Zusammengefasst garantieren diese drei Lösungen, dass der VPN-Start nur nach einer positiven Endgeräte-Authentifizierung und eventuellen Fehlerbehebung erfolgt. Indem DeviceID ein einmal verwendbares Passwort ausgibt, kann iPassConnect nur dann eine VPN-Verbindung herstellen, wenn das Endgerät sämtliche Prüfpunkte erfolgreich passiert hat, bei Bedarf die entsprechenden Korrekturmaßnahmen durchlaufen hat und als richtlinienkonform eingestuft wurde. Somit lässt sich der Zugang auf zuverlässig geschützte Endgeräte beschränken und garantieren, dass mobile und Remote-Mitarbeiter die Sicherheitsupdates erhalten, die sie für einen Zugang zum Unternehmensnetz und eine produktive Tätigkeit benötigen.

KOORDINIERTER RICHTLINIEN-DURCHSETZUNG IM NETZ

Mit iPass ist Ihr Unternehmensnetz vor einer Gefährdung durch Nutzer, die über das VPN eine Verbindung herstellen, zuverlässig geschützt. Gleichzeitig droht jedoch noch von anderer Seite Gefahr – von Endgeräten, die über das LAN zugreifen möchten. Aus diesem Grund setzt iPass auf die Integration in führende Produkte für die Netzdurchsetzung. Durch die Einbindung der entsprechenden Funktionen in die iPass Policy Orchestration erhält Ihre IT-Abteilung die notwendigen Daten, um fundierte Entscheidungen hinsichtlich der Endgeräte zu treffen, die auf das Unternehmensnetz zugreifen möchten. Diese zusätzlichen Informationen machen die iPass-Lösung zu einem effizienten Instrument, das sehr viel leistungsfähiger ist, als es isolierte Einzelprodukte jemals

sein können. Gleichzeitig kann die Policy Orchestration auch Patch-Management-Systeme von Drittherstellern, mit denen Netzsysteme auf notwendige Anwendungsupdates überprüft werden, mit wertvollen Informationen versorgen. Welche Systeme auch immer in Ihrem Unternehmen vorhanden sind – mit iPass lassen sie sich intelligenter nutzen.

KONTROLLE OHNE KOMPROMISSE

Das iPass „Policy Orchestration“-Konzept und die zugehörigen Technologien heben den mobilen und Remote-Netzzugang auf eine völlig neue Ebene, bieten zusätzliche Security Services für optimal geschützte Endgeräte und leisten einen wichtigen Beitrag zur Sicherheit des Unternehmensnetzes insgesamt. Der Zugriff von Remote- und mobilen Nutzern auf das Firmennetz steckt voller Gefahren und muss sorgfältig kontrolliert werden. Diese Aufgabe wird Ihnen nun erheblich leichter gemacht: Mit der iPass Policy Orchestration erhalten Sie die uneingeschränkte Kontrolle über mobile und Remote-Endgeräte, die auf das Unternehmensnetz zugreifen. Auf diese Weise können Sie die notwendige Sicherheit gewährleisten, ohne die Produktivität der Mitarbeiter und die Effizienz der IT-Abteilung zu schmälern. Weitere Informationen erhalten Sie unter www.ipass.de.

EINE NEUE EBENE DER UNTERNEHMENSICHERHEIT

Die iPass-Services sind in Produkte der folgenden führenden Hersteller integriert. Eine ausführliche Liste der einzelnen Produkte ist unter www.ipass.com abrufbar.

Virtual Private Networks

- Aventail
- Check Point
- Cisco Systems
- Juniper
- Microsoft
- NCP
- Nortel Networks

Personal Firewalls und Intrusion Detection-Systeme

- Check Point (Zone Labs)
- Internet Security Systems
- Sygate

Anti-Virus-Software

- Computer Associates
- McAfee
- Symantec
- Trend Micro

AAA

- Active Directory
- RADIUS
- LDAP

Produkte für die Durchsetzung im Netz

- iPass ist mit Produkten der folgenden Hersteller interoperabel:
- Check Point (Zone Labs)
 - ENDFORCE
 - InfoExpress

- Nortel
- Senforce
- Sygate

Mitgliedschaft in Branchenverbänden

- iPass ist Mitglied in den folgenden Verbänden:
- Cisco Network Access Control
 - Microsoft Network Access Protocol
 - TCG Trusted Network Connect

*Für die Eigenquarantäne ist eine Integration in Sygate-Produkte erforderlich.

iPass Deutschland GmbH
Wiener Platz
D-81667 München

+49 89 44 142 – 100
+49 89 44 142 – 111 fx

www.ipass.de

