kaspersky BRING ON THE FUTURE

Kaspersky Embedded Systems Security

Zuverlässige Sicherheit für Embedded Systems

Der Markt rund um Embedded Systems wächst stetig und auch Cyberkriminelle lernen immer weiter dazu. So gab es 2019 28 Prozent mehr Infektionsversuche auf Geldautomaten und PoS-Systeme als noch 2018.

Embedded Systems werden in verschiedensten Bereichen unseres alltäglichen Lebens eingesetzt. Wir nutzen sie für alles von PoS-Systemen und Geldautomaten bis hin zu medizinischen Geräten und Telekommunikation. Das führt zu mehr Angriffsvektoren als je zuvor.

Nach dem jüngsten Supportende von Windows 7 dürfen Unternehmen die Aktualisierung der Betriebssysteme ihrer Embedded Systems nicht länger hinauszögern, sondern müssen alle nötigen Maßnahmen treffen, um den Schutz zu steigern. Hierbei ist erwähnenswert, dass Windows XP – obwohl es schon seit vielen Jahren nicht mehr unterstützt wird – noch immer das am häufigsten verwendete Betriebssystem in Embedded Systems ist. Diese Tatsache ist eine offene Einladung für Hacker.

Cyberkriminelle richten ihre Aufmerksamkeit und Angriffe zunehmend auf diese Embedded Devices – mit potentiell verheerenden finanziellen Folgen. Deshalb müssen Unternehmen beim Schutz ihrer Systeme und Daten intelligenter vorgehen als je zuvor. Mit leistungsstarker Threat Intelligence, Malware-Erkennung in Echtzeit, umfassender Anwendungs- und Gerätesteuerung und flexibler Verwaltung bietet Kaspersky Embedded Systems Security einen umfassenden Schutz speziell für Embedded Systems.

Wichtigste Vorteile

Effizientes Design selbst für Low-End-Hardware

Kaspersky Embedded Systems Security wurde speziell für den effektiven Betrieb auch auf Low-End-Hardware (ab 256 MB RAM und Pentium III-CPU) und alter Software (ab Windows XP) entwickelt, ohne dass die Gefahr einer Systemüberlastung besteht. Auch Verbindungen (ab nur 56 kbit/s) sind kein Problem, selbst wenn ein Mobilfunkmodem die einzige Verbindungsoption ist und aufgrund eines schlechten Signals nur mit 2G funktioniert.

Leistungsstarker Speicherschutz

Die leistungsstarke Exploit Prevention-Technologie überwacht geschützte Prozesse, um zu verhindern, dass Exploits ungepatchte oder sogar Zero-Day-Schwachstellen in Programmen und Systemkomponenten angreifen. Dies ist besonders wichtig für den Schutz vor weit verbreiteten Ransomware-Angriffen wie z. B. WannaCry und ExPetr.

Für Windows XP optimiert

Die meisten Embedded Systems laufen immer noch unter dem nicht mehr unterstützten Betriebssystem Windows® XP. Kaspersky Embedded Systems Security wurde für den Betrieb mit voller Funktionalität unter Windows XP sowie unter Windows 7, Windows 8 und Windows 10 optimiert.

Kaspersky Embedded Systems Security bietet in absehbarer Zukunft 100-prozentige Unterstützung für Windows XP – so haben Unternehmen Zeit, nötige Upgrades schrittweise vorzunehmen.

Compliance

Die umfassenden Schutzkomponenten in Kaspersky Embedded Systems Security – Malware-Schutz, Programm- und Gerätekontrolle, Firewall Management, File Integrity Monitoring und Protokollüberprüfung – identifizieren und blockieren schädliche Aktivitäten in Ihrem System und erkennen verschiedene Indikatoren einer Sicherheitsverletzung. So können Kunden die Compliance-Anforderungen in Vorschriften wie z. B. PCI DSS und SWIFT einhalten.

Geldautomaten

PoS-Systeme

Ticketautomaten

Kassen

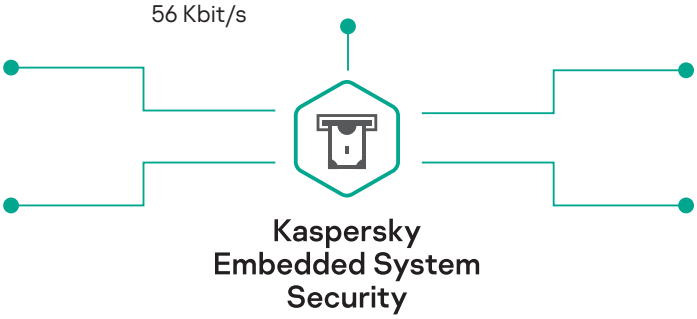
Alte PCs

Medizinische Geräte

Optimierte Systemanforderungen
- RAM: mindestens 256 MB
- BS: Windows XP oder höher
- Netzwerkbandbreite: mindestens 56 Kbit/s

Malware-Schutz
- Optional
- Echtzeit/On Demand
- Exploit Prevention gegen Ransomware und andere Bedrohungen

Netzwerkschutz
- Firewall-Management
- Network Threat Protection



System Integrity Monitoring
- File Integrity Monitoring
- Protokollüberprüfung

Systemhärtung
- Programmstart-Kontrolle
- Kontrolle der Softwareverteilung
- Gerätekontrolle

Funktionen

Leistungsstarker Malware-Schutz

Die vorausschauende Cloud-basierte Erkennung und Analyse von Bedrohungen bietet in Kombination mit bewährten Technologien Schutz vor bekannten und unbekannten hochentwickelten Bedrohungen. Die optionale (aber dringend empfohlene) Anti-Malware-Komponente kann in Szenarien mit Low-End-Hardware oder langsamen Kommunikationskanälen deaktiviert werden.

Malware-Erkennung in Echtzeit durch das Kaspersky Security Network

Das Kaspersky Security Network (KSN) ist ein globales, Cloud-basiertes Threat Intelligence-Netzwerk von Kaspersky. Millionen von weltweit verbreiteten Nodes speisen unentwegt Threat Intelligence in unsere Systeme, wodurch eine rasche Reaktion auf selbst die neuesten und hochentwickelten Bedrohungen – einschließlich Massenangriffen – sichergestellt wird.

Dieser konstante Datenstrom über versuchte Malware-Angriffe und verdächtiges Verhalten ermöglicht sofortige Dateieinschätzungen und bietet so Echtzeitschutz vor modernsten Malware-Bedrohungen.

Programmkontrolle

Durch Annahme eines Default-Deny-Szenarios mittels Programmstart-Kontrolle wird die Stabilität Ihres Systems gegenüber Datenschutzverletzungen optimiert. Durch das Unterbinden der Ausführung jeglicher Programme, Services und vertrauenswürdiger Systemkomponenten, die nicht explizit von Ihnen zugelassen wurden, können Sie die meisten Formen von Malware automatisch vollständig blockieren. Die Softwareverteilungssteuerung verwendet einen „Trusted Installer"-Ansatz, wodurch zeitraubendes manuelles Whitelisting von Dateien entfällt, die während Software-Updates oder -Installationen erstellt oder geändert werden. Geben Sie das Installationsprogramm einfach als vertrauenswürdig an und führen Sie das Update wie gewohnt durch.

Geräteüberwachung und -kontrolle

Mit der Gerätekontrolle von Kaspersky können Sie USB-Speichergeräte überwachen, die physisch an Systemhardware angeschlossen werden. Indem Sie den Zugriff auf unautorisierte Geräte verhindern, blockieren Sie einen Angriffsvektor, der von Cyberkriminellen häufig als einer der ersten Schritte bei Malware-Attacken genutzt wird.

Alle USB-Geräteverbindungen werden überwacht und protokolliert, damit die unzulässige USB-Nutzung bei der Vorfallsuntersuchung und -reaktion als mögliche Angriffsquelle identifiziert werden kann.

Verwaltung der Windows-Firewall

Die Windows-Firewall kann direkt über das Kaspersky Security Center konfiguriert werden, sodass die Verwaltung lokaler Firewalls bequem über eine einzige, einheitliche Konsole erfolgen kann. Dies ist besonders wichtig, wenn Embedded Systems nicht zu einer Domäne gehören und die Einstellungen der Windows-Firewall nicht zentral konfiguriert werden können.

Network Threat Protection

Diese Komponente verhindert Netzwerkbedrohungen, einschließlich Portüberwachung, Denial-of-Service-Angriffen und Pufferüberläufen. Die Komponente überwacht durchgehend die Netzwerkaktivitäten und führt bei verdächtigem Verhalten vordefinierte Reaktionen aus.

File Integrity Monitoring*

File Integrity Monitoring verfolgt Aktionen festgelegter Dateien und Ordner. Sie können auch konfigurieren, dass Änderungen nachverfolgt werden, während die Überwachung unterbrochen ist.

Protokollüberprüfung*

Kaspersky Embedded Systems Security überwacht mögliche Sicherheitsverletzungen durch die Überprüfung von Windows-Ereignisprotokollen. Wenn ein anormales Verhalten festgestellt wird, das auf den Versuch eines Cyberangriffs hindeutet, benachrichtigt das Programm den Administrator.

SIEM-Integration

Kaspersky Embedded Systems Security kann Ereignisse in Anwendungsprotokollen in vom Syslog-Server unterstützte Formate konvertieren, sodass diese an alle SIEM-Systeme übertragen und von diesen erfolgreich erkannt werden können. Ereignisse können direkt von Kaspersky Embedded Systems Security an ein SIEM-System exportiert werden – oder zentral über das Kaspersky Security Center.

Flexible Verwaltung

Sicherheitsrichtlinien, Signatur-Updates, Malware-Schutzscans und die Erfassung von Ergebnissen werden über eine einzige zentralisierte Verwaltungskonsole problemlos verwaltet: das Kaspersky Security Center. Darüber hinaus können Clients im lokalen Netzwerk über eine lokale GUI-Konsole oder Befehlszeile verwaltet werden. Das ist insbesondere in den isolierten und segmentierten Netzwerken von Embedded Systems hilfreich.

* Erfordert Kaspersky Embedded Systems Security Compliance Edition-Lizenz

Cyber Threats News: https://de.securelist.com
Neuigkeiten zur IT-Sicherheit: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency.

Getestet.
Transparent.
Unabhängig.