A TSC Company
BLUEBIRD

WHITE PAPER

DOCUMENTO TÉCNICO SOBRE SEGURANÇA DE COMPUTAÇÃO MÓVEL DA BLUEBIRD

Melhores práticas de segurança móvel com Bluebird

As iniciativas móveis estão na vanguarda das prioridades estratégicas da maioria das empresas atualmente. Essa maior mobilidade dentro das organizações se traduz em mais usuários acessando e utilizando dispositivos em diversos locais, incluindo ambientes remotos. Embora isso proporcione maior produtividade e eficiência para sua força de trabalho, as equipes de TI e segurança enfrentam o desafio crescente de proteger um número cada vez maior de terminais e garantir a segurança de dados críticos em uma infinidade de dispositivos.

As organizações que buscam proteger seus dispositivos móveis, como smartphones corporativos, tablets e computadores móveis especializados, podem alcançar isso implementando as robustas melhores práticas de segurança em computação móvel da Bluebird.

Para ressaltar a importância crítica da segurança em nível de dispositivo no universo móvel, vamos considerar estas estatísticas relevantes:

- Uma pesquisa da Gartner de 2024 indica que 63% das organizações globais adotaram total ou parcialmente uma estratégia zero trust[1], destacando uma mudança significativa no setor rumo à proteção abrangente de dispositivos, incluindo todos os ativos de computação móvel, dentro das redes corporativas.

- Um Relatório Global de Ameaças Móveis de 2025 revelou que mais de 50% dos dispositivos móveis rodam em sistemas operacionais desatualizados a qualquer momento, criando vulnerabilidades significativas.[2]

- Segundo a Forbes, as violações de segurança aumentaram 72% em 2023 em comparação com 2021, com a IBM reportando um ciclo de vida médio de 292 dias.[3]

Estatísticas de segurança para dispositivos móveis

Adotando o Zero Trust

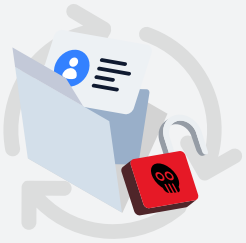
63 %

das organizações implementaram uma estratégia de zero trust

Sistemas operacionais móveis desatualizados

50 %▲

dos dispositivos móveis rodam em sistemas operacionais desatualizados.



Tempo de detecção de violação

292 dias

Ciclo médio de vida de uma violação

1. **Pesquisa da Gartner:** https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy
2. **Relatório Global de Ameaças Móveis 2025 (Zimperium):** https://lp.zimperium.com/hubfs/Reports/2025%20Global%20Mobile%20Threat%20Report.pdf
3. **Estatísticas Globais de Cibersegurança:** https://www.varonis.com/blog/cybersecurity-statistics

Esses números ilustram fortemente por que integrar todos os dispositivos móveis em uma estratégia de segurança holística é fundamental, não apenas para proteger dados valiosos, mas também para evitar que se tornem o elo mais fraco da cadeia de defesa da sua organização.

Bluebird: Uma postura proativa em segurança

Proteger dispositivos e dados sensíveis é fundamental para garantir fluxos de trabalho fluidos e promover um forte desempenho empresarial. A Bluebird mitiga ativamente riscos e vulnerabilidades de segurança ao integrar múltiplas camadas de proteção em nossos dispositivos e soluções. Cada componente da nossa oferta – do design de hardware aos softwares e serviços completes – é meticulosamente projetado para defender contra ameaças comuns de segurança como malware, phishing, falhas criptográficas e design inseguro, tudo isso sem comprometer a produtividade ou acessibilidade essenciais.

À medida que as empresas se tornam cada vez mais interconectadas, suas redes e dados valiosos ficam mais suscetíveis a acessos não autorizados e a diversas vulnerabilidades de segurança. A Bluebird aborda esses riscos ao seguir princípios fundamentais de cibersegurança e implementar uma abordagem de defesa aprofundada em toda a arquitetura e processos de design. Graças à nossa tecnologia inovadora e altamente configurável, a Bluebird capacita as organizações a alcançar um equilíbrio ideal entre objetivos operacionais críticos e posturas robustas de segurança.

Aprendendo com vulnerabilidades para construir soluções seguras

A Bluebird analisa continuamente e aprende com vulnerabilidades passadas de dispositivos móveis, desde métodos históricos de ataque até descobertas mais recentes. Essa visão contínua impulsiona nosso compromisso em desenvolver soluções de segurança mais inteligentes e resilientes, especificamente projetadas para enfrentar os desafios complexos atuais da computação móvel.

Sempre que uma nova vulnerabilidade é identificada, a equipe dedicada da Bluebird toma uma ação rápida para preparar e implantar um patch. Esse processo é baseado em um rigoroso sistema de classificação baseado na lista de Vulnerabilidades e Exposições Comuns (CVE), que é cuidadosamente gerenciado pelo National Vulnerability Database. Cada vulnerabilidade ou ameaça recebe um nível de severidade — que varia de 0,1 (baixo) a 10 (crítico) segundo o Sistema Comum de Pontuação de Vulnerabilidades (CVSS) — detalhando as ações essenciais que as empresas devem tomar para protegê-los.

A Bluebird também monitora de perto o Open Web Application Security Project (OWASP), que fornece informações e relatórios anuais sobre grandes vulnerabilidades móveis. Por exemplo, ao abordar vulnerabilidades chave como falhas no controle de

Lista CVE*

*CVE: Vulnerabilidades e exposições comuns

CVSS*

*CVSS: Sistema Comum de Pontuação de Vulnerabilidades

OWASP*

*OWASP: Projeto de Segurança de Aplicações Web Abertas

SDLC*

*SDLC: Ciclo de Vida do Desenvolvimento de Software

acesso e falhas de injeção, a Bluebird garante que todas as principais vulnerabilidades móveis sejam analisadas minuciosamente. Nosso ecossistema holístico, que abrange tanto o hardware quanto o software de nossos dispositivos, foi projetado para abordar de forma abrangente as vulnerabilidades móveis existentes. Nossos dispositivos passam por extensas fases de testes de segurança, incluindo rigorosas avaliações internas de segurança (análise estática e dinâmica de código), bem como testes de penetração independentes realizados por terceiros. Esses testes de terceiros garantem a robustez dos nossos controles de segurança, já que os testadores de penetração simulam tentativas reais de hackers de burlar as várias camadas de proteção.

Os dispositivos Bluebird são desenvolvidos estritamente seguindo um Ciclo de Vida de Desenvolvimento de Software (SDLC) exigido pela empresa. Isso garante que todo o software Bluebird seja projetado e testado seguindo rigorosas diretrizes de segurança incorporadas ao nosso SDLC. A implementação rigorosa do princípio do menor privilégio e controles robustos da Interface de Programação de Aplicações (API) impede que usuários não autorizados acessem dispositivos.

Além disso, testes extensos de aplicações de ponta a ponta melhoram consistentemente a segurança. A Bluebird está comprometida em expandir continuamente nosso portfólio de recursos de segurança à medida que novas ameaças surgem.

A Bluebird monitora diligentemente vulnerabilidades e ameaças do Android™ monitorando CVE e OWASP. Colaboramos com fornecedores e aproveitamos nossa expertise interna para fornecer os corretos certos, garantindo que todos os dispositivos móveis estejam protegidos contra ameaças de baixa e crítica por meio de nossos mecanismos abrangentes de atualização de segurança.

A Bluebird garante que cada vulnerabilidade móvel crítica seja analisada minuciosamente, e que todo o nosso ecossistema — que abrange tanto o hardware quanto o software dos nossos dispositivos — seja projetado para abordar proativamente as vulnerabilidades móveis existentes.

Simplifique a gestão do ciclo de vida do dispositivo com as soluções BOS ™ da Bluebird.

Baseando-se em décadas de pesquisa e desenvolvimento, bem como em insights de inúmeros casos de uso empresarial, a suíte Business Optimizing Solution (BOS) ™ da Bluebird oferece um conjunto abrangente de ferramentas empresariais projetadas para maximizar a produtividade do usuário móvel e minimizar as complexidades de TI ao longo do ciclo de vida do dispositivo. Essa suíte inclui inúmeras soluções projetadas para simplificar e otimizar o gerenciamento do ciclo de vida dos dispositivos móveis, desde integração até segurança robusta e muito mais. As soluções de BOS™ da Bluebird aprimoram a capacidade da sua equipe de TI de responder a ameaças de segurança novas e emergentes com recursos como:

• **Princípio do menor privilégio:**
Além de limitar o acesso aos dispositivos, o Bluebird aprimora ainda mais esse princípio ao detectar qualquer escalonamento de privilégios para chamadas de sistema, aplicação ou componente, garantindo controle granular.

• **Defesa em profundidade:**
A abordagem em camadas da Bluebird à segurança garante que os dados permaneçam completamente seguros, tanto em movimento quanto em repouso. Nossa arquitetura protege todas as camadas de um dispositivo móvel contra vulnerabilidades e as analisa para oferecer proteção abrangente e uma verdadeira abordagem de "defesa em profundidade". O Bluebird oferece proteção superior contra uma infinidade de ameaças à segurança, reduzindo os riscos e prolongando a vida útil dos dispositivos. Isso inclui proteção de hardware do armazenamento de firmware para garantir que o sistema operacional e o carregador de boot não sejam modificados, além de comunicações seguras de ponta a ponta.

• **Suporte de segurança expandido para o sistema operacional:**
A Bluebird oferece suporte de segurança estendido para o sistema operacional, garantindo que seus dispositivos recebam atualizações de segurança em tempo hábil por anos, maximizando sua vida útil.

• **Atualizações do BOS NEST™ para OTA (Over the Air):**
Nossa ferramenta de gerenciamento de mobilidade corporativa BOS, NEST,™ permite que você controle e agende atualizações de dispositivos remotamente, alinhando-se aos requisitos de segurança e à flexibilidade operacional do negócio.

• **Suporte à conformidade regulatória:**
Com o compromisso da Bluebird com atualizações de segurança e manutenção, as organizações ganham tranquilidade sabendo que seus dispositivos podem ajudá-las a cumprir regulamentos em constante evolução, como a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) ou a Certificação do Modelo de Maturidade em Cibersegurança (CMMC).

• **BOS™ Kiosk / Enterprise Launcher:**
Evite interrupções operacionais e proteja a produtividade da força de trabalho personalizando interfaces de usuário e acesso aos dispositivos: especifique quais aplicativos os usuários podem acessar, desative recursos indesejados nos dispositivos e inicie automaticamente os aplicativos necessários.

• **BOS™ Power Manager:**
Monitore centralmente a saúde da bateria e a saúde de toda a frota de dispositivos, possibilitando gerenciamento proativo e reduzindo indisponibilidades inesperadas..

• **BOS™ Device Finder:**
Localize rapidamente dispositivos perdidos ou perdidos usando sinais BLE, melhorando a recuperação de ativos e reduzindo os tempos de busca.

• **Mensagens Seguras:**
Facilitar canais de comunicação seguros entre o pessoal, garantindo a troca segura de informações sensíveis dentro do ambiente operacional.

Maior confiança na segurança dos dispositivos móveis

A Bluebird adere rigorosamente aos pilares fundamentais da cibersegurança, oferecendo confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das ações com nossos produtos. A Bluebird é confiável por indústrias críticas, incluindo segurança pública, socorristas e uma variedade de clientes governamentais e corporativos ao redor do mundo. A Bluebird mantém um forte compromisso com as melhores práticas de segurança e colabora com especialistas do setor para garantir que nossos dispositivos atendam a rigorosos padrões de segurança, que coletivamente promovem a confiança dos usuários na segurança dos dispositivos.

Confiança reforçada com um ambiente de execução confiável (TEE)

Um mecanismo chave que as organizações usam para proteger operações criptográficas e materiais sensíveis é o Ambiente de Execução Confiável (TEE). Esse ambiente opera isoladamente do Rich Execution Environment (REE) do dispositivo, onde residem o sistema operacional central e as aplicações. Dentro do TEE, o código roda com alto nível de confiança, pois seu ambiente é completamente isolado do restante do sistema. Qualquer ameaça detectada no REE não pode afetar o TEE. Mesmo que o REE seja comprometido, os dados dentro do TEE permanecem seguros.

O Bluebird oferece uma camada extra de segurança aos TEEs das organizações, integrando recursos como nosso quiosque BOS™ / Enterprise Launcher. Por exemplo, nosso Enterprise Launcher permite que administradores controlem quais usuários têm acesso a ambientes específicos, garantindo que dados sensíveis ou confidenciais permaneçam seguros. Ao seguir consistentemente as melhores práticas de TEE (que estão integradas em todos os dispositivos Bluebird recém-produzidos), os TEEs ficam fortemente protegidos contra novas e emergentes ameaças à segurança.

Coletores de dados Portáteis

Solução RFID

Tablets Empresariais*

Programa proativo de testes de segurança Bluebird

Bluebird adota uma postura proativa em relação à segurança. Em vez de simplesmente reagir a ameaças de segurança, realizamos regularmente testes internos de segurança, incluindo tentativas de identificar vulnerabilidades de código ou fraquezas do sistema em nossos próprios dispositivos. Uma vez identificada, a Bluebird resolve rapidamente o problema — corrigindo bugs ou criando uma atualização de segurança específica para eliminar a vulnerabilidade. Isso reduz significativamente a probabilidade de cibercriminosos identificarem e explorarem vulnerabilidades, que poderiam ter consequências potencialmente devastadoras para as empresas.

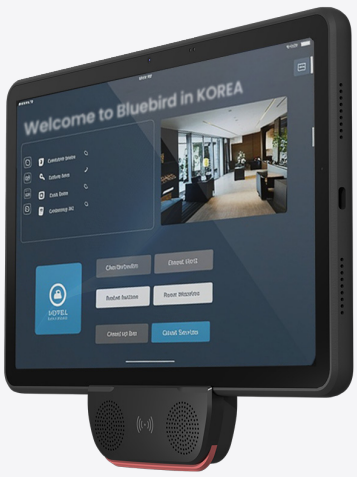
Fortaleça a segurança da computação móvel com a Bluebird

Por quase três décadas, a Bluebird tem sido líder em inovação em dispositivos móveis corporativos, e estamos comprometidos em fornecer às organizações soluções de segurança abrangentes, projetadas de acordo com as melhores práticas do setor. Todo o nosso portfólio de soluções de segurança é cuidadosamente projetado para garantir total segurança, sem comprometer acessibilidade ou escalabilidade. Quando se trata de segurança para dispositivos móveis, a Bluebird oferece proteção e controle incomparáveis.

Para saber mais sobre como a Bluebird protege seus dispositivos móveis com recursos de segurança de primeira linha, visite https://latam.tscprinters.com/en/mobile-computers

Terminais de Pagamento*

Quiosque Interativo*



Automotivo*

*Disponibilidade limitada nos EUA, Canadá e América Latina; entre em contato com seu representante de vendas local.

Bluebird Inc. (Sede Corporativa)

www.bluebirdcorp.com

Tel. +82-1577-0778 Fax. +82-2-6499-2242

06355, 3F, 115, Irwon ro, Gangnam gu, Seoul, Republic of Korea

Bluebird Alemanha GmbH

EUROPE@bluebirdcorp.com

Tel. +49-6196-7761262, 06196-7761263

FAX. +49-6196-7761264

Ober der Röth 4, 65824 Schwalbach am Taunus, Germany

Bluebird Europe S.L.

bluebird.spain@bluebirdcorp.com

C/ José Abascal, 53, 6ª Planta, 28003, Madrid, Spain

Bluebird USA Inc.

bluebird.usa@bluebirdcorp.com

3775 Venture DR, BLDG E, Duluth, GA, 30096, USA

Bluebird América Latina

latam@bluebirdcorp.com

AV. Paseo de la Reforma 265, Edificio Axtel Piso 2, Cuauhtemoc, C.P. 06500, CDMX, Mexico

Bluebird Índia - Centro de Pesquisa e Desenvolvimento

2nd Floor, RPR Complex, Site No. A 52, Kamadhenu Nagar, B.Narayanapura, Mahadevapura, Bangalore, Karnataka, India

Bluebird Coreia - Centro de Serviços

TEL. +82-1660-3202

21315, #B-710, Bupyeong-daero 283, Bupyeong-gu, Incheon, Republic of Korea

Centro de tecnologia de fabricação da Bluebird

TEL. +82-1588-1380 FAX. +82-31-731-4341

13216, B 6F~8F, 531, Dunchon-daero, Jungwon-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

SEDE CORPORATIVA
TSC Auto ID Technology Co., Ltd.
Tel: +886 2 2218 6789
E-mail: apac_sales@tscprinters.com

LI ZE PLANT
TSC Auto ID Technology Co., Ltd.
Tel: +886 3 990 6677
E-mail: apac_sales@tscprinters.com

CHINA
Tianjin TSC Auto ID Technology Co., Ltd.
Tel: +86 22 5981 6661
E-mail: apac_sales@tscprinters.com

ÁSIA-PACÍFICO
TSC Auto ID Technology Co., Ltd.
Tel: +886 2 2218 6789
E-mail: apac_sales@tscprinters.com

CORÉIA
Escritório de Representação da TSC Coréia
Tel: +82 2 852 3322
E-mail: apac_sales@tscprinters.com

ÍNDIA
Escritório de Representação da TSC Índia
Tel: +91 2249 679 315
E-mail: apac_sales@tscprinters.com

EMEA
TSC Auto ID Technology EMEA GmbH
Tel: +49 (0) 8106 37979 000
E-mail: emea_sales@tscprinters.com

RÚSSIA
TSC Auto ID Technology EMEA GmbH
Tel: +7 495 646 3538
E-mail: emea_sales@tscprinters.com

MÉDIO ORIENTE
TSC Auto ID Technology ME Ltd, FZE
Tel: +971 4 2533 069
E-mail: emea_sales@tscprinters.com

AMÉRICAS
TSC Auto ID Technology America Inc.
Tel: +1 657 258 0808
E-mail: americas_sales@tscprinters.com

MÉXICO
Escritório de Representação da TSC México
Tel: +1 52 (33) 3673 1406
E-mail: americas_sales@tscprinters.com

BRASIL
Escritório de Representação da TSC Brasil
Tel: +55 (11) 3554 7225
E-mail: americas_sales@tscprinters.com