TRANSIÇÃO DE SISTEMAS OPERACIONAIS MÓVEIS

Insights e Considerações

Honeywell

ÍNDICE

INTRODUÇÃO

Nos últimos anos ocorreu uma mudança no cenário dos sistemas operacionais de dispositivos móveis. A transição do Windows® está bem encaminhada. Embora ainda existam várias opções, os tradeoffs e compromissos associados a cada uma delas tornaram-se mais claros. Este documento irá discorrer sobre esses pontos e fornecer ao leitor orientações sobre as soluções recomendadas.

SISTEMAS OPERACIONAIS ANTERIORES

2

Os clientes que atualmente executam aplicativos que exigem sistema operacional da Microsoft® (Windows CE 6 ou Windows Mobile/ Windows Embedded Handheld 6.5) em breve enfrentarão o fim do suporte à sua plataforma. O suporte principal, que inclui atualizações regulares, terminou para ambos os sistemas.

O suporte estendido da Microsoft (correções de segurança) terminou para o Windows CE 6 no início de 2018 e terminará para o Windows Embedded Handheld 6.5 no início de 2020. Após essas datas, os fornecedores não poderão fornecer patches caso seja encontrada uma vulnerabilidade ou erro no código da Microsoft. Por essa e outras razões, muitos consumidores começaram a planejar uma transição para novos aplicativos baseados em Android™

Como a aproximação das datas de fim de suporte dos sistemas operacionais, os consumidores precisam tomar decisões e planejar para seguir em frente, já que o desenvolvimento de aplicativos pode exigir tempo e esforço consideráveis.

A grande presença do Android no mercado dá suporte a uma ampla variedade de OEMs e hardware, tornando mais provável que um dispositivo esteja disponível para atender aos requisitos de custo e utilização do consumidor, incluindo dispositivos que oferecem teclados físicos integrados.

EVOLUÇÃO DO ANDROID ENTERPRISE

3

Antes do 4.0 "*Ice Cream Sandwich*", o Android oferecia pouco em termos de recursos corporativos. O sistema operacional focado no consumidor foi ampliado por extensões OEM e software de terceiros para permitir que ele fosse controlado e gerenciado no ambiente corporativo.

Os recursos corporativos começaram a aparecer gradualmente nas versões 4.2 *Jelly Bean* e 4.4 *KitKat*, culminando com a introdução do Android for Work no *Lollipop* 5.0. O Android for Work forneceu um conjunto estendido de APIs de gerenciamento e um sistema de container para separar e gerenciar de forma independente aplicativos, dados pessoais e de trabalho.

O Google® continuou a investir fortemente nas capacidades empresariais em cada uma das suas últimas versões, renomeando o Android for Work para Android Enterprise.

Os recursos adicionais incluem provisionamento em massa para acelerar a configuração do dispositivo, Modo Device Owner [Dono do Dispositivo] (Android Enterprise) para permitir dispositivos totalmente gerenciados em nível corporativo, VPN sempre ativa e criptografia habilitada para proteger dados pessoais e corporativos.

Sistemas operacionais móveis populares, como o Android, permitem que as empresas acessem um grande ecossistema de aplicativos, ferramentas de desenvolvimento e recursos, mas também envolvem riscos de segurança que devem ser abordados e mitigados. O Google tem desenvolvido progressivamente a sua abordagem em relação à segurança.

À medida que seu market share cresceu, o Android se tornou um alvo para explorações e ataques de malware. O Google respondeu aumentando as proteções para evitar a introdução de aplicativos potencialmente nocivos (PHAs, em inglês), bem como implementando defesas dentro do sistema operacional que limitam a capacidade do sistema de ser comprometido caso um PHA seja instalado. Algumas dessas proteções são discutidas abaixo.

Informações detalhadas estão disponíveis no relatório Android Security 2018 Year in Review do Google, localizado aqui:

https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf

COMO A HONEYWELL ATUA

4

A Honeywell está fortemente comprometida com a segurança cibernética. Os nossos negócios globais incluem soluções aeroespaciais e de processos que exigem um elevado grau de segurança em todos os aspectos das operações.

Uma força-tarefa de segurança cibernética corporativa define e mantém políticas e padrões de segurança, incluindo procedimentos de teste usados durante o desenvolvimento de produtos, que identificam especificamente problemas de software que podem tornar os sistemas mais vulneráveis a explorações. Essa abordagem elimina possíveis vulnerabilidades antes mesmo que os produtos sejam lançados.

A equipe de segurança cibernética monitora várias fontes de informação para aprender sobre possíveis problemas de segurança do sistema o mais cedo possível e implementou um protocolo de escalonamento que mobiliza recursos em toda a empresa para tratar prioritariamente desses problemas.

Assim que uma vulnerabilidade do Android é revelada e uma ação corretiva é publicada pelo Google, os especialistas em segurança da Honeywell para Android implementam a correção e a entregam aos clientes. A distribuição direta de patches e atualizações permite que a Honeywell reduza o tempo de resposta em comparação com os OEMs que precisam passar por canais secundários para entregar suas atualizações.

Manuais de Segurança são publicados para todos os produtos da Honeywell para orientar os clientes na implementação das melhores práticas para proteger seu ambiente e dispositivos. A orientação é fornecida na configuração das definições do dispositivo, das definições de rede e na manutenção de um ambiente de TI seguro

Essas medidas preventivas destinam-se a reduzir os caminhos pelos quais as ameaças podem entrar no ambiente do cliente.

Muitos clientes corporativos optarão por restringir ainda mais os usuários "travando" o dispositivo através do uso de um agente ou aplicativo de Enterprise Mobility Management (EMM), como o Enterprise Launcher da Honeywell. Essas ferramentas controlam o acesso aos recursos do sistema e podem restringir o sistema para executar apenas aplicativos específicos. A remoção da capacidade do usuário de instalar ou executar aplicativos não autorizados torna o sistema muito menos vulnerável a explorações de segurança causadas por ações do usuário.

A Honeywell oferece ferramentas que permitem aos clientes estabelecer listas brancas ou negras de aplicativos, controlar a disponibilidade de uma ampla gama de recursos de dispositivos e controlar quais endereços IP são acessíveis através do firewall. O Enterprise Launcher da Honeywell substitui a tela inicial padrão do Android por uma experiência em modo quiosque que permite que o usuário veja e execute apenas os aplicativos necessários para executar seu trabalho. A Honeywell também oferece um Enterprise Browser que permite a renderização de páginas da web usando controles padrão do Android, mas controla os sites que os usuários têm permissão para acessar. Ao limitar o que o usuário pode fazer com o dispositivo, o suporte de TI se torna mais fácil e as oportunidades para a introdução de malware no sistema são substancialmente reduzidas.

Outro aspecto importante da segurança é manter o sistema atualizado. Os pesquisadores estão constantemente descobrindo e relatando de forma responsável vulnerabilidades na base de código do Android que podem estar potencialmente sujeitas a explorações maliciosas. O Google oferece até mesmo um programa de recompensas para encorajar os pesquisadores a encontrar e relatar problemas potenciais.

O Google e os provedores de chipset, como a Qualcomm®, fornecem patches de segurança para OEMs regularmente para incorporação em suas compilações de software. A Honeywell atualiza suas imagens do sistema Android regularmente a cada 60 dias, com patches para explorações extremamente críticas disponíveis em apenas alguns dias (conforme necessário). Os patches são fornecidos como atualizações incrementais para imagens de linha de base, minimizando o tamanho do pacote de atualização para facilitar a implementação em toda a rede do cliente. Ao contrário dos OEMs, os pacotes da Honeywell podem ser baixados a partir de um site para permitir a realização de testes de aceitação por parte dos clientes antes da implementação em grande escala. Uma assinatura de notificação por e-mail está disponível para que os clientes sejam informados assim que novas atualizações forem publicadas.

GESTÃO DO CICLO DE VIDA DO ANDROID

5

Os clientes que implementam soluções de computação móvel robustas no ambiente empresarial esperam um ciclo de utilização mais longo. Como os smartphones geralmente expiram em 2-3 anos, as empresas esperam que seus sistemas durem 3-5 anos ou mais.

Historicamente, os sistemas operacionais usados em computadores móveis robustos tinham um ciclo de vida correspondente aos casos de uso corporativo. O Windows CE e Windows Embedded Handheld tiveram suporte da Microsoft durante 10 anos após a introdução inicial.

Embora o Android tenha sido expandido pelo Google com uma variedade de novos recursos empresariais, a cada grande lançamento, o suporte estendido não está entre eles. As versões principais do Android (ou "*dessert releases*") ocorrem aproximadamente a cada ano e são geralmente suportadas com patches de segurança do Google e dos fornecedores de chipsets por um período de 3 anos. Isto cria uma lacuna na cobertura do suporte em relação às expectativas da empresa. A seleção de chipsets OEM que são suportados para subsequentes "*dessert releases*" ajudará a estender a linha do tempo, mas, a política de suporte do Google fica aquém das expectativas dos clientes corporativos.

A Honeywell oferece o programa Sentinel™, para fornecer patches para vulnerabilidades de segurança graves aplicáveis ao sistema operacional suportado, periodicamente por mais de 2 anos após o término do suporte a patches de segurança do Google.

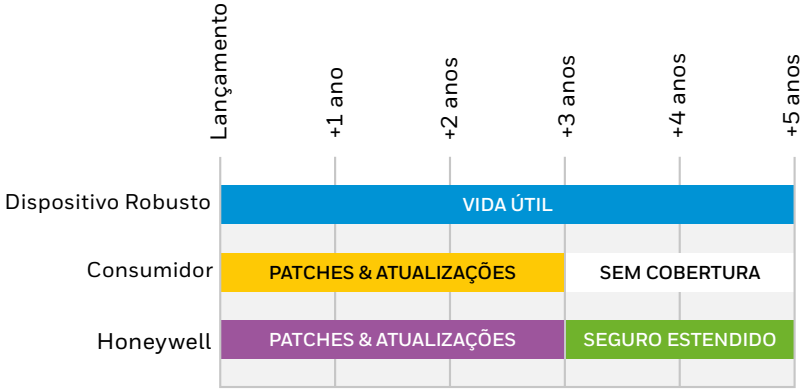
O PRAZO DE ENTREGA AOS CLIENTES SERÁ TRIMESTRAL, ou menor, se nenhuma correção severa aplicável à versão do sistema operacional suportado for relatada. Os patches aplicáveis serão geralmente entregues dentro de 90 dias após a divulgação pública, com exceções possíveis para ameaças iminentes.

ESPERA-SE QUE OS CLIENTES QUE UTILIZEM ESTE SERVIÇO instalem todos os patches lançados anteriormente, antes de instalar o patch mais recente. Em outras palavras, os patches são cumulativos. Patches específicos não podem ser aplicados individualmente.

PATCHES DE SEGURANÇA SERÃO TESTADOS SEGUINDO os procedimentos de teste padrão da Honeywell aplicáveis a todas as versões de software. Continua sendo responsabilidade do cliente testar todas as atualizações de software recebidas da Honeywell antes de realizar uma atualização.

OS CLIENTES PODEM RECEBER ESTES BENEFÍCIOS sob os termos de um contrato de prestação de serviços, seja autônomo ou incorporado a outro tipo de contrato de prestação de serviços. Os clientes sem um contrato não receberão patches de segurança após o término do suporte de patches de segurança do Google.

Este programa está disponível em dispositivos Honeywell com Android 6.0 *Marshmallow* e versões posteriores, após a expiração do suporte a patches de segurança do Google.



CONCLUSÃO E RECOMENDAÇÕES

O Android é um sistema operacional seguro, que utiliza o isolamento de aplicativos e técnicas de mitigação de exploração para fornecer um alto nível de segurança ao usuário. A implementação de técnicas de bloqueio via EMM ou do Enterprise Launcher da Honeywell pode reduzir ainda mais o risco de invasão de malware, limitando o que o usuário pode fazer e quais aplicativos podem ser executados.

Os produtos da Honeywell são concebidos para satisfazer as rigorosas normas de segurança da Honeywell. A segurança é avaliada durante todo o processo de desenvolvimento, identificando e mitigando vulnerabilidades mesmo antes dos produtos serem lançados.

A educação dos clientes e o monitoramento constante de vulnerabilidades e falhas de segurança, com processos definidos para lidar com os problemas descobertos, evitam ainda mais comprometimentos aos sistemas de nossos clientes. Um modelo de notificação baseado em assinatura permite que os clientes tomem medidas imediatas para mitigar os riscos enquanto o software está sendo corrigido e testado. Os clientes podem ter a certeza de que os seus sistemas são projetados e suportados de acordo com os mais elevados padrões e podem operar os seus negócios com confiança, sabendo que a Honeywell está empenhada em ajudá-los a manter a segurança desses sistemas.

Com seu grande market share e um amplo ecossistema de aplicativos, desenvolvedores e VARs, o Android se tornou a escolha mais óbvia para muitas empresas em uma variedade de indústrias. A transição para o Android envolve desenvolver novos aplicativos, adaptar fluxos de trabalho e mudar o uso de dispositivos móveis por parte dos usuários. Este pode ser um dispendioso e complicado esforço.

MOBILITY EDGE

Uma maneira das empresas simplificarem o processo de migração é selecionar dispositivos que são construídos em uma plataforma móvel unificada, como o Mobility Edge™ da Honeywell. Os dispositivos desenvolvidos nesta plataforma comum de hardware e software são mais fáceis e menos trabalhosos de implementar e gerenciar, e têm ciclos de vida mais longos do que os dispositivos concorrentes similares.

Os dispositivos Mobility Edge apresentam um hardware comum *System On Module*, ou SOM, que é um módulo único e certificado que inclui a CPU do dispositivo, memória, WWAN (em dispositivos selecionados), WLAN, Bluetooth®, comunicação por campo de proximidade (NFC) e Zigbee (em dispositivos selecionados). Eles também apresentam uma imagem comum de softwares de sistemas operacionais e um ecossistema de software comum, que inclui não apenas o software da Honeywell, mas também softwares de fornecedores independentes aprovados (ISVs) pela Honeywell.

Ter uma imagem de software do sistema operacional e um SOM comum proporciona flexibilidade e reduz os custos para as empresas implantarem dispositivos adicionais, porque não há custos adicionais de desenvolvimento ou certificação. As empresas podem validar todos os seus dispositivos móveis, utilizações e software uma vez e, em seguida, implementar em vários dispositivos, mais rapidamente e a um custo menor do que as implementações típicas.

As empresas que pretendem aumentar o ciclo de vida dos seus produtos e obter um melhor retorno do seu investimento em tecnologia serão asseguradas pelo fato de os dispositivos da plataforma Mobility Edge poderem ser atualizados aé o Android R. A Honeywell também fornece atualizações críticas de segurança por até dois anos após o último patch de segurança do Google através de seu serviço Sentinel, dando aos clientes um ciclo de vida do produto até pelo menos 2025.

HONEYWELL MARKETPLACE

Para empresas que precisam de ajuda com sua estratégia de transição para Android, o Honeywell Marketplace oferece um recurso útil. O Marketplace da Honeywell é uma loja de aplicativos empresariais que fornece às empresas acesso direto a softwares e soluções desenvolvidas pela Honeywell e seus fornecedores ISVs. As empresas podem procurar soluções por indústria, por tipo de solução (ferramentas de desenvolvimento, ERP, etc.), ou por tecnologia (computador móvel, veicular, etc.) e encontrar um conjunto diversificado de aplicações para ajudar a facilitar as suas transições.

Para mais informações
www.honeywellaidc.com/pt-BR
SPSMarketingBrasil@Honeywell.com

Honeywell Safety and Productivity Solutions
Av. Tamboré, 267 - 16º e 17º andares
Barueri, SP, 06460-000
(11) 3711-6770
www.honeywell.com

Mobile Operating System Transition White Paper | Rev B | 06/19

THE FUTURE IS WHAT WE MAKE IT

Honeywell