

CA Host-Based Intrusion Prevention System r8

CA HOST-BASED INTRUSION PREVENTION SYSTEM (CA HIPS) VERBINDET EINE STANDALONE-FIREWALL MIT WARN- UND ABWEHRFUNKTIONEN GEGEN ANGRIFFE VON AUßEN UND ERMÖGLICHT AUF DIESE WEISE EINEN ZENTRALEN UND PROAKTIV WIRKSAMEN SCHUTZ VOR ONLINE-BEDROHUNGEN. GEMEINSAM MIT DEN SIGNATURBASIERTE TECHNOLOGIEN SORGT DER VERHALTENSGESTEUERTE ECHTZEITSCHUTZ FÜR ZUGRIFFSSTEUERUNG AUF HÖCHSTEM SICHERHEITSNIVEAU, RICHTLINIENDURCHSETZUNG UND DIE ABWEHR VON EINDRINGLINGEN ÜBER EINE EINZELNE, INTUITIV BEDIENBARE KONSOLE.

Überblick

Bösartiger Code und Blended Threats (komplexe Malware) entwickeln sich zu schnell für den herkömmlichen Bedrohungsschutz. Sie benötigen einen komplexen, mehrstufigen Abwehrmechanismus, der verschiedene Maßnahmen für die Sicherheit von Endgeräten kombiniert.

CA HIPS kombiniert eine Standalone-Firewall mit einem Warn- und Abwehrsystem gegen Angriffe von außen (Intrusion Detection and Prevention System), wodurch signaturbasierte Technologien mit zentral verwalteten, proaktiven Schutzmechanismen gegen bekannte und unbekannte Online-Bedrohungen ergänzt werden.

Nutzen

Durch die Erweiterung Ihres vorhandenen Verteidigungssystems um CA HIPS können Sie den Schutz Ihrer Arbeitsplatz-Computer um eine zentrale Zugriffssteuerung und Funktionen zur Richtliniendurchsetzung erweitern.

Eine Reihe bekannter und unbekannter Bedrohungen wird effektiv blockiert, wodurch einerseits das Ausfallrisiko sinkt und andererseits geringere bis gar keine Aufwendungen für Gegenmaßnahmen bzw. Helpdesk-Aktivitäten anfallen. Dies führt zu einer gesteigerten betrieblichen Effizienz und einer höheren Produktivität der Endanwender und IT-Mitarbeiter, sodass die Verfügbarkeit der Services sichergestellt ist (Service-Continuity).

Vorteile

CA HIPS ergänzt andere CA-Produkte für das Threat Management und bildet gemeinsam mit diesen ein umfassendes, mehrstufiges Bollwerk gegen bekannte und unbekannte Bedrohungen.

Die Sicherheitslösungen von CA gehören zu den Grundkomponenten der übergeordneten CA-Strategie des Enterprise IT Management (EITM), die Sie bei der Vereinheitlichung, Vereinfachung und Sicherung des Technologie-Managements unterstützt.

CA HIPS: Kombinierte Verteidigungsmechanismen gegen Blended Threats

Das Phänomen Malware hat sich von einem Sport der Amateurracker, die sich gern mit der erfolgreichen Umgehung von Zugangsrechten brüsten, zu einem Akt der Wirtschaftskriminalität gewandelt, mit dem Software-Experten unrechtmäßige Ziele verfolgen. Diese Crimeware-Autoren verwenden ausgereifte Kombinationen aus Angriffstechniken, um herkömmliche Produkte für den Bedrohungsschutz zu überlisten. Als Ziel wählen sie den schnell wachsenden und immer vielfältiger werdenden Markt für Remote-Geräte und mobile Endgeräte. Mit den so genannten „Zero-Day-Attacken“ nutzen sie zudem die Möglichkeiten aus, die ihnen gerade erst bekannt gewordene Schwachstellen bieten.

Signaturbasierte Virenschutz- und Anti-Spyware-Produkte spielen in der Endgerätesicherheit eine wichtige Rolle. Hierbei handelt es sich jedoch um reaktive Technologien mit einer gewissen Echtzeit-Diskrepanz, die durch das Aufkommen von Blended Threats und Zero-Day-Attacken noch gravierendere Folgen haben kann. Blended Threats verlangen nach mehrstufigen und kombinierten Verteidigungsmechanismen, während sich Zero-Day-Attacken nur mit einer proaktiven, verhaltensgesteuerten Schutzlösung abwehren lassen.

CA HIPS ist eine leistungsstarke 3-in-1-Lösung für den Bedrohungsschutz, die in einem zentralen, richtlinienbasierten Management-System eine Standalone-Firewall mit Intrusion Detection- und Intrusion-Prevention-Funktionen kombiniert. Mit CA HIPS können Sie den Netzwerkverkehr und das Systemverhalten beobachten und auf bestimmte Auffälligkeiten überwachen, die häufig neue Bedrohungen ankündigen.

Diese hostbasierte Software schützt Endgeräte auch dann noch, wenn sie nicht mit dem Netzwerk verbunden sind. Beim erneuten Anschluss der Geräte an das Netzwerk verteilt die Serverkomponente automatisch alle neuen Richtlinien-Updates an diese.

CA HIPS bietet ein ausgereiftes Richtlinienmanagement mit einer hochgradig intuitiven Benutzeroberfläche. Sie können Sicherheitsregeln basierend auf einer Reihe von Faktoren festlegen, z. B. dem Standort des Benutzers, der Tageszeit oder der jeweiligen Funktion des Benutzers im Unternehmen. Diese Regeln lassen sich dann dynamisch anwenden. Ihre Administratoren können diese stark differenzierten Funktionen zum Festlegen von Richtlinien und einen „Lernmodus“ einsetzen, um CA HIPS an die Prozesse zur Bereitstellung von Software in Ihrem Unternehmen anzupassen.

Leistungsmerkmale

DREI SCHUTZTECHNOLOGIEN IN EINEM PAKET Die Kombination aus einer Standalone-Firewall mit Warn- und Abwehrfunktionen gegen Angriffe von außen ermöglicht den proaktiven Schutz von Endgeräten vor bekannten und unbekanntem Bedrohungen. Zugriffssteuerung, Richtliniendurchsetzung und Bereitstellung werden über eine intuitive, webgestützte Konsole verwaltet.

VERHALTENSGESTEUERTER ECHTZEITSCHUTZ CA HIPS verfügt über einen Lernmodus, mit dem Sie eine Basiskonfiguration für das derzeitige Verhalten des Systems erstellen und entsprechende Sicherheitsrichtlinien anlegen oder anpassen können. Dies ermöglicht Ihnen die Feineinstellung der Auffälligkeitserkennung, um Fehlalarme auszuschließen und den Bedrohungsschutz an die Anforderungen Ihres Unternehmens anzupassen.

ZENTRALES RICHTLINIENMANAGEMENT Durch die zentrale Erstellung, Bereitstellung und Maintenance lassen sich die Sicherheitsrichtlinien einfach und flexibel für das gesamte Unternehmen verwalten. Über die intuitive grafische Benutzeroberfläche können Sie Richtlinien festlegen, anhand derer Regeln für Benutzergruppen, bestimmte Endgerätetypen, Sicherheitsfunktionen und Sicherheitsstufen umgesetzt werden.

DIFFERENZIERTE EINSTELLUNG VON RICHTLINIEN UND REGELN Systemadministratoren können die Zugriffs- und Kontrollebene für ein System, eine Gruppe von Benutzern oder einzelne Benutzer festlegen. Außerdem können sie Richtlinien für einzelne Benutzer festlegen, die zu bestimmten Zeiten oder bei Ausübung einer bestimmten Tätigkeit bzw. bei der Arbeit an bestimmten Standorten gelten.

UMFASSENDES EREIGNISMANAGEMENT Der CA HIPS-Server erfasst die Ereignisse der einzelnen Clients und zeichnet sie auf. Über die bereitgestellten Filter kann der Administrator dann wichtige Ereignisse herausfiltern, wobei die Filterkriterien in einem praktischen Dropdown-Menü ausgewählt werden können.

RICHTLINIENBASIERTE CLIENT-BENUTZEROBERFLÄCHE CA HIPS bietet eine intuitive Client-Benutzeroberfläche für Endanwender. Abhängig von den Richtlinien, die der Systemadministrator festgelegt hat, können Ihre Endanwender die Schutzmechanismen von CA HIPS für die eigenen PCs anzeigen und ändern, um beispielsweise neue Angriffe auf den Desktop abwehren zu können. Diese Funktion wird zentral gesteuert und kann vom Administrator nach eigenem Ermessen aktiviert bzw. deaktiviert werden.

GRAFISCHE BERICHTE ZU TECHNISCHEN ODER GESCHÄFTSBEZOGENEN BEDROHUNGEN Mit Hilfe der grafischen Berichte von CA HIPS können Sie Vorfälle nachverfolgen und nach Mustern suchen. Die grafischen Berichte erleichtern Ihnen das Sammeln, Analysieren, Verstehen und Präsentieren von Informationen zu Bedrohungen. Die Darstellung kann dabei in Tabellenform oder als Torten- bzw. Balkendiagramm erfolgen.

UNTERSTÜTZUNG MEHRERER SPRACHEN FÜR INTERNATIONALE IMPLEMENTIERUNGEN CA HIPS unterstützt die Sprachen Englisch, Französisch, Italienisch, Deutsch, Chinesisch (vereinfacht), brasilianisches Portugiesisch und Spanisch.

ABBILDUNG A:

Der Hauptbildschirm von CA HIPS steuert die CA HIPS-Software in Ihrer Umgebung. Der Administrator kann Richtlinien und Regeln erstellen und diese an alle CA HIPS Clients innerhalb des Unternehmens verteilen.

HAUPTBILDSCHIRM DES ADMINISTRATORS

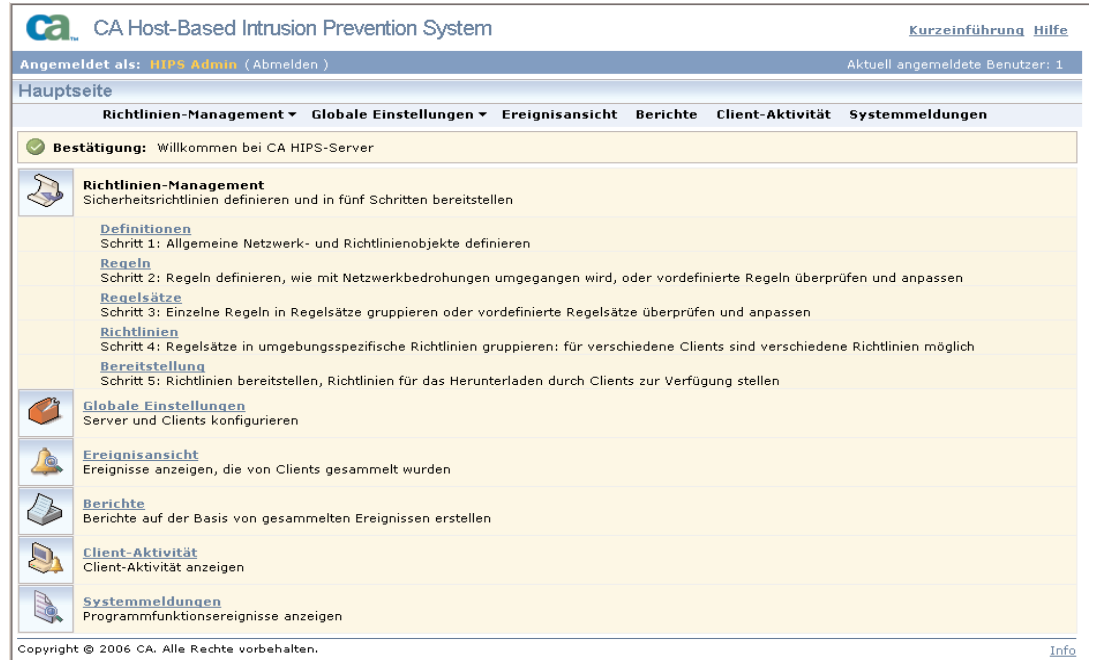
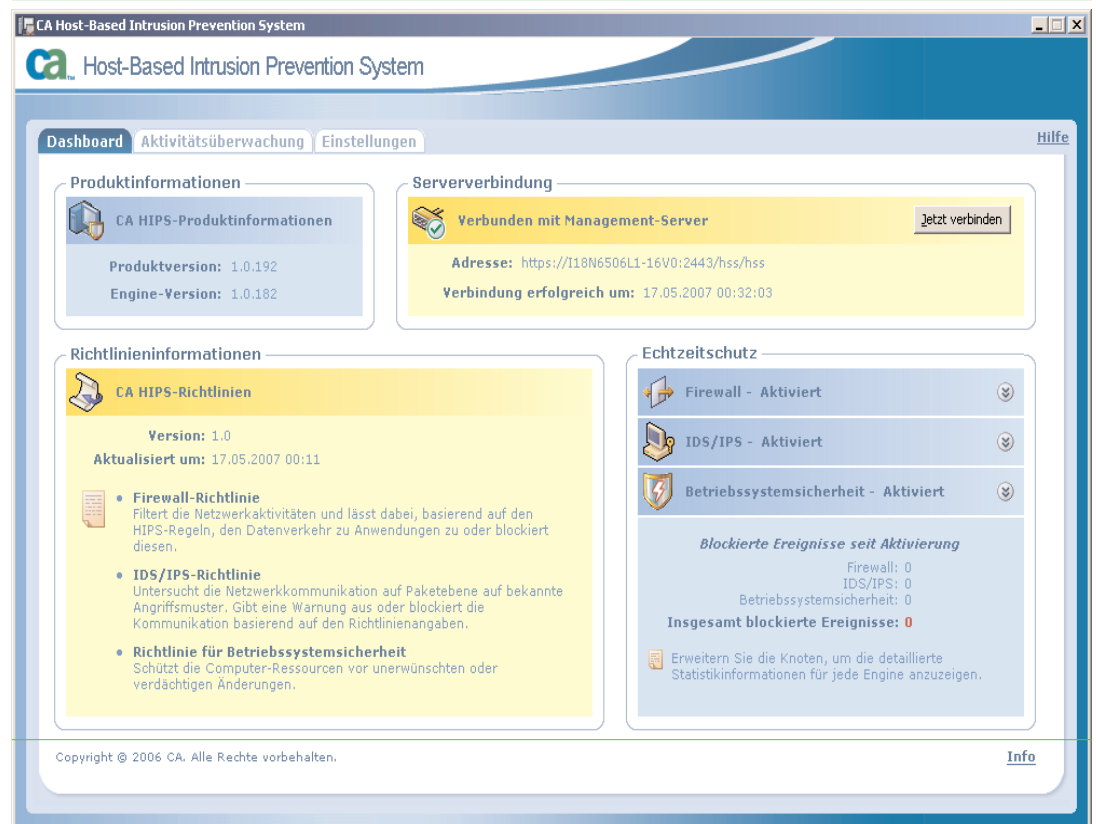


ABBILDUNG B:

Die GUI des CA HIPS Clients macht es für Endbenutzer einfach, neue Attacken auf ihre Desktops abzublocken.

CLIENT-BENUTZEROBERFLÄCHE



CA HIPS schützt Assets, verringert Ausfallzeiten und optimiert die betriebliche Effizienz

Durch Anwendung der CA HIPS-Funktionen für den proaktiven Echtzeitschutz, die zentrale Zugriffssteuerung und Richtliniendurchsetzung können Sie Ihre Endgeräte besser vor bekannten und unbekanntem Bedrohungen schützen. CA HIPS senkt das Ausfallrisiko, weil Malware, Spyware, Adware und bösartige Software nicht mehr über Arbeitsplatz-Computer in das Netzwerk eindringen können. Weniger Infektionen durch Malware sind zudem mit geringeren Aufwendungen für Gegenmaßnahmen und Helpdesk-Aktivitäten verbunden, wodurch sich die betriebliche Effizienz erhöht.

Service-Continuity ist dank der proaktiven Erkennung von Auffälligkeiten in CA HIPS und trotz der Bedrohung durch Zero-Day-Attacken gewährleistet. CA HIPS nutzt wichtige Informationen, damit Systemadministratoren das normale Systemverhalten kennenlernen und Richtlinien zur Erkennung von Auffälligkeiten erstellen können. Dadurch werden Sie in die Lage versetzt, Ihre IT-Ressourcen und -Prozesse zu schützen, damit diese auch bei fehlenden Signatur-Updates stets sicher vor Bedrohungen sind. Auf Grundlage derselben Informationen können Sie den Bedrohungsschutz an Ihre geschäftlichen Anforderungen anpassen, und nicht umgekehrt.

Ausgereifte Sicherheitsmaßnahmen und ein umfassender Bedrohungsschutz sind Teil einer soliden Geschäftspraxis; maßgeblich für den Umfang des Schutzes sind häufig die Art der zu schützenden Informationen und IT-Assets sowie Vorschriften und Gesetze. CA HIPS bietet Ihnen umfangreiche Protokollierungs- und Reporting-Funktionen, die die Einhaltung von Vorschriften erleichtern. Außerdem lässt es sich mit bereits vorhandenen Investitionen in Form herkömmlicher, signaturbasierter Lösungen für den Schutz von Endgeräten kombinieren. Sie erhalten so ein mehrstufiges System für den Bedrohungsschutz, das Bedrohungen, die auf einer Ebene nicht erkannt wurden, ggf. auf einer anderen Ebene als solche klassifiziert und abwehrt.

PRODUKT	FUNKTION	EIGENSCHAFTEN	NUTZEN
CA HIPS	Verbessert den Schutz von Windows-Computern durch die proaktive Überwachung des Netzwerkverkehrs und des Systemverhaltens sowie die Erkennung von Auffälligkeiten.	<ul style="list-style-type: none">• 3-in-1-Schutz• Verhaltensgesteuert• Zentrale Richtlinien• Ausgereiftes Reporting	<ul style="list-style-type: none">• Einfache Installation und Verwaltung• Echtzeitschutz• Differenzierte Steuerung• Einfache Datenanalyse

Vorteile

CA HIPS ergänzt andere Produkte der CA Threat Management-Lösung, die zusammengekommen ein umfassendes, mehrstufiges Schutzsystem vor Viren, Spyware, Adware, bösartiger Software und anderen bekannten sowie unbekanntem Bedrohungen ergeben. Das integrierte Threat Management von CA ist ein wichtiger Bestandteil der allgemeinen CA-Strategie zur Erneuerung des IT-Management-Ansatzes. Das Enterprise IT Management von CA zielt auf die Vereinheitlichung und Vereinfachung des IT-Managements im gesamten Unternehmen ab, damit Sie Ihre Geschäftsergebnisse noch weiter steigern können.

Die nächsten Schritte

Das CA Host-Based Intrusion Prevention System ist ein fertiges Unternehmensprodukt, das das vorhandene Threat Management-System erweitert und optimiert, die Produktivität der Mitarbeiter steigert, die Auslastung von IT-Ressourcen verbessert, die Einhaltung von Vorschriften erleichtert und die Service-Continuity verbessert.

Lassen auch Sie sich überzeugen, wie Sie mit CA HIPS den Schutz von Endgeräten vor bekannten und unbekanntem Bedrohungen verbessern können.

Weitere Informationen finden Sie unter ca.com/de/products. Dort erfahren Sie beispielsweise, wie CA-Softwarelösungen Unternehmen bei der Optimierung ihres IT-Managements zum Erzielen noch besserer Geschäftsergebnisse unterstützen.

**Weitere Informationen, wie CA das
IT-Management vereinheitlicht und vereinfacht,
finden Sie unter:**

CA Deutschland GmbH
ca.com/de

CA Software Österreich GmbH
ca.com/at

CA (Schweiz) IT Solutions Management AG
ca.com/ch/de