

Ao

MINISTÉRIO PÚBLICO DO ESTADO DE GOIÁS

ATT: COMISSÃO DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO Nº 117/2025

DIL0019-26

A DATEN TECNOLOGIA LTDA., pessoa jurídica de direito privado, com sede à Rodovia Ilhéus – Uruçuca, Km 3,5, S/N, Galpão, Distrito Industrial de Ilhéus, Ilhéus/BA, inscrita no CNPJ sob o nº 04.602.789/0001-01, vem respeitosamente perante V.Sa., apresentar a resolução da diligência enviada nesta data, relativa ao PREGÃO ELETRÔNICO Nº 117/2025.

QUESTIONAMENTO 01: *1. Ausência de Identificação e Documentação Técnica do Equipamento. Em diligência realizada no site oficial do fabricante, não foram localizados o modelo do equipamento ofertado (MINI PC-DC8B-U) tampouco o part number indicado na proposta comercial. Adicionalmente, não foi encontrada a documentação técnica (datasheets, manuais ou especificações detalhadas) correspondente a este equipamento no portal do fabricante.*

RESPOSTA: O modelo MINI PC DC8B-U é um equipamento recém-lançado, e no momento da diligência, o site oficial está em processo de atualização, para a adição dos novos equipamentos. Para suprir essa solicitação de forma definitiva, encaminhamos os links no site oficial para consulta:

Link do manual: [Manual DC8B-U](#)

Link do equipamento: [DC8B-U](#)

Link do SSD: [DS4000](#)

Link da memória: [Memória RAM Daten DDR5](#)

Link do teclado: [CK510U](#)

Link do mouse: [CM627U](#)

Destacamos que o item 8.1 do edital admite como formas de comprovação, de maneira alternativa, catálogos, datasheets ou declaração oficial do fabricante. Os documentos apresentados se enquadram plenamente nessas modalidades, atendendo ao exigido.

Declaramos, ainda, que os modelos e componentes indicados na proposta correspondem ao modelo ofertado para o Pregão Eletrônico Nº 117/2025.

QUESTIONAMENTO 02: *2. Pendências no Item 5.1.8 - Segurança e Gerenciamento (Software CUCo). A proposta comercial apresenta o software CUCo para o atendimento deste requisito,*

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45.658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

contudo, identificamos as seguintes não conformidades: • Não consta na proposta comercial a comprovação técnica exigida para o "Software de SEGURANÇA E GERENCIAMENTO"

RESPOSTA: A CUCo, desenvolvedora do software persistente CUCo Security Suite, emitiu uma declaração, comprovando as funcionalidades do software e o atendimento aos pontos solicitados no item 5.1.8. do Termo de Referência.

Segue em anexo o arquivo "Declaração CUCo" e "CATÁLOGO – CUCo", comprovando o solicitado.

Diante dos pontos diligenciados e da documentação complementar anexada, resta claro que o equipamento ofertado para o Pregão Eletrônico nº 117/2025 atende plenamente às especificações técnicas exigidas no edital.

Ilhéus-Ba, 27 de maio de 2026.

Atenciosamente,

Documento assinado digitalmente
 **IGOR LEONARDO DE SANTANA CRUZ**
Data: 27/05/2026 12:21:49-0300
Verifique em <https://validar.it.gov.br>

Igor Leonardo de Santana Cruz
RG nº 100.176.46-17 - SSP-BA
CPF nº 039.693.675-06
Lider Pré-venda - Comercial Governo

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45.658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

DECLARAÇÃO

A CUCo Firmware Security, Lda. vem por este meio garantir o cumprimento, pelo CUCo Security Suite, dos seguintes requisitos, refutando as questões levantadas após a análise inicial, pela entidade reguladora do concurso público MP DE GOIÁS - (PID 1658-25).

5.1.8. SEGURANÇA e GERENCIAMENTO:

5.1.8.1. O equipamento deve acompanhar ferramenta de segurança já licenciada e com gerenciamento centralizado, acessada através de browser que contemple

5.1.8.1.1. Geolocalização: Rastreamento de ativos, utilizando tecnologia como Google Wifi ou GPS, mas não restrita a elas, e que inclua o local atual do ativo e seu histórico de localizações. Possibilidade de criar áreas geográficas demarcadas com base em políticas corporativas. Possibilidade de investigação de dispositivos extraviados, perdidos ou roubados ou dos que estão fora dos limites geográficos estabelecidos ou entrando em um local não autorizado;

5.1.8.1.2. A solução deve possuir recursos para que em caso de extravio, perda ou roubo do equipamento, após conectá-lo novamente à Internet, seja possível bloqueá-lo, excluir suas informações confidenciais remotamente e gerar relatórios para comprovar sua conformidade com regulamentos governamentais e corporativos;

5.1.8.1.3. Possuir grau de persistência integrado à BIOS/Firmware ativada de fábrica com recursos para se autorreparar caso o sistema operacional Windows ou a imagem de softwares utilizada pela CONTRATANTE, baseada em Windows, sejam reinstalados ou mesmo o disco rígido substituído;

5.1.8.1.4. Deverá apresentar comprovação que o equipamento fornecido é compatível com os requisitos solicitados, por meio de site oficial do fabricante/desenvolvedor, como por exemplo Absolute Software (<https://www.absolute.com/en-gb/partners/compatibility>) ou outro site público de outro fabricante que comprove as mesmas funcionalidade solicitadas;

5.1.8.1.5. Deverá funcionar por todo o tempo de garantia do equipamento

A CUCo Firmware Security garante que, os dispositivos DATEN, que incluam o sistema CUCo Security Suite, cumprem com os requisitos mencionados acima, no item **Solução de Bloqueio, Rastreo e Segurança**, definidos no concurso e que irão funcionar por todo o tempo de garantia do equipamento.

O CUCo Security Suite funciona com base em firmware, garantindo a sua persistência e dos módulos integrados no mesmo.

Esta informação poderá ser, inclusive, verificada na nossa página web: <https://cuco.net> ou, alternativamente, no nosso catálogo, incluídos em anexo.

Adicionalmente, no catálogo nas páginas 3 a 7, incluído em anexo, poderão verificar o cumprimento das funcionalidades mencionadas no item acima.

Aveiro, 26 de maio de 2026

CUCo Firmware Security, Lda.

A Gerência

Jorge S. Pinto – Managing Director

cucod Security
Suite



Firmware based secure endpoint

CUCo Security Suite

CUCo Security Suite integra agentes de hardware, firmware e software, combinando-os de forma transparente para oferecer uma solução robusta de segurança em múltiplas camadas ⁽¹⁾ para computadores, tablets e smartphones. Entre outras funcionalidades, CUCo Security Suite permite que os dispositivos realizem verificações de conformidade de forma autônoma, antes mesmo de o Sistema Operacional (SO) iniciar, além de bloqueios e desbloqueios remotos automáticos ou manuais.

CUCo Security Suite integra funcionalidades de Monitoramento e Gerenciamento Remoto (RMM), atualizações remotas em massa e serviços de geolocalização ⁽²⁾. Prometendo continuar se adaptando e evoluindo, CUCo Security Suite está expandindo sua gama de funcionalidades para atender aos seus novos desafios, permitindo que seja não apenas integrado em novos tipos de projetos, mas também melhorando sua utilidade nos projetos nos quais já está integrado.

CUCo Security Suite

é a solução completa para garantir a segurança dos seus dispositivos. Com sua tecnologia patenteada de firmware, CUCo Security Suite é um conjunto complexo em evolução permanente, atendendo às necessidades de segurança dos seus projetos.



⁽¹⁾ Concebida e patenteada como parte de um Consórcio Europeu de engenheiros especializados em pesquisa de segurança, essa tecnologia integra um sistema pioneiro de comunicação UEFI.

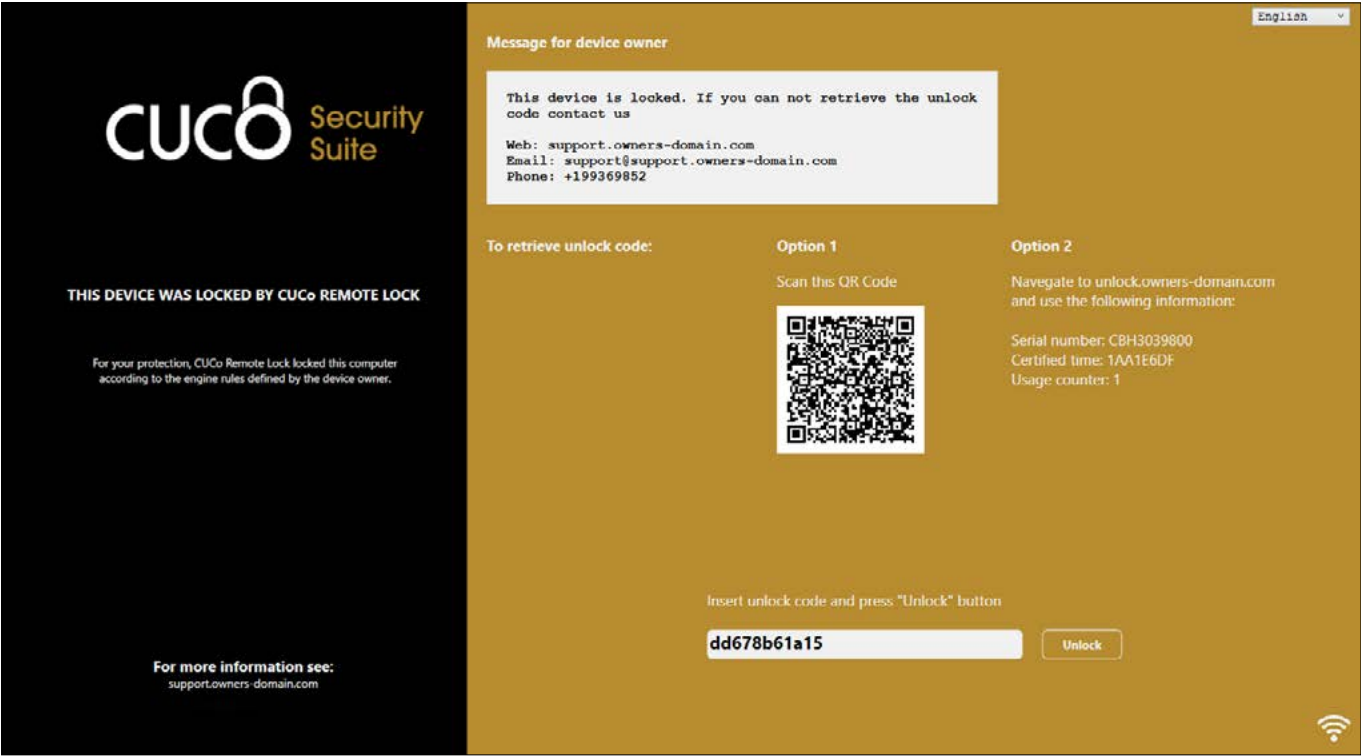
⁽²⁾ Disponibilidade sujeita a regulamentações locais.

CUCo Remote Lock

CUCo Remote Lock é um módulo de segurança robusto projetado para aprimorar a proteção dos dispositivos e prevenir o acesso não autorizado. Sendo o primeiro de seu tipo a operar no nível de firmware, ele permite que as organizações realizem verificações de conformidade nos dispositivos com base em parâmetros personalizáveis, como número de inicializações, número de dias sem uso, etc. Independente da conexão com a internet, CUCo Remote Lock aplica protocolos de segurança antes do carregamento do SO. Essa funcionalidade age como um dissuasor contra roubo,

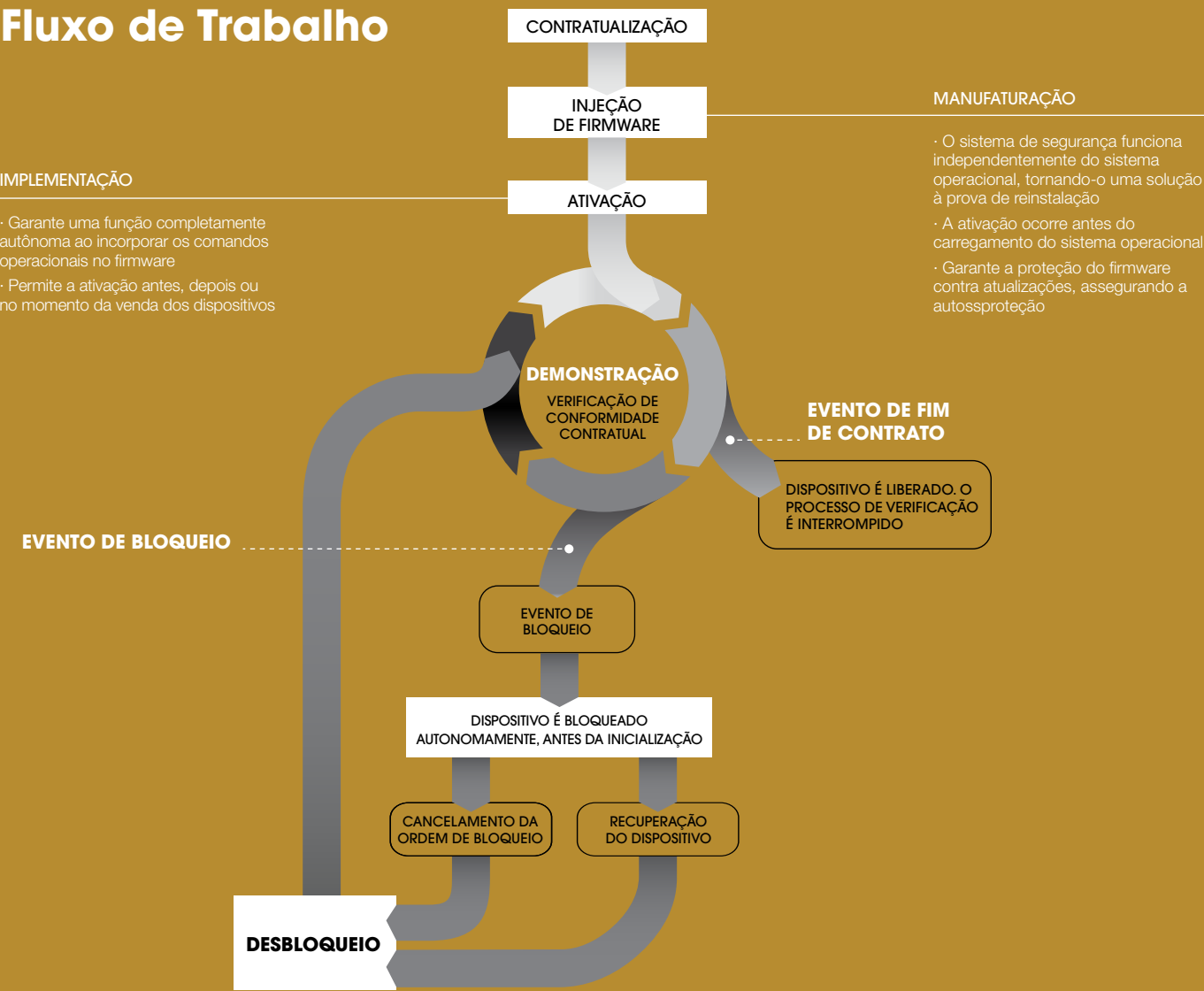
permitindo um bloqueio pré-inicialização não destrutivo, protegendo tanto o usuário quanto seus dados sensíveis.

Sempre que o dispositivo estiver bloqueado, qualquer usuário legítimo pode desbloqueá-lo de forma rápida e segura por meio de várias opções de recuperação, como QR-code, portal web ou entrando em contato com as respectivas plataformas de suporte. Esse processo garante a máxima proteção, enquanto assegura um tempo de inatividade mínimo e reduz os custos de administração.



Captura de tela de dispositivo bloqueado

Fluxo de Trabalho



Lista de funcionalidades

Construído sobre uma base segura UEFI, garante proteção robusta e confiabilidade

Todas as funcionalidades são garantidas pelo UEFI ⁽³⁾, eliminando a dependência de software externo

Compatível com múltiplos sistemas operacionais, incluindo Windows, Linux e Android

Realiza verificações automáticas de conformidade para manter a integridade da segurança

Bloqueio remoto baseado em regras, independente de conectividade, permitindo o bloqueio remoto de dispositivos mesmo sem conexão à internet

Bloqueio pré-inicialização não destrutivo, impedindo o acesso não autorizado sem causar perda de dados ou danos

Protegido contra tentativas de reflash do BIOS malicioso

Impede o carregamento do SO se o dispositivo estiver bloqueado

Suporta recuperação de desbloqueio usando um código de evento único, QR-code, portal web, smartphone ou conexão API remota ⁽⁴⁾

Detecta adulterações ou falhas e reinstala automaticamente o agente de software para restaurar a funcionalidade

Opcionalmente utiliza TPM para geração segura de chaves durante a comunicação com o servidor ⁽⁴⁾

Comunicação segura e assíncrona verificada com o servidor

Permite a desativação irrevogável do CUCo Security Suite e liberação remota do dispositivo

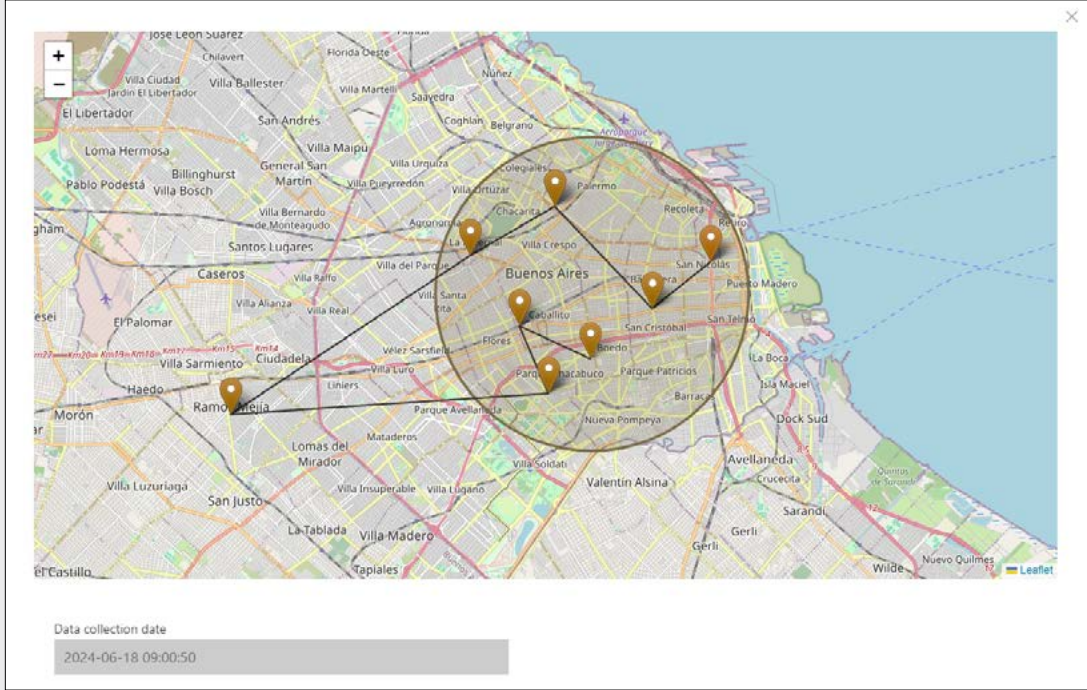
⁽³⁾ Para cenários específicos, oferecemos uma solução de bloqueio remoto exclusivamente de software, que, embora seja menos segura, garante a eficácia da conformidade contratual ao impor rapidamente as restrições do dispositivo conforme necessário.

⁽⁴⁾ Some restrictions may apply.

CUCo
Secure
Endpoint

CUCo Secure Endpoint permite que as organizações monitorem, gerenciem e protejam seus endpoints remotamente. Ele oferece funcionalidades de gerenciamento de software remoto, permitindo que os administradores implantem, atualizem ou removam software nos dispositivos da rede de forma contínua.

Este módulo inclui localização de endpoints, permitindo que os usuários gerenciem a localização física dos dispositivos, garantindo que permaneçam dentro de áreas autorizadas. Além disso, ele mede parâmetros de uso, oferecendo informações sobre como os dispositivos estão sendo utilizados, para garantir conformidade e eficiência.



Captura de tela de encontrar meu dispositivo

Lista de
funcionali-
dades

Ferramentas de gerenciamento remoto de software, permitindo monitoramento, remoção ou instalação de software em múltiplos dispositivos ao mesmo tempo

Impede a instalação de software não autorizado

Acesso ao inventário de software e hardware

Reimagem do SO remoto e exclusão de dados do usuário para dispositivos ⁽⁵⁾

Garante conformidade com acordos de licenciamento

Audita as tarefas de gerenciamento realizadas

Acesso ao histórico de localização do dispositivo

Ferramentas de geofencing que aplicam procedimentos pré-determinados

Rastreamento em tempo real da localização do dispositivo ⁽⁶⁾

Relatórios e alertas baseados em protocolos especificados

Identificação e registro de dispositivos reportados como perdidos

Alertas imediatos ao conectar um dispositivo perdido à internet

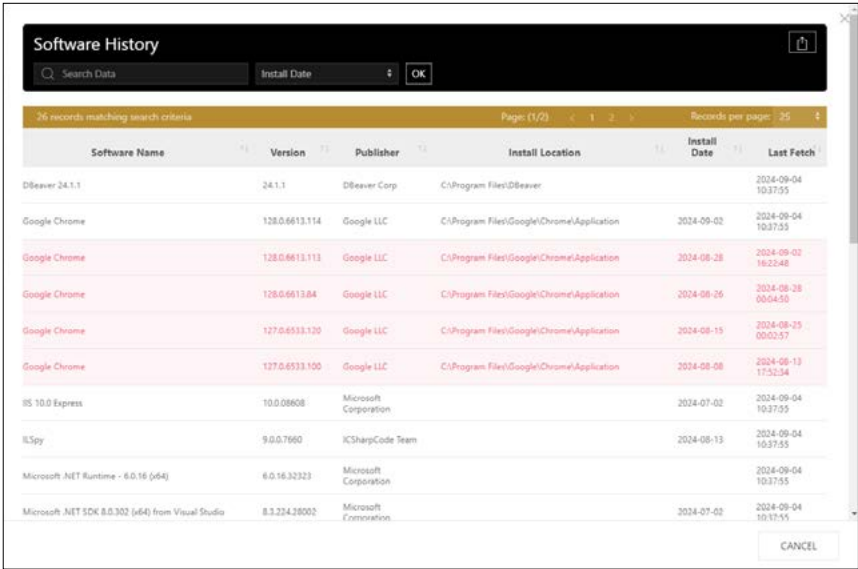
Rastreamento de eventos de login e desbloqueio

Monitoramento de desempenho de hardware, incluindo alertas quando o dispositivo excede o uso de RAM e CPU, juntamente com os limites de capacidade de armazenamento

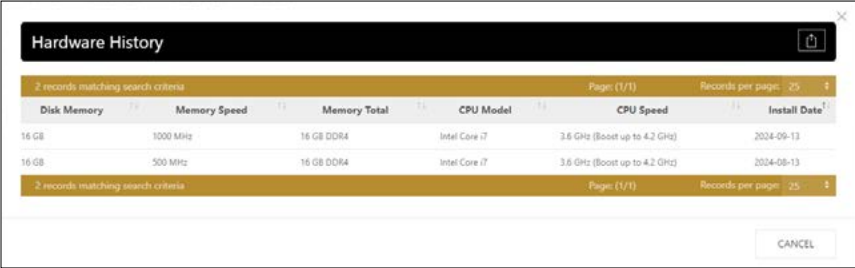
Programa de internet segura, incluindo filtros de conteúdo parental, DNS e filtros de gerenciamento de conteúdo e proteção contra malware

⁽⁵⁾ Dependente do BIOS do dispositivo.

⁽⁶⁾ Disponibilidade sujeita à regulamentação local.



Captura de tela do inventário de software

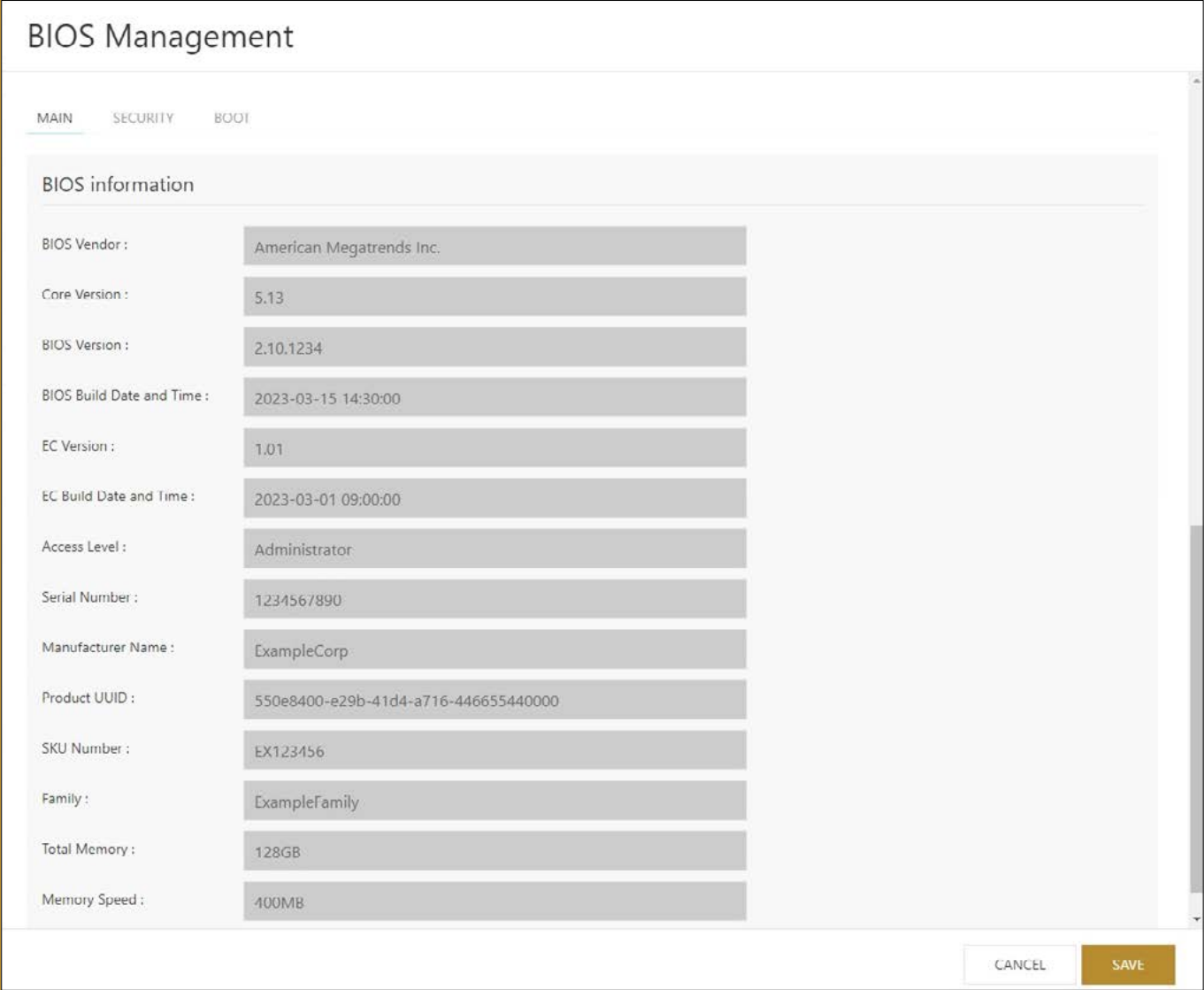


Captura de tela do inventário de hardware

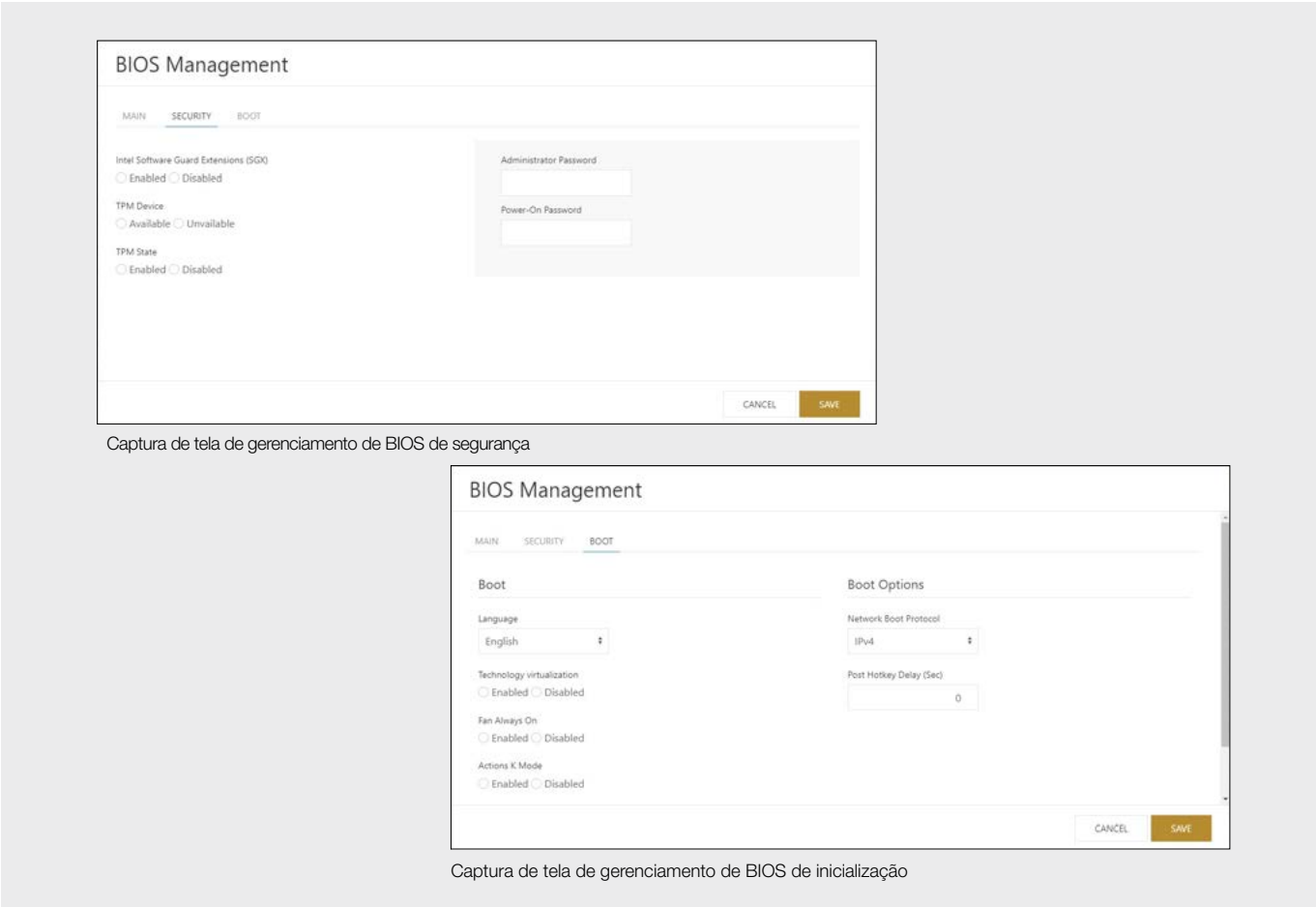
CUCo Remote BIOS Management

CUCo Remote BIOS Management permite que os administradores gerenciem e protejam remotamente as configurações de BIOS/UEFI em seus dispositivos, por meio de uma plataforma simplificada e fácil de usar. Este módulo inclui funcionalidades como gerenciamento de senha de BIOS, atualização remota de BIOS, alternância de chave de inicialização PXE, etc., apoiando as organizações na

implantação de atualizações em massa de firmware e concedendo aos administradores controle sobre as configurações de inicialização pela rede, aprimorando a segurança e reduzindo eficientemente a carga de trabalho. Finalmente, ele garante a integridade de segurança do BIOS, protegendo o firmware do dispositivo contra adulterações ou corrupções, mantendo assim a segurança geral do dispositivo.



Captura de tela principal de gerenciamento de BIOS



Captura de tela de gerenciamento de BIOS de segurança

Captura de tela de gerenciamento de BIOS de inicialização

Lista de Recursos

Aplicar atualizações remotamente ao BIOS/UEFI em vários dispositivos
Mantenha-os atualizados com os patches de segurança mais recentes, melhorias de estabilidade e aprimoramentos de compatibilidade de hardware, sem a necessidade de acesso físico

Ativar ou desativar remotamente a senha de acesso ao BIOS” Garanta a segurança das configurações do BIOS contra alterações não autorizadas, permitindo acesso controlado para fins de solução de problemas e manutenção

Ofereça a capacidade adicionar, modificar ou remover remotamente senhas de acesso de usuários do BIOS, permitindo alinhar com políticas organizacionais ou necessidades específicas de segurança

Habilitar ou desabilitar remotamente a opção de inicialização PXE, facilitando a inicialização baseada em rede para tarefas como implantação de sistema operacional, recuperação de sistema ou diagnósticos, melhorando a gerenciabilidade em ambientes grandes ou dispersos

Permitir o habilitamento ou desabilitamento remoto de opções específicas de inicialização no BIOS/UEFI, ajustando o controle sobre como os dispositivos inicializam, aprimorando a segurança ao evitar acessos não autorizados e garantindo conformidade com políticas de TI

Habilitar a recuperação remota da configuração atual da ordem de inicialização de um dispositivo, permitindo a verificação ou solução de problemas nas configurações de inicialização, garantindo que o dispositivo inicie a partir da fonte correta, conforme as políticas organizacionais

Restaurar remotamente as configurações do BIOS para os valores padrão, Útil para resolver problemas de configuração, preparar dispositivos para redistribuição ou redefinir configurações de segurança para um estado conhecido e estável

CUCo no setor de Educação

Em ambientes educacionais, a segurança dos dispositivos eletrônicos é fundamental para apoiar o ensino e a aprendizagem eficazes. CUCo Security Suite oferece uma variedade de funcionalidades exclusivas, adaptadas para atender às necessidades específicas de projetos educacionais, garantindo a segurança e a integridade dos dispositivos e dados.

Segurança baseada em firmware

Uma característica de destaque do CUCo Security Suite é seu modelo de segurança baseado em firmware, proporcionando proteção robusta desde o nível de firmware. Essa abordagem garante uma segurança abrangente, além da simples prevenção de roubo, permitindo a implementação de políticas de segurança personalizadas, adaptadas às necessidades de escolas e estudantes.

Independência de Sistema Operacional

CUCo Security Suite é compatível com diversos sistemas operacionais comumente encontrados em

ambientes educacionais, como Windows, Linux e Android. Essa versatilidade permite uma integração contínua com os ambientes de dispositivos existentes, simplificando os processos de implantação e gerenciamento para as instituições educacionais.

Funcionalidades RMM e MDM

CUCo Security Suite se destaca nas capacidades de gerenciamento remoto de dispositivos, facilitando atualizações de firmware, diagnósticos remotos e funcionalidades de bloqueio de dispositivos. Isso permite que os educadores monitorem e mantenham os dispositivos de

maneira eficiente em salas de aula e campi, garantindo experiências de aprendizagem ininterruptas.

Segurança do Dispositivo

A integração do CUCo Security Suite com recursos avançados de segurança, incluindo proteção contra malware no firmware e detecção de ameaças em tempo real, reforça sua posição como uma solução de segurança completa para ambientes educacionais. Essas capacidades não apenas protegem os dispositivos contra ameaças de segurança, mas também salvaguardam a privacidade dos estudantes e a integridade dos dados.

Estudo de Caso

CUCo Security Suite na Educação Protegendo os Estudantes no projeto “Escola Digital”

Introdução

Em resposta à crescente digitalização da educação, em 2020, o Ministério da Educação de Portugal lançou o projeto “Escola Digital”, com o objetivo de fornecer a cada aluno em Portugal acesso a um laptop. Com mais de 1,2 milhões de alunos envolvidos, essa iniciativa representou um investimento substancial, superior a 300 milhões de euros, necessitando de medidas robustas de proteção. Além do valor financeiro, a segurança dos estudantes contra possíveis furtos e danos foi primordial, dado o valor atrativo dos dispositivos e sua vulnerabilidade à exploração.

Problema

O Ministério enfrentou o desafio de proteger tanto os dispositivos quanto os estudantes, garantindo que os laptops fossem devolvidos ao final de cada ano letivo para redistribuição. Casos de alunos retendo os laptops levantaram preocupações sobre responsabilidade e gestão de ativos, demandando uma solução segura e econômica. Ao mesmo tempo, surgiram preocupações de que o projeto enfrentaria os mesmos problemas da iniciativa “e-escolinhas” (2007), criticada pela falta de opções de segurança e controle parental, além de sobrecarregar os professores com tarefas administrativas.

Análise

É aqui que o CUCo Security Suite entra em cena, oferecendo uma solução ideal para enfrentar esses desafios complexos. O CUCo capacita os responsáveis pelo projeto, como escolas e o Ministério da Educação, a bloquear ou desbloquear remotamente os dispositivos em caso de perda ou furto. Operando no nível de firmware, o CUCo permanece imune a tentativas de reinstalar o SO ou substituir os discos rígidos, garantindo uma proteção robusta. O CUCo também é eficaz em prevenir o acesso não autorizado a endpoints furtados. Ao proteger os dispositivos no nível de firmware, o CUCo garante que, mesmo se um dispositivo for roubado, os dados sensíveis sobre os estudantes e a instituição permaneçam protegidos. Além disso, o CUCo oferece um back office intuitivo para gerenciamento simplificado dos dispositivos

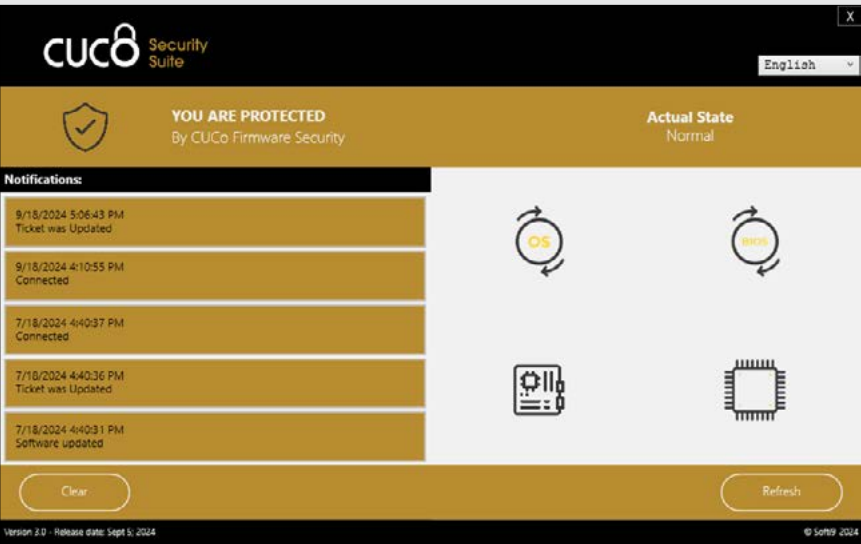
e integração perfeita com plataformas de gerenciamento existentes, por meio de APIs pré-desenvolvidas, aumentando a eficiência operacional. Como resultado da implementação bem-sucedida do CUCo Security Suite no projeto “Escola Digital”, uma nova fase foi alcançada, envolvendo a integração de funcionalidades adicionais de Mobile Device Management (MDM). Essas novas funcionalidades foram uma evolução natural do projeto e consideradas essenciais para seu sucesso contínuo, visando reduzir a carga de trabalho associada ao gerenciamento desses dispositivos.

Resultado

A adoção generalizada do CUCo Security Suite funcionou como um poderoso dissuasor contra furtos, desestimulando possíveis infratores e protegendo os alunos e os dispositivos. Além disso, casos de devoluções tardias foram rapidamente resolvidos por meio do bloqueio remoto dos dispositivos, garantindo conformidade e responsabilização. Ao implementar o CUCo Security Suite, o Ministério da Educação de Portugal gerenciou e protegeu com sucesso seu investimento, garantindo o uso correto dos dispositivos com o mínimo esforço de gestão e a um custo marginal para o projeto, ressaltando a eficácia e eficiência da solução.

Conclusão

De maneira geral, a integração do CUCo neste projeto levou ao desenvolvimento contínuo do CUCo Security Suite, desafiando-nos a introduzir uma nova gama de funcionalidades com o objetivo de lidar com novos problemas. Nossa solução agora inclui provisionamento automatizado de dispositivos, solução remota de problemas e ferramentas de gerenciamento de frota abrangentes, que capacitam administradores escolares e equipes de TI a gerenciar e manter os dispositivos de forma eficiente, garantindo que as atividades educacionais ocorram sem interrupções técnicas.



Captura de tela de Dispositivo protegido pelo CUCo

CUCo no setor Corporativo

No cenário corporativo atual, proteger dados sensíveis e informações confidenciais é de extrema importância. O CUCo Security Suite oferece uma camada adicional de proteção, blindando os dispositivos contra ameaças de firmware, como malware e manipulação não autorizada.

Facilitador de “Bring Your Own Device” (BYOD)

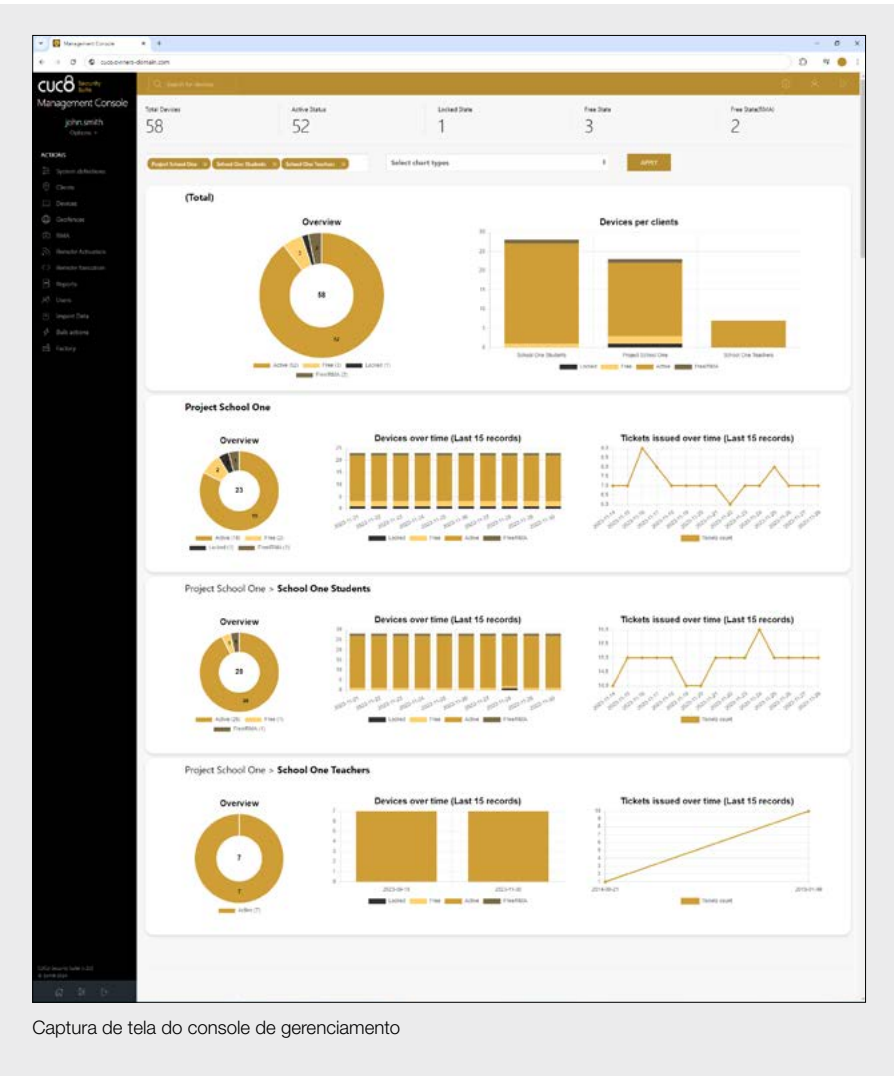
As funcionalidades de bloqueio de dispositivos, geofencing, firewall e filtragem de conteúdo do CUCo Security Suite permitem o método de trabalho “Bring Your Own Device” (BYOD), protegendo os dados e o próprio dispositivo em caso de roubo e garantindo que os dados da empresa estejam seguros contra malware.

Garantir Conformidade Regulamentar

As funcionalidades de monitoramento do CUCo Security Suite permitem que os administradores gerenciem quais softwares estão instalados nos dispositivos da empresa, modifiquem, instalem ou desinstalem remotamente e impeçam a instalação de software não autorizado.

Proporcionar Tranquilidade às Partes Interessadas

As diversas funcionalidades de segurança do CUCo Security Suite protegem o investimento, os ativos e os dados sensíveis da empresa.



Estudo de Caso

Projeto Piloto do CUCo Remote Lock Viabilizando Projetos DaaS

Introdução

Um projeto piloto liderado por um fabricante privado de computadores foi lançado em uma faculdade para testar a eficácia do CUCo Remote Lock como um sistema de execução de contratos e prevenção de furtos. Vários mil laptops, cada um no valor de €500, foram disponibilizados para estudantes de baixa renda por €149 cada, juntamente com um contrato de serviço de €14,90 por mês durante 2 anos. Não foi necessária verificação de crédito; os estudantes simplesmente precisavam assinar o contrato e pagar o valor inicial por meio de débito direto da conta bancária especificada no contrato.

Problema

Anteriormente, projetos Device as a Service (DaaS) enfrentaram muitos desafios relacionados à execução de contratos, gerenciamento de recursos e rastreamento de ativos. Portanto, negócios e projetos dessa natureza foram considerados inviáveis na maioria das vezes.

Análise

Neste contexto, o CUCo Remote Lock é um verdadeiro facilitador do modelo de negócios DaaS, proporcionando segurança robusta, garantindo a conformidade com os contratos de serviço e protegendo contra furtos e acessos não autorizados. Ao bloquear dispositivos não conformes e rastrear unidades perdidas ou roubadas, o CUCo minimiza perdas financeiras e aumenta a viabilidade de projetos de implantação em larga escala. Essa abordagem abrangente torna o CUCo um ativo inestimável para manter a integridade dos dispositivos e garantir o sucesso de iniciativas que dependem da distribuição generalizada de tecnologia.

Resultado

Após a execução do programa por mais de 2 anos, os dados estatísticos mostraram que 27,9% dos usuários pararam de pagar as parcelas mensais em algum

momento. O CUCo Remote Lock detectou a não conformidade e bloqueou automaticamente os dispositivos. Após a mensagem personalizada de “perdido-encontrado/bloqueado”, 98,6% dos usuários entraram em contato com o centro de atendimento, pagaram as parcelas em atraso e receberam um código único para desbloquear e reativar seus dispositivos. O CUCo Remote Lock reduziu significativamente o número de inadimplências ao bloquear unidades não conformes. Além disso, foi constatado que 3% das unidades estavam offline por mais de 2 meses. As regras internas do CUCo Remote Lock bloquearam esses dispositivos mesmo sem conectividade de rede. Durante esse período, 2% das unidades foram relatadas pelos usuários como roubadas ou perdidas. No entanto, devido à sua ‘pegada digital’ ao se conectar ao servidor do CUCo Remote Lock, a maioria dessas unidades foi recuperada e retornada ao usuário ou denunciada às autoridades. Ao final do período contratual, todas as unidades em conformidade foram liberadas do controle do CUCo Remote Lock. Sem o CUCo Remote Lock, a maioria das parcelas inadimplentes teria sido perdida, e o custo de recuperação por meio de agentes tradicionais ou do sistema jurídico teria sido muito alto. O CUCo Remote Lock economizou mais de 20% do preço de venda por unidade. Sem a solução CUCo Remote Lock, projetos de grande implantação baseados em fluxos financeiros futuros não seriam viáveis.

Conclusão

A implementação do CUCo Remote Lock neste projeto foi considerada bem-sucedida e confirmou ainda mais sua capacidade de melhorar e viabilizar projetos DaaS. Ao comparar dados de projetos DaaS passados com a iniciativa do CUCo Remote Lock, conseguimos verificar sua capacidade de executar contratos, prevenir furtos e proteger os investimentos feitos pelo fornecedor dos dispositivos.

Análise Comparativa do CUCo Remote Lock em relação aos 3 principais concorrentes	CUCo	C1	C2	C3
Plataforma aberta, baseada nos padrões UEFI, compatível com várias marcas de dispositivos finais	✓	✓	✓	✗
Bloqueio remoto de firmware de único propósito, controle automático de dispositivo, bloqueio pré-boot do OS	✓	✗	✓	✓
Nenhum acesso aos dados do usuário no dispositivo pelo gerente da plataforma (compliance com o GDPR)	✓	✗	✓	✗
Reativação remota do dispositivo após o evento de bloqueio (sem dependência de software)	✓	✗	✓	✓
Autoproteção contra tentativas de hackeamento para desativar a segurança no dispositivo	✓	✓	✗	✗
Baixa largura de banda e funcionamento sem conectividade por um período definido	✓	✗	✗	✗
Suporte a múltiplos sistemas operacionais, incluindo Windows, Linux, Android. Bloqueio via firmware	✓	✗	✓	✗
Foco em segurança “apenas de hardware”. Agnóstico a dados e conteúdo	✓	✗	✗	✗
Desativação remota irrevogável do mecanismo de segurança	✓	✓	✗	✓
Resiliência a alterações do sistema operacional	✓	✗	✗	✗

Análise Comparativa do CUCo Secure Endpoint em relação aos 3 principais concorrentes	CUCo	C1	C2	C3
Agente de software de endpoint resiliente	✓	✓	✗	✗
Ferramentas de gerenciamento de hardware	✓	✓	✓	✓
Ferramentas de geofencing	✓	✗	✗	✗
Execução de instruções críticas certificadas com base em blockchain	✓	✗	✗	✗
Acesso ao rastreamento em tempo real do dispositivo e histórico de localização	✓	✗	✗	✗
Rastreamento de eventos de login e desbloqueio	✓	✗	✓	✗
Programa Safer Internet, filtragem de DNS e filtros de conteúdo	✓	✗	✓	✓

Análise Comparativa do CUCo Remote BIOS Management em relação aos 2 principais concorrentes	CUCo	C1	C2
Atualização remota do BIOS em múltiplos dispositivos simultaneamente	✓	✗	✓
Ativação e desativação remota da senha do BIOS	✓	✗	✗
Habilitação/desabilitação remota da opção de inicialização PXE	✓	✓	✓
Recuperação remota das configurações atuais da ordem de inicialização	✓	✗	✗
Restauração remota das configurações padrão	✓	✗	✗

Tecnologia Blockchain

A integração da tecnologia Blockchain foi o próximo passo natural para a evolução contínua e desenvolvimento do CUCo Security Suite.

Blockchain é uma tecnologia que permite a criação de registros digitais imutáveis, possibilitando transações e registros seguros em uma rede ponto-a-ponto (P2P), descentralizando a informação e eliminando a necessidade de envolver terceiros no processo de verificação de dados. O Blockchain realiza isso codificando informações em “blocos”, de modo que cada novo “bloco” de informações adicionado é criptografado com um código baseado no bloco anterior. Esse processo mantém todos os dados ordenados cronologicamente e vinculados através de seus próprios códigos, criando a “cadeia” de informações.

A manipulação das informações nesta tecnologia é inviável, pois tentativas de fazê-lo resultariam em blocos totalmente novos de informações, tornando fácil para outros pares detectarem rapidamente a anomalia e rejeitarem os dados não autorizados.

A tecnologia Blockchain como campo está crescendo exponencialmente, estando presente em diversos setores como cibersegurança, bancos, saúde, logística e contratos inteligentes.

Atualmente, o CUCo Security Suite implementa contratos inteligentes como uma forma de verificar o cumprimento das regras entre as diferentes partes de forma mais eficaz e segura. Os contratos inteligentes funcionam armazenando as informações do contrato em um blockchain, descentralizando-as e tornando-as prontamente disponíveis para consulta de todas as partes, sem o risco de adulteração. Os contratos inteligentes verificam simultaneamente se todas as partes estão em conformidade com as condições predeterminadas, garantindo a segurança dos negócios para todas as partes envolvidas.

Modelo de Negocio

Licenciamento e Parcerias
A maioria dos principais fabricantes de computadores já licenciou e certificou seus dispositivos como compatíveis com o CUCo Security Suite. Nosso novo programa de certificação de dispositivos permite que o CUCo Security Suite ofereça oportunidades de licenciamento para vários parceiros OEM, seja sob a marca CUCo ou por meio de acordos de marca branca.

Ativação e Implantação
O CUCo Security Suite pode ser ativado por meio de planos de assinatura fornecidos por provedores de serviços licenciados e parceiros confiáveis, exclusivamente em hardware aprovado e previamente provisionado. Cada dispositivo pronto para CUCo passa por rigorosos testes e validações pela nossa equipe de engenharia especializada antes de ser lançado no mercado.

Opções de Entrega Flexíveis
Os provedores de serviços têm a flexibilidade de entregar nossa solução de segurança de ponta, seja por meio de acesso seguro baseado em nuvem ou implantando servidores de autorização diretamente nas instalações do cliente. Isso garante conformidade com as preferências e requisitos legais do cliente, incluindo total aderência às regulamentações do RGPD.

Para mais informações sobre qualquer uma dessas opções ou para discutir como podemos trabalhar juntos, entre em contato conosco pelo e-mail partners@cuco-firmware.com. Estamos aqui para ajudá-lo a encontrar a melhor solução para as necessidades do seu negócio.

cucô Security Suite

cucô Security Suite
www.cuco-firmware.com
sales@cuco-firmware.com

Desenvolvido por



Cofinanciado por



201BR01D.001

cucod Security Suite



Firmware based secure endpoint

CUCo Security Suite

CUCo Security Suite integra agentes de hardware, firmware e software, combinando-os de forma transparente para oferecer uma solução robusta de segurança em múltiplas camadas ⁽¹⁾ para computadores, tablets e smartphones. Entre outras funcionalidades, CUCo Security Suite permite que os dispositivos realizem verificações de conformidade de forma autônoma, antes mesmo de o Sistema Operacional (SO) iniciar, além de bloqueios e desbloqueios remotos automáticos ou manuais.

CUCo Security Suite integra funcionalidades de Monitoramento e Gerenciamento Remoto (RMM), atualizações remotas em massa e serviços de geolocalização ⁽²⁾. Prometendo continuar se adaptando e evoluindo, CUCo Security Suite está expandindo sua gama de funcionalidades para atender aos seus novos desafios, permitindo que seja não apenas integrado em novos tipos de projetos, mas também melhorando sua utilidade nos projetos nos quais já está integrado.

CUCo Security Suite

é a solução completa para garantir a segurança dos seus dispositivos. Com sua tecnologia patenteada de firmware, CUCo Security Suite é um conjunto complexo em evolução permanente, atendendo às necessidades de segurança dos seus projetos.



⁽¹⁾ Concebida e patenteada como parte de um Consórcio Europeu de engenheiros especializados em pesquisa de segurança, essa tecnologia integra um sistema pioneiro de comunicação UEFI.

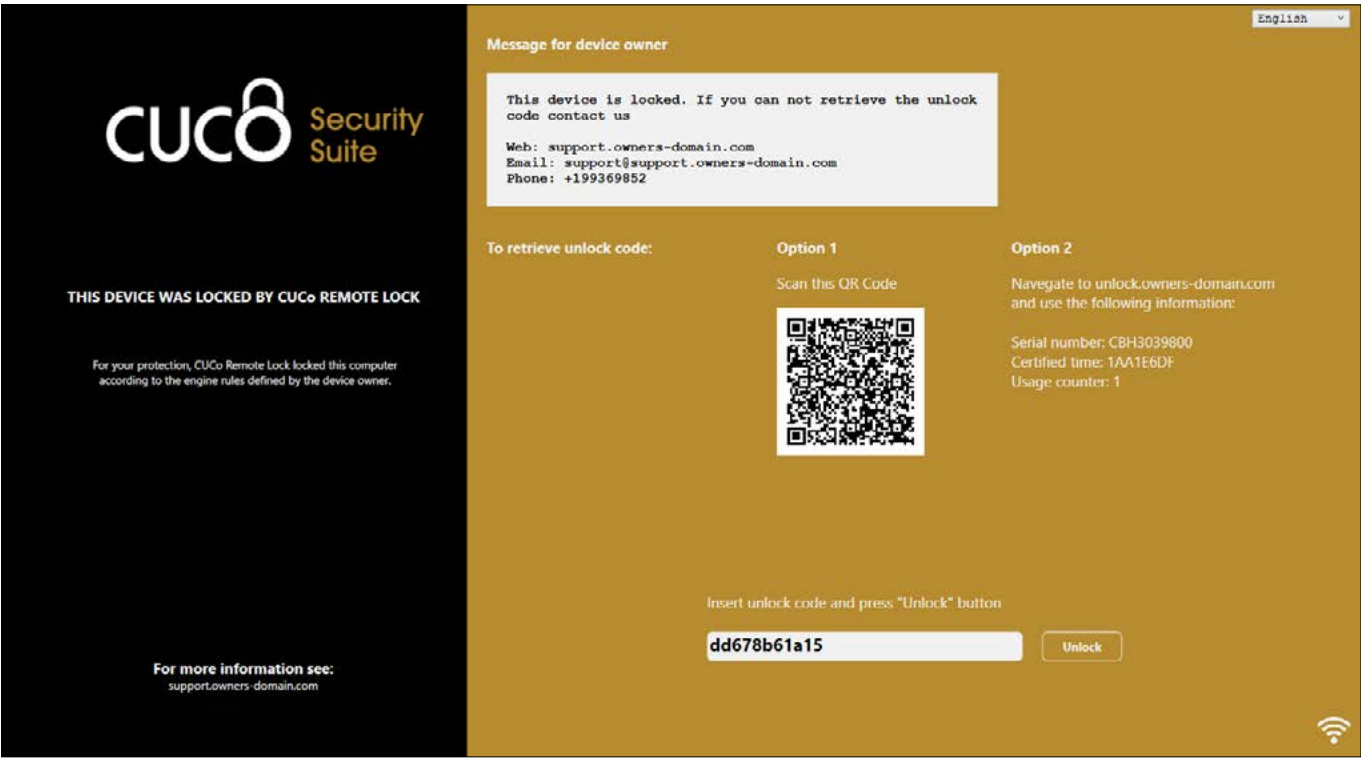
⁽²⁾ Disponibilidade sujeita a regulamentações locais.

CUCo Remote Lock

CUCo Remote Lock é um módulo de segurança robusto projetado para aprimorar a proteção dos dispositivos e prevenir o acesso não autorizado. Sendo o primeiro de seu tipo a operar no nível de firmware, ele permite que as organizações realizem verificações de conformidade nos dispositivos com base em parâmetros personalizáveis, como número de inicializações, número de dias sem uso, etc. Independente da conexão com a internet, CUCo Remote Lock aplica protocolos de segurança antes do carregamento do SO. Essa funcionalidade age como um dissuasor contra roubo,

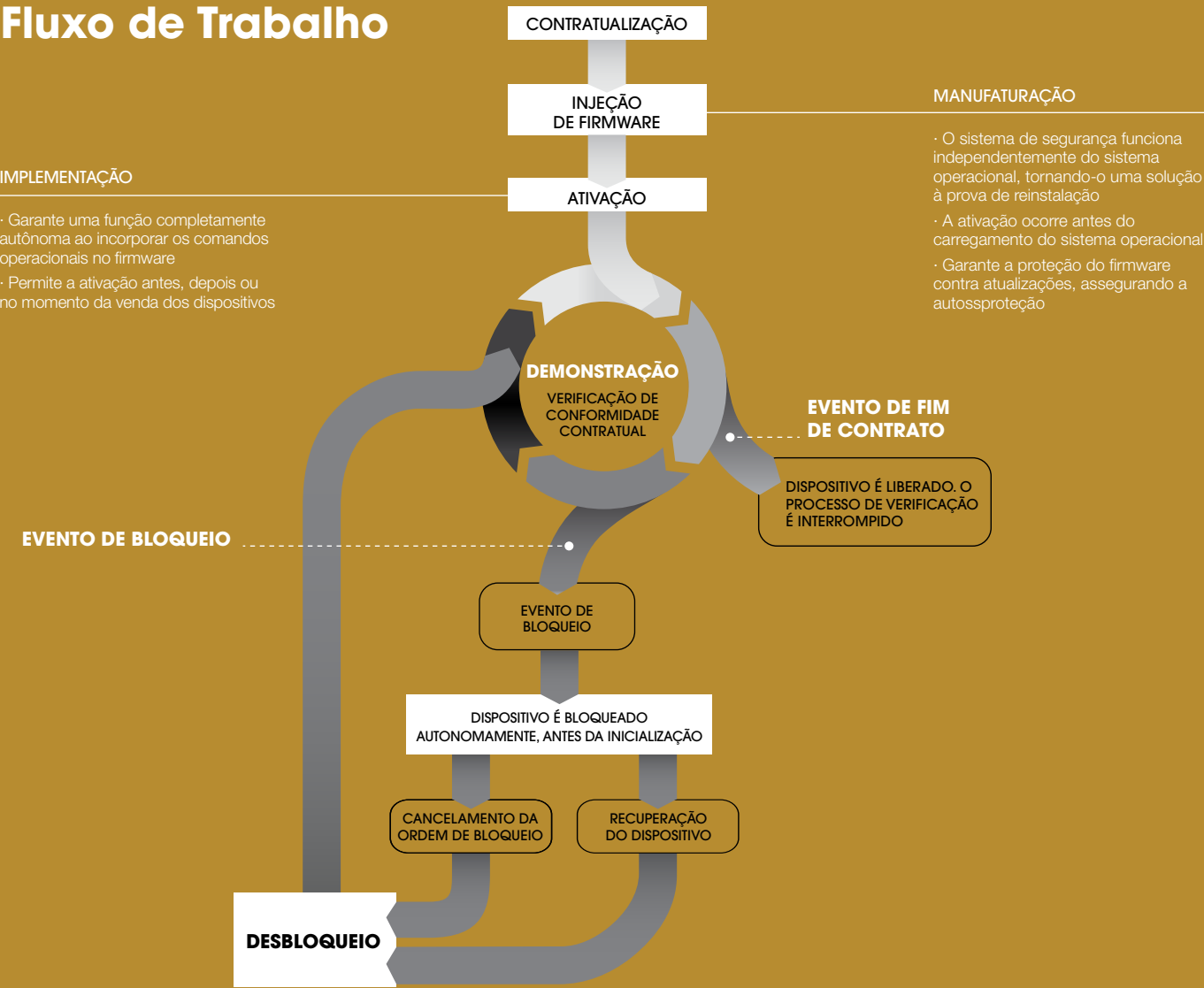
permitindo um bloqueio pré-inicialização não destrutivo, protegendo tanto o usuário quanto seus dados sensíveis.

Sempre que o dispositivo estiver bloqueado, qualquer usuário legítimo pode desbloqueá-lo de forma rápida e segura por meio de várias opções de recuperação, como QR-code, portal web ou entrando em contato com as respectivas plataformas de suporte. Esse processo garante a máxima proteção, enquanto assegura um tempo de inatividade mínimo e reduz os custos de administração.



Captura de tela de dispositivo bloqueado

Fluxo de Trabalho



Lista de funcionalidades

Construído sobre uma base segura UEFI, garante proteção robusta e confiabilidade

Todas as funcionalidades são garantidas pelo UEFI ⁽³⁾, eliminando a dependência de software externo

Compatível com múltiplos sistemas operacionais, incluindo Windows, Linux e Android

Realiza verificações automáticas de conformidade para manter a integridade da segurança

Bloqueio remoto baseado em regras, independente de conectividade, permitindo o bloqueio remoto de dispositivos mesmo sem conexão à internet

Bloqueio pré-inicialização não destrutivo, impedindo o acesso não autorizado sem causar perda de dados ou danos

Protegido contra tentativas de reflash do BIOS malicioso

Impede o carregamento do SO se o dispositivo estiver bloqueado

Suporta recuperação de desbloqueio usando um código de evento único, QR-code, portal web, smartphone ou conexão API remota ⁽⁴⁾

Detecta adulterações ou falhas e reinstala automaticamente o agente de software para restaurar a funcionalidade

Opcionalmente utiliza TPM para geração segura de chaves durante a comunicação com o servidor ⁽⁴⁾

Comunicação segura e assíncrona verificada com o servidor

Permite a desativação irrevogável do CUCo Security Suite e liberação remota do dispositivo

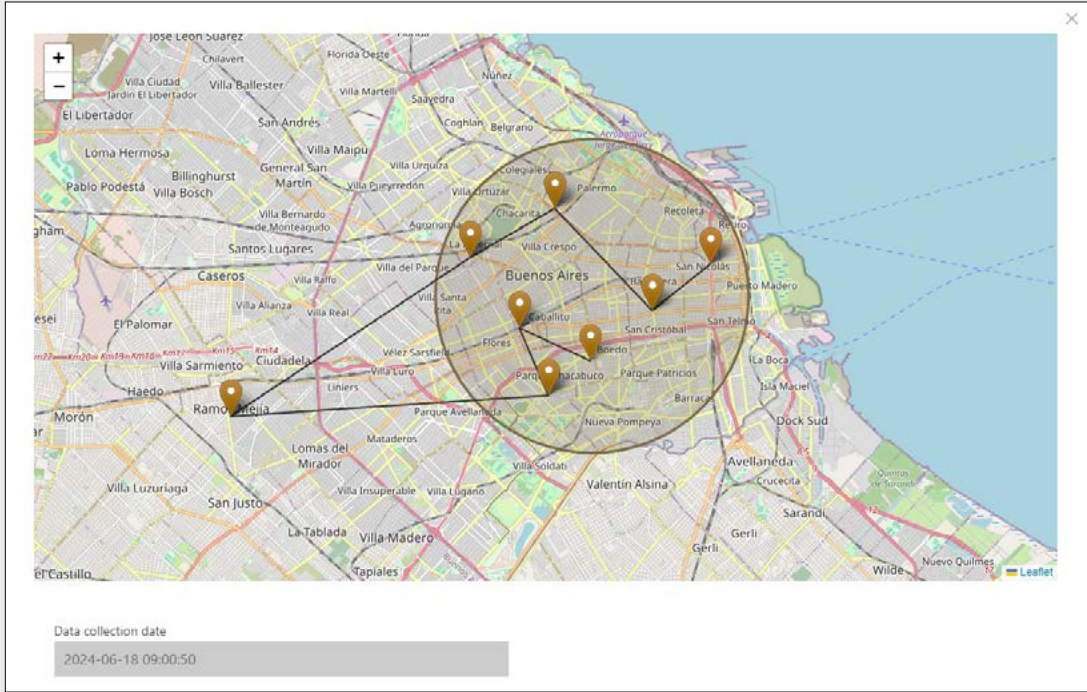
⁽³⁾ Para cenários específicos, oferecemos uma solução de bloqueio remoto exclusivamente de software, que, embora seja menos segura, garante a eficácia da conformidade contratual ao impor rapidamente as restrições do dispositivo conforme necessário.

⁽⁴⁾ Some restrictions may apply.

CUCo
Secure
Endpoint

CUCo Secure Endpoint permite que as organizações monitorem, gerenciem e protejam seus endpoints remotamente. Ele oferece funcionalidades de gerenciamento de software remoto, permitindo que os administradores implantem, atualizem ou removam software nos dispositivos da rede de forma contínua.

Este módulo inclui localização de endpoints, permitindo que os usuários gerenciem a localização física dos dispositivos, garantindo que permaneçam dentro de áreas autorizadas. Além disso, ele mede parâmetros de uso, oferecendo informações sobre como os dispositivos estão sendo utilizados, para garantir conformidade e eficiência.



Captura de tela de encontrar meu dispositivo

Lista de
funcionali-
dades

Ferramentas de gerenciamento remoto de software, permitindo monitoramento, remoção ou instalação de software em múltiplos dispositivos ao mesmo tempo

Impede a instalação de software não autorizado

Acesso ao inventário de software e hardware

Reimagem do SO remoto e exclusão de dados do usuário para dispositivos ⁽⁵⁾

Garante conformidade com acordos de licenciamento

Audita as tarefas de gerenciamento realizadas

Acesso ao histórico de localização do dispositivo

Ferramentas de geofencing que aplicam procedimentos pré-determinados

Rastreamento em tempo real da localização do dispositivo ⁽⁶⁾

Relatórios e alertas baseados em protocolos especificados

Identificação e registro de dispositivos reportados como perdidos

Alertas imediatos ao conectar um dispositivo perdido à internet

Rastreamento de eventos de login e desbloqueio

Monitoramento de desempenho de hardware, incluindo alertas quando o dispositivo excede o uso de RAM e CPU, juntamente com os limites de capacidade de armazenamento

Programa de internet segura, incluindo filtros de conteúdo parental, DNS e filtros de gerenciamento de conteúdo e proteção contra malware

⁽⁵⁾ Dependente do BIOS do dispositivo.

⁽⁶⁾ Disponibilidade sujeita à regulamentação local.

Software History						
Search Data Install Date OK						
26 records matching search criteria						
Page: 1/20						
Records per page: 25						
Software Name	Version	Publisher	Install Location	Install Date	Last Fetch	
DBeever 24.1.1	24.1.1	DBeever Corp	C:\Program Files\DBeever	2024-09-04 10:37:55		
Google Chrome	128.0.6613.114	Google LLC	C:\Program Files\Google\Chrome\Application	2024-09-02 10:37:55		
Google Chrome	128.0.6613.113	Google LLC	C:\Program Files\Google\Chrome\Application	2024-08-28 16:23:48		
Google Chrome	128.0.6613.84	Google LLC	C:\Program Files\Google\Chrome\Application	2024-08-26 06:04:50		
Google Chrome	127.0.6533.120	Google LLC	C:\Program Files\Google\Chrome\Application	2024-08-15 00:00:57		
Google Chrome	127.0.6533.100	Google LLC	C:\Program Files\Google\Chrome\Application	2024-08-08 17:52:34		
MS 10.0 Express	10.0.08608	Microsoft Corporation		2024-07-02 10:37:55		
ISpy	9.0.0.7960	ICSharpCode Team		2024-08-13 10:37:55		
Microsoft .NET Runtime - 6.0.16 (x64)	6.0.16.32323	Microsoft Corporation		2024-09-04 10:37:55		
Microsoft .NET SDK 8.0.302 (x64) from Visual Studio	8.0.302.18002	Microsoft Corporation		2024-07-02 10:37:55		

Captura de tela do inventário de software

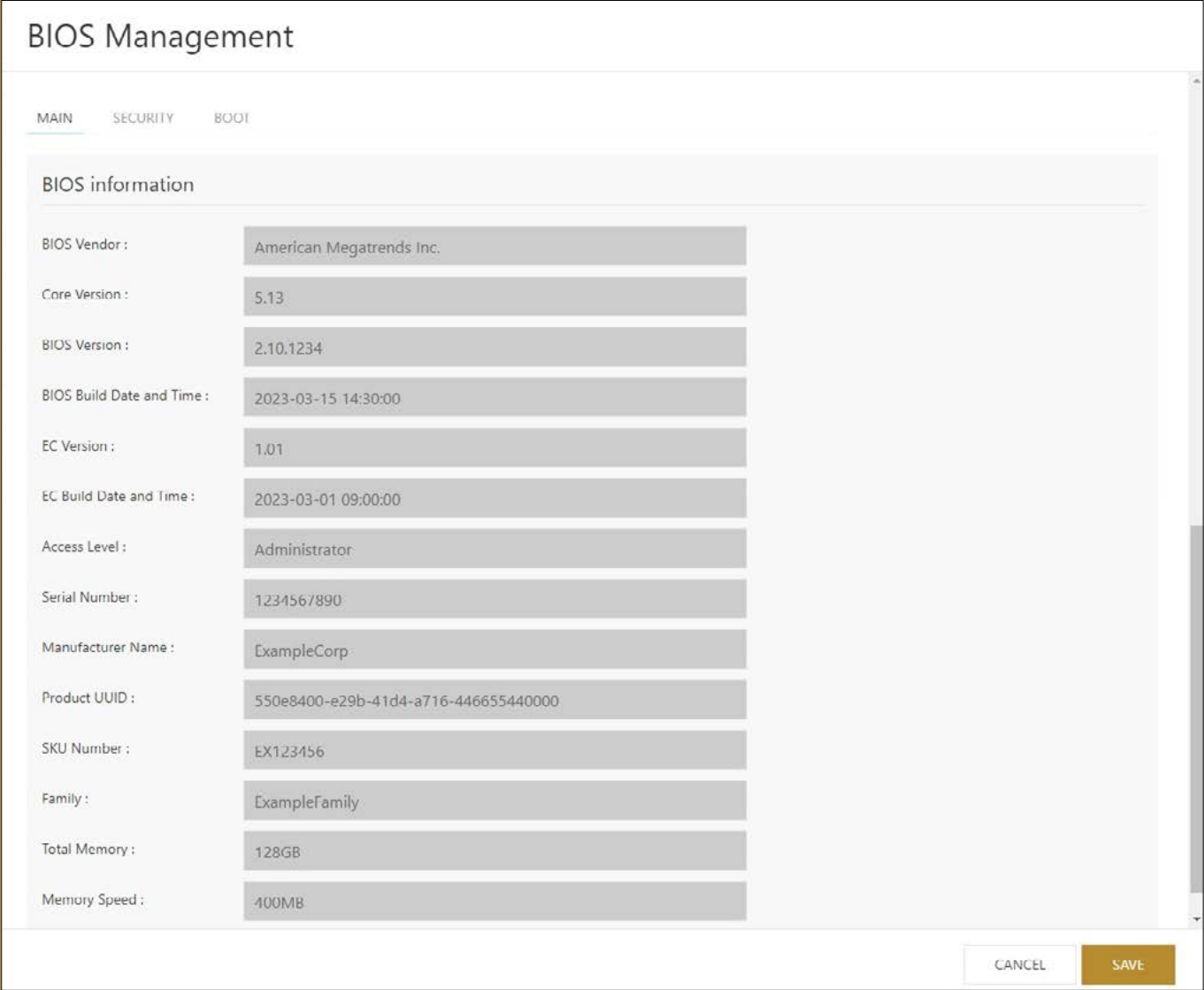
Hardware History					
2 records matching search criteria					
Page: 1/1					
Records per page: 25					
Disk Memory	Memory Speed	Memory Total	CPU Model	CPU Speed	Install Date
16 GB	1000 MHz	16 GB DDR4	Intel Core i7	3.6 GHz (Boost up to 4.2 GHz)	2024-09-13
16 GB	500 MHz	16 GB DDR4	Intel Core i7	3.6 GHz (Boost up to 4.2 GHz)	2024-08-13
2 records matching search criteria					
Page: 1/1					
Records per page: 25					

Captura de tela do inventário de hardware

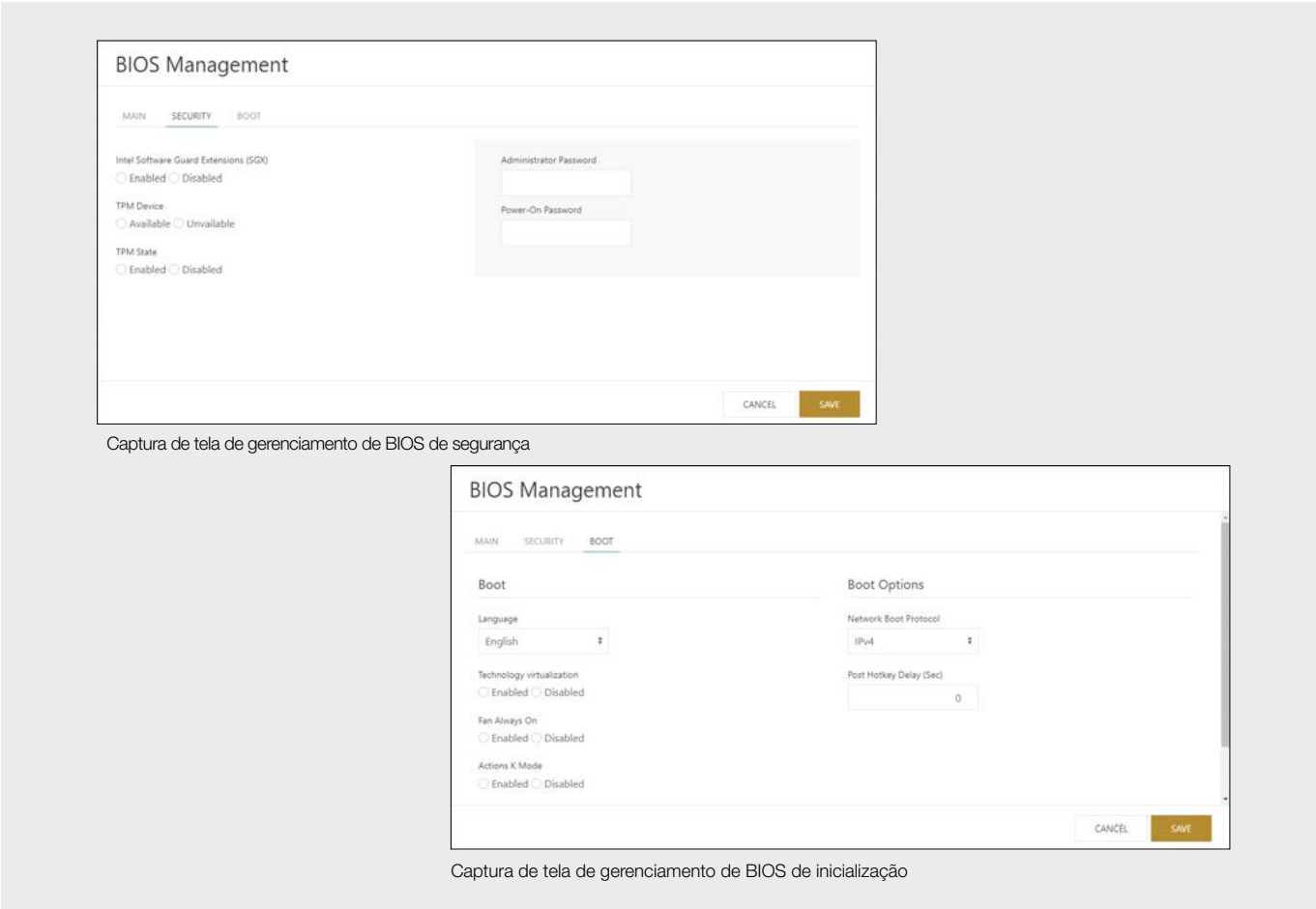
CUCo Remote BIOS Management

CUCo Remote BIOS Management permite que os administradores gerenciem e protejam remotamente as configurações de BIOS/UEFI em seus dispositivos, por meio de uma plataforma simplificada e fácil de usar. Este módulo inclui funcionalidades como gerenciamento de senha de BIOS, atualização remota de BIOS, alternância de chave de inicialização PXE, etc., apoiando as organizações na

implantação de atualizações em massa de firmware e concedendo aos administradores controle sobre as configurações de inicialização pela rede, aprimorando a segurança e reduzindo eficientemente a carga de trabalho. Finalmente, ele garante a integridade de segurança do BIOS, protegendo o firmware do dispositivo contra adulterações ou corrupções, mantendo assim a segurança geral do dispositivo.



Captura de tela principal de gerenciamento de BIOS



Captura de tela de gerenciamento de BIOS de segurança

Captura de tela de gerenciamento de BIOS de inicialização

Lista de Recursos

Aplicar atualizações remotamente ao BIOS/UEFI em vários dispositivos. Mantenha-os atualizados com os patches de segurança mais recentes, melhorias de estabilidade e aprimoramentos de compatibilidade de hardware, sem a necessidade de acesso físico.

Ativar ou desativar remotamente a senha de acesso ao BIOS. Garanta a segurança das configurações do BIOS contra alterações não autorizadas, permitindo acesso controlado para fins de solução de problemas e manutenção.

Ofereça a capacidade de adicionar, modificar ou remover remotamente senhas de acesso de usuários do BIOS, permitindo alinhar com políticas organizacionais ou necessidades específicas de segurança.

Habilitar ou desabilitar remotamente a opção de inicialização PXE, facilitando a inicialização baseada em rede para tarefas como implantação de sistema operacional, recuperação de sistema ou diagnósticos, melhorando a gerenciabilidade em ambientes grandes ou dispersos.

Permitir o habilitamento ou desabilitamento remoto de opções específicas de inicialização no BIOS/UEFI, ajustando o controle sobre como os dispositivos inicializam, aprimorando a segurança ao evitar acessos não autorizados e garantindo conformidade com políticas de TI.

Habilitar a recuperação remota da configuração atual da ordem de inicialização de um dispositivo, permitindo a verificação ou solução de problemas nas configurações de inicialização, garantindo que o dispositivo inicie a partir da fonte correta, conforme as políticas organizacionais.

Restaurar remotamente as configurações do BIOS para os valores padrão. Útil para resolver problemas de configuração, preparar dispositivos para redistribuição ou redefinir configurações de segurança para um estado conhecido e estável.

CUCo no setor de Educação

Em ambientes educacionais, a segurança dos dispositivos eletrônicos é fundamental para apoiar o ensino e a aprendizagem eficazes. CUCo Security Suite oferece uma variedade de funcionalidades exclusivas, adaptadas para atender às necessidades específicas de projetos educacionais, garantindo a segurança e a integridade dos dispositivos e dados.

Segurança baseada em firmware

Uma característica de destaque do CUCo Security Suite é seu modelo de segurança baseado em firmware, proporcionando proteção robusta desde o nível de firmware. Essa abordagem garante uma segurança abrangente, além da simples prevenção de roubo, permitindo a implementação de políticas de segurança personalizadas, adaptadas às necessidades de escolas e estudantes.

Independência de Sistema Operacional

CUCo Security Suite é compatível com diversos sistemas operacionais comumente encontrados em

ambientes educacionais, como Windows, Linux e Android. Essa versatilidade permite uma integração contínua com os ambientes de dispositivos existentes, simplificando os processos de implantação e gerenciamento para as instituições educacionais.

Funcionalidades RMM e MDM

CUCo Security Suite se destaca nas capacidades de gerenciamento remoto de dispositivos, facilitando atualizações de firmware, diagnósticos remotos e funcionalidades de bloqueio de dispositivos. Isso permite que os educadores monitorem e mantenham os dispositivos de

maneira eficiente em salas de aula e campi, garantindo experiências de aprendizagem ininterruptas.

Segurança do Dispositivo

A integração do CUCo Security Suite com recursos avançados de segurança, incluindo proteção contra malware no firmware e detecção de ameaças em tempo real, reforça sua posição como uma solução de segurança completa para ambientes educacionais. Essas capacidades não apenas protegem os dispositivos contra ameaças de segurança, mas também salvaguardam a privacidade dos estudantes e a integridade dos dados.

Estudo de Caso

CUCo Security Suite na Educação Protegendo os Estudantes no projeto “Escola Digital”

Introdução

Em resposta à crescente digitalização da educação, em 2020, o Ministério da Educação de Portugal lançou o projeto “Escola Digital”, com o objetivo de fornecer a cada aluno em Portugal acesso a um laptop. Com mais de 1,2 milhões de alunos envolvidos, essa iniciativa representou um investimento substancial, superior a 300 milhões de euros, necessitando de medidas robustas de proteção. Além do valor financeiro, a segurança dos estudantes contra possíveis furtos e danos foi primordial, dado o valor atrativo dos dispositivos e sua vulnerabilidade à exploração.

Problema

O Ministério enfrentou o desafio de proteger tanto os dispositivos quanto os estudantes, garantindo que os laptops fossem devolvidos ao final de cada ano letivo para redistribuição. Casos de alunos retendo os laptops levantaram preocupações sobre responsabilidade e gestão de ativos, demandando uma solução segura e econômica. Ao mesmo tempo, surgiram preocupações de que o projeto enfrentaria os mesmos problemas da iniciativa “e-escolinhas” (2007), criticada pela falta de opções de segurança e controle parental, além de sobrecarregar os professores com tarefas administrativas.

Análise

É aqui que o CUCo Security Suite entra em cena, oferecendo uma solução ideal para enfrentar esses desafios complexos. O CUCo capacita os responsáveis pelo projeto, como escolas e o Ministério da Educação, a bloquear ou desbloquear remotamente os dispositivos em caso de perda ou furto. Operando no nível de firmware, o CUCo permanece imune a tentativas de reinstalar o SO ou substituir os discos rígidos, garantindo uma proteção robusta. O CUCo também é eficaz em prevenir o acesso não autorizado a endpoints furtados. Ao proteger os dispositivos no nível de firmware, o CUCo garante que, mesmo se um dispositivo for roubado, os dados sensíveis sobre os estudantes e a instituição permaneçam protegidos. Além disso, o CUCo oferece um back office intuitivo para gerenciamento simplificado dos dispositivos

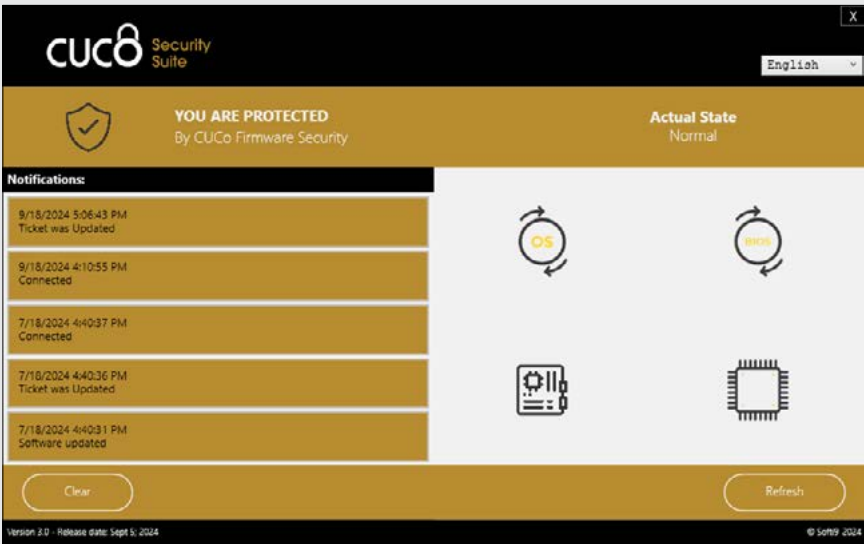
e integração perfeita com plataformas de gerenciamento existentes, por meio de APIs pré-desenvolvidas, aumentando a eficiência operacional. Como resultado da implementação bem-sucedida do CUCo Security Suite no projeto “Escola Digital”, uma nova fase foi alcançada, envolvendo a integração de funcionalidades adicionais de Mobile Device Management (MDM). Essas novas funcionalidades foram uma evolução natural do projeto e consideradas essenciais para seu sucesso contínuo, visando reduzir a carga de trabalho associada ao gerenciamento desses dispositivos.

Resultado

A adoção generalizada do CUCo Security Suite funcionou como um poderoso dissuasor contra furtos, desestimulando possíveis infratores e protegendo os alunos e os dispositivos. Além disso, casos de devoluções tardias foram rapidamente resolvidos por meio do bloqueio remoto dos dispositivos, garantindo conformidade e responsabilização. Ao implementar o CUCo Security Suite, o Ministério da Educação de Portugal gerenciou e protegeu com sucesso seu investimento, garantindo o uso correto dos dispositivos com o mínimo esforço de gestão e a um custo marginal para o projeto, ressaltando a eficácia e eficiência da solução.

Conclusão

De maneira geral, a integração do CUCo neste projeto levou ao desenvolvimento contínuo do CUCo Security Suite, desafiando-nos a introduzir uma nova gama de funcionalidades com o objetivo de lidar com novos problemas. Nossa solução agora inclui provisionamento automatizado de dispositivos, solução remota de problemas e ferramentas de gerenciamento de frota abrangentes, que capacitam administradores escolares e equipes de TI a gerenciar e manter os dispositivos de forma eficiente, garantindo que as atividades educacionais ocorram sem interrupções técnicas.



Captura de tela de Dispositivo protegido pelo CUCo

CUCo no setor Corporativo

No cenário corporativo atual, proteger dados sensíveis e informações confidenciais é de extrema importância. O CUCo Security Suite oferece uma camada adicional de proteção, blindando os dispositivos contra ameaças de firmware, como malware e manipulação não autorizada.

Facilitador de “Bring Your Own Device” (BYOD)

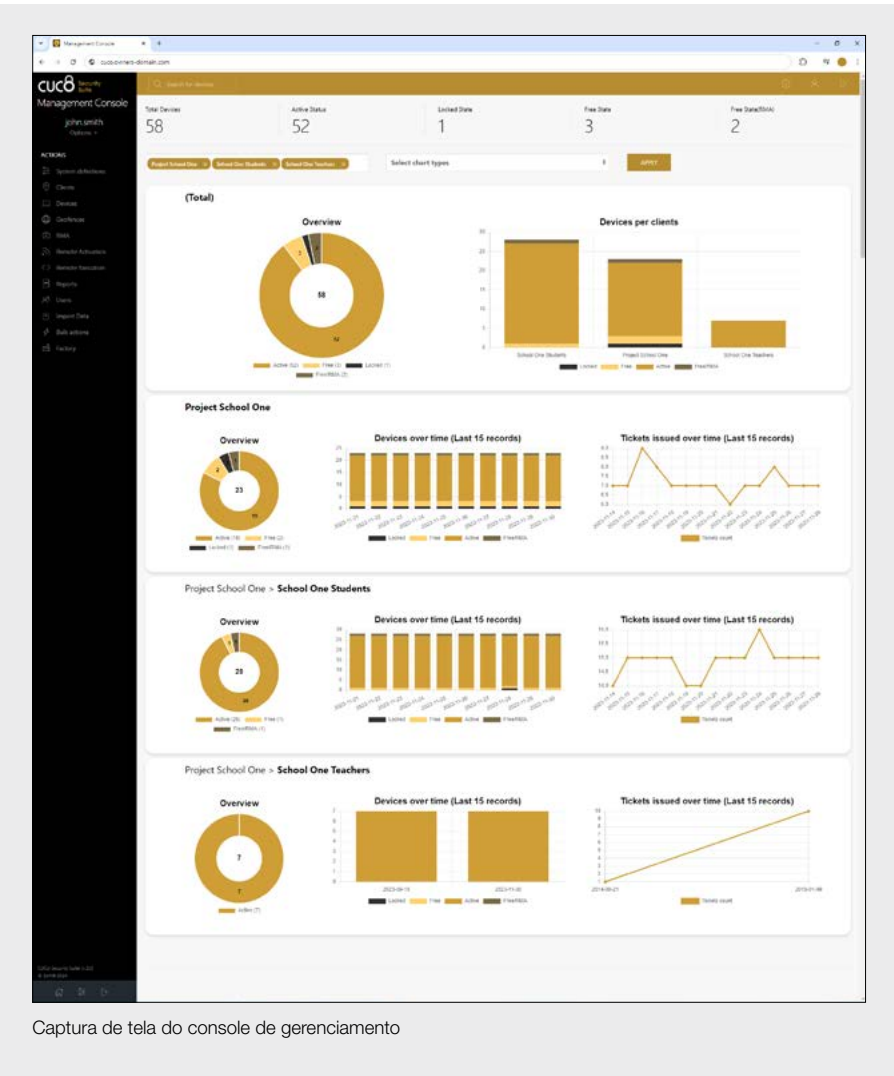
As funcionalidades de bloqueio de dispositivos, geofencing, firewall e filtragem de conteúdo do CUCo Security Suite permitem o método de trabalho “Bring Your Own Device” (BYOD), protegendo os dados e o próprio dispositivo em caso de roubo e garantindo que os dados da empresa estejam seguros contra malware.

Garantir Conformidade Regulamentar

As funcionalidades de monitoramento do CUCo Security Suite permitem que os administradores gerenciem quais softwares estão instalados nos dispositivos da empresa, modifiquem, instalem ou desinstalem remotamente e impeçam a instalação de software não autorizado.

Proporcionar Tranquilidade às Partes Interessadas

As diversas funcionalidades de segurança do CUCo Security Suite protegem o investimento, os ativos e os dados sensíveis da empresa.



Estudo de Caso

Projeto Piloto do CUCo Remote Lock Viabilizando Projetos DaaS

Introdução

Um projeto piloto liderado por um fabricante privado de computadores foi lançado em uma faculdade para testar a eficácia do CUCo Remote Lock como um sistema de execução de contratos e prevenção de furtos. Vários mil laptops, cada um no valor de €500, foram disponibilizados para estudantes de baixa renda por €149 cada, juntamente com um contrato de serviço de €14,90 por mês durante 2 anos. Não foi necessária verificação de crédito; os estudantes simplesmente precisavam assinar o contrato e pagar o valor inicial por meio de débito direto da conta bancária especificada no contrato.

Problema

Anteriormente, projetos Device as a Service (DaaS) enfrentaram muitos desafios relacionados à execução de contratos, gerenciamento de recursos e rastreamento de ativos. Portanto, negócios e projetos dessa natureza foram considerados inviáveis na maioria das vezes.

Análise

Neste contexto, o CUCo Remote Lock é um verdadeiro facilitador do modelo de negócios DaaS, proporcionando segurança robusta, garantindo a conformidade com os contratos de serviço e protegendo contra furtos e acessos não autorizados. Ao bloquear dispositivos não conformes e rastrear unidades perdidas ou roubadas, o CUCo minimiza perdas financeiras e aumenta a viabilidade de projetos de implantação em larga escala. Essa abordagem abrangente torna o CUCo um ativo inestimável para manter a integridade dos dispositivos e garantir o sucesso de iniciativas que dependem da distribuição generalizada de tecnologia.

Resultado

Após a execução do programa por mais de 2 anos, os dados estatísticos mostraram que 27,9% dos usuários pararam de pagar as parcelas mensais em algum

momento. O CUCo Remote Lock detectou a não conformidade e bloqueou automaticamente os dispositivos. Após a mensagem personalizada de “perdido-encontrado/bloqueado”, 98,6% dos usuários entraram em contato com o centro de atendimento, pagaram as parcelas em atraso e receberam um código único para desbloquear e reativar seus dispositivos. O CUCo Remote Lock reduziu significativamente o número de inadimplências ao bloquear unidades não conformes. Além disso, foi constatado que 3% das unidades estavam offline por mais de 2 meses. As regras internas do CUCo Remote Lock bloquearam esses dispositivos mesmo sem conectividade de rede. Durante esse período, 2% das unidades foram relatadas pelos usuários como roubadas ou perdidas. No entanto, devido à sua ‘pegada digital’ ao se conectar ao servidor do CUCo Remote Lock, a maioria dessas unidades foi recuperada e retornada ao usuário ou denunciada às autoridades. Ao final do período contratual, todas as unidades em conformidade foram liberadas do controle do CUCo Remote Lock. Sem o CUCo Remote Lock, a maioria das parcelas inadimplentes teria sido perdida, e o custo de recuperação por meio de agentes tradicionais ou do sistema jurídico teria sido muito alto. O CUCo Remote Lock economizou mais de 20% do preço de venda por unidade. Sem a solução CUCo Remote Lock, projetos de grande implantação baseados em fluxos financeiros futuros não seriam viáveis.

Conclusão

A implementação do CUCo Remote Lock neste projeto foi considerada bem-sucedida e confirmou ainda mais sua capacidade de melhorar e viabilizar projetos DaaS. Ao comparar dados de projetos DaaS passados com a iniciativa do CUCo Remote Lock, conseguimos verificar sua capacidade de executar contratos, prevenir furtos e proteger os investimentos feitos pelo fornecedor dos dispositivos.

Análise Comparativa do CUCo Remote Lock em relação aos 3 principais concorrentes

	CUCo	C1	C2	C3
Plataforma aberta, baseada nos padrões UEFI, compatível com várias marcas de dispositivos finais	✓	✓	✓	✗
Bloqueio remoto de firmware de único propósito, controle automático de dispositivo, bloqueio pré-boot do OS	✓	✗	✓	✓
Nenhum acesso aos dados do usuário no dispositivo pelo gerente da plataforma (compliance com o GDPR)	✓	✗	✓	✗
Reativação remota do dispositivo após o evento de bloqueio (sem dependência de software)	✓	✗	✓	✓
Autoproteção contra tentativas de hackeamento para desativar a segurança no dispositivo	✓	✓	✗	✗
Baixa largura de banda e funcionamento sem conectividade por um período definido	✓	✗	✗	✗
Suporte a múltiplos sistemas operacionais, incluindo Windows, Linux, Android. Bloqueio via firmware	✓	✗	✓	✗
Foco em segurança “apenas de hardware”. Agnóstico a dados e conteúdo	✓	✗	✗	✗
Desativação remota irrevogável do mecanismo de segurança	✓	✓	✗	✓
Resiliência a alterações do sistema operacional	✓	✗	✗	✗

Análise Comparativa do CUCo Secure Endpoint em relação aos 3 principais concorrentes

	CUCo	C1	C2	C3
Agente de software de endpoint resiliente	✓	✓	✗	✗
Ferramentas de gerenciamento de hardware	✓	✓	✓	✓
Ferramentas de geofencing	✓	✗	✗	✗
Execução de instruções críticas certificadas com base em blockchain	✓	✗	✗	✗
Acesso ao rastreamento em tempo real do dispositivo e histórico de localização	✓	✗	✗	✗
Rastreamento de eventos de login e desbloqueio	✓	✗	✓	✗
Programa Safer Internet, filtragem de DNS e filtros de conteúdo	✓	✗	✓	✓

Análise Comparativa do CUCo Remote BIOS Management em relação aos 2 principais concorrentes

	CUCo	C1	C2
Atualização remota do BIOS em múltiplos dispositivos simultaneamente	✓	✗	✓
Ativação e desativação remota da senha do BIOS	✓	✗	✗
Habilitação/desabilitação remota da opção de inicialização PXE	✓	✓	✓
Recuperação remota das configurações atuais da ordem de inicialização	✓	✗	✗
Restauração remota das configurações padrão	✓	✗	✗

Tecnologia Blockchain

A integração da tecnologia Blockchain foi o próximo passo natural para a evolução contínua e desenvolvimento do CUCo Security Suite.

Blockchain é uma tecnologia que permite a criação de registros digitais imutáveis, possibilitando transações e registros seguros em uma rede ponto-a-ponto (P2P), descentralizando a informação e eliminando a necessidade de envolver terceiros no processo de verificação de dados. O Blockchain realiza isso codificando informações em “blocos”, de modo que cada novo “bloco” de informações adicionado é criptografado com um código baseado no bloco anterior. Esse processo mantém todos os dados ordenados cronologicamente e vinculados através de seus próprios códigos, criando a “cadeia” de informações.

A manipulação das informações nesta tecnologia é inviável, pois tentativas de fazê-lo resultariam em blocos totalmente novos de informações, tornando fácil para outros pares detectarem rapidamente a anomalia e rejeitarem os dados não autorizados.

A tecnologia Blockchain como campo está crescendo exponencialmente, estando presente em diversos setores como cibersegurança, bancos, saúde, logística e contratos inteligentes.

Atualmente, o CUCo Security Suite implementa contratos inteligentes como uma forma de verificar o cumprimento das regras entre as diferentes partes de forma mais eficaz e segura. Os contratos inteligentes funcionam armazenando as informações do contrato em um blockchain, descentralizando-as e tornando-as prontamente disponíveis para consulta de todas as partes, sem o risco de adulteração. Os contratos inteligentes verificam simultaneamente se todas as partes estão em conformidade com as condições predeterminadas, garantindo a segurança dos negócios para todas as partes envolvidas.

Modelo de Negocio

Licenciamento e Parcerias

A maioria dos principais fabricantes de computadores já licenciou e certificou seus dispositivos como compatíveis com o CUCo Security Suite. Nosso novo programa de certificação de dispositivos permite que o CUCo Security Suite ofereça oportunidades de licenciamento para vários parceiros OEM, seja sob a marca CUCo ou por meio de acordos de marca branca.

Ativação e Implantação

O CUCo Security Suite pode ser ativado por meio de planos de assinatura fornecidos por provedores de serviços licenciados e parceiros confiáveis, exclusivamente em hardware aprovado e previamente provisionado. Cada dispositivo pronto para CUCo passa por rigorosos testes e validações pela nossa equipe de engenharia especializada antes de ser lançado no mercado.

Opções de Entrega Flexíveis

Os provedores de serviços têm a flexibilidade de entregar nossa solução de segurança de ponta, seja por meio de acesso seguro baseado em nuvem ou implantando servidores de autorização diretamente nas instalações do cliente. Isso garante conformidade com as preferências e requisitos legais do cliente, incluindo total aderência às regulamentações do RGPD.

Para mais informações sobre qualquer uma dessas opções ou para discutir como podemos trabalhar juntos, entre em contato conosco pelo e-mail partners@cuco-firmware.com. Estamos aqui para ajudá-lo a encontrar a melhor solução para as necessidades do seu negócio.

cucô Security Suite

cucô Security Suite
www.cuco-firmware.com
sales@cuco-firmware.com

Desenvolvido por



Cofinanciado por



201BR01D.001

DECLARAÇÃO

A CUCo Firmware Security, Lda. vem por este meio garantir o cumprimento, pelo CUCo Security Suite, dos seguintes requisitos, refutando as questões levantadas após a análise inicial, pela entidade reguladora do concurso público MP DE GOIÁS - (PID 1658-25).

5.1.8. SEGURANÇA e GERENCIAMENTO:

5.1.8.1. O equipamento deve acompanhar ferramenta de segurança já licenciada e com gerenciamento centralizado, acessada através de browser que contemple

5.1.8.1.1. Geolocalização: Rastreamento de ativos, utilizando tecnologia como Google Wifi ou GPS, mas não restrita a elas, e que inclua o local atual do ativo e seu histórico de localizações. Possibilidade de criar áreas geográficas demarcadas com base em políticas corporativas. Possibilidade de investigação de dispositivos extraviados, perdidos ou roubados ou dos que estão fora dos limites geográficos estabelecidos ou entrando em um local não autorizado;

5.1.8.1.2. A solução deve possuir recursos para que em caso de extravio, perda ou roubo do equipamento, após conectá-lo novamente à Internet, seja possível bloqueá-lo, excluir suas informações confidenciais remotamente e gerar relatórios para comprovar sua conformidade com regulamentos governamentais e corporativos;

5.1.8.1.3. Possuir grau de persistência integrado à BIOS/Firmware ativada de fábrica com recursos para se autorreparar caso o sistema operacional Windows ou a imagem de softwares utilizada pela CONTRATANTE, baseada em Windows, sejam reinstalados ou mesmo o disco rígido substituído;

5.1.8.1.4. Deverá apresentar comprovação que o equipamento fornecido é compatível com os requisitos solicitados, por meio de site oficial do fabricante/desenvolvedor, como por exemplo Absolute Software (<https://www.absolute.com/en-gb/partners/compatibility>) ou outro site público de outro fabricante que comprove as mesmas funcionalidade solicitadas;

5.1.8.1.5. Deverá funcionar por todo o tempo de garantia do equipamento

A CUCo Firmware Security garante que, os dispositivos DATEN, que incluam o sistema CUCo Security Suite, cumprem com os requisitos mencionados acima, no item **Solução de Bloqueio, Rastreo e Segurança**, definidos no concurso e que irão funcionar por todo o tempo de garantia do equipamento.

O CUCo Security Suite funciona com base em firmware, garantindo a sua persistência e dos módulos integrados no mesmo.

Esta informação poderá ser, inclusive, verificada na nossa página web: <https://cuco.net> ou, alternativamente, no nosso catálogo, incluídos em anexo.

Adicionalmente, no catálogo nas páginas 3 a 7, incluído em anexo, poderão verificar o cumprimento das funcionalidades mencionadas no item acima.

Aveiro, 26 de maio de 2026

CUCo Firmware Security, Lda.

A Gerência

Jorge S. Pinto – Managing Director

Ao

MINISTÉRIO PÚBLICO DO ESTADO DE GOIÁS

ATT: COMISSÃO DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO Nº 117/2025

DIL0019-26

A DATEN TECNOLOGIA LTDA., pessoa jurídica de direito privado, com sede à Rodovia Ilhéus – Uruçuca, Km 3,5, S/N, Galpão, Distrito Industrial de Ilhéus, Ilhéus/BA, inscrita no CNPJ sob o nº 04.602.789/0001-01, vem respeitosamente perante V.Sa., apresentar a resolução da diligência enviada nesta data, relativa ao PREGÃO ELETRÔNICO Nº 117/2025.

QUESTIONAMENTO 01: *1. Ausência de Identificação e Documentação Técnica do Equipamento. Em diligência realizada no site oficial do fabricante, não foram localizados o modelo do equipamento ofertado (MINI PC-DC8B-U) tampouco o part number indicado na proposta comercial. Adicionalmente, não foi encontrada a documentação técnica (datasheets, manuais ou especificações detalhadas) correspondente a este equipamento no portal do fabricante.*

RESPOSTA: O modelo MINI PC DC8B-U é um equipamento recém-lançado, e no momento da diligência, o site oficial está em processo de atualização, para a adição dos novos equipamentos. Para suprir essa solicitação de forma definitiva, encaminhamos os links no site oficial para consulta:

Link do manual: [Manual DC8B-U](#)

Link do equipamento: [DC8B-U](#)

Link do SSD: [DS4000](#)

Link da memória: [Memória RAM Daten DDR5](#)

Link do teclado: [CK510U](#)

Link do mouse: [CM627U](#)

Destacamos que o item 8.1 do edital admite como formas de comprovação, de maneira alternativa, catálogos, datasheets ou declaração oficial do fabricante. Os documentos apresentados se enquadram plenamente nessas modalidades, atendendo ao exigido.

Declaramos, ainda, que os modelos e componentes indicados na proposta correspondem ao modelo ofertado para o Pregão Eletrônico Nº 117/2025.

QUESTIONAMENTO 02: *2. Pendências no Item 5.1.8 - Segurança e Gerenciamento (Software CUCo). A proposta comercial apresenta o software CUCo para o atendimento deste requisito,*

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45.658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

contudo, identificamos as seguintes não conformidades: • Não consta na proposta comercial a comprovação técnica exigida para o "Software de SEGURANÇA E GERENCIAMENTO"

RESPOSTA: A CUCo, desenvolvedora do software persistente CUCo Security Suite, emitiu uma declaração, comprovando as funcionalidades do software e o atendimento aos pontos solicitados no item 5.1.8. do Termo de Referência.

Segue em anexo o arquivo "Declaração CUCo" e "CATÁLOGO – CUCo", comprovando o solicitado.

Diante dos pontos diligenciados e da documentação complementar anexada, resta claro que o equipamento ofertado para o Pregão Eletrônico nº 117/2025 atende plenamente às especificações técnicas exigidas no edital.

Ilhéus-Ba, 27 de maio de 2026.

Atenciosamente,

Documento assinado digitalmente
 **IGOR LEONARDO DE SANTANA CRUZ**
Data: 27/05/2026 12:21:49-0300
Verifique em <https://validar.it.gov.br>

Igor Leonardo de Santana Cruz
RG nº 100.176.46-17 - SSP-BA
CPF nº 039.693.675-06
Lider Pré-venda - Comercial Governo

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45.658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

DECLARAÇÕES PARA HABILITAÇÃO

DATEN TECNOLOGIA LTDA

PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DE GOIÁS
PREGÃO ELETRÔNICO Nº 117/2025
PID (PROCESSO INTERNO DATEN) = 1658-25

Ilhéus-Ba, 20 de maio de 2026

À

PROCURADORIA-GERAL DE JUSTIÇA DO ESTADO DE GOIÁS

ATT: COMISSÃO DE LICITAÇÃO

REF.: PREGÃO ELETRÔNICO Nº 117/2025

DECLARAÇÃO GERAL

A Daten Tecnologia Ltda., inscrita no CNPJ 04.602.789/0001-01, Rodovia BA 262, KM 3,5, Sentido Uruçuca - Distrito Industrial de Ilhéus -Iguape, CEP: 45658-335, Ilhéus/BA, declara, sob as penas da Lei:

- a) que a Propostas Econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, na forma do §1º do art. 63 da Lei Federal nº 14.133, de 2021
- b) que até a presente data inexistem fatos impeditivos para sua habilitação, ciente da obrigatoriedade de declarar ocorrências posteriores.
- c) cumprimos ao disposto no artigo 7º, Inc. XXXIII da Constituição Federal, quanto à proibição de trabalho noturno, perigoso ou insalubre a menor de dezoito anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
- d) elaboramos de forma Independente a Proposta, de acordo com o disposto na Portaria SDE nº 51 de 3 de julho de 2009 do Ministério da Justiça.
- e) não utilizamos Trabalho Degradante ou Forçado.
- f) acessibilidade, nos termos do Art. 93 da Lei nº 8.213, de 24 de julho de 1991.
- g) o pleno conhecimento e atendimento às exigências previstas no Edital.
- h) a exequibilidade da proposta encaminhada, estando incluso nos preços propostos todas as despesas relacionadas com o objeto da licitação, como impostos, fretes, seguros, taxas, encargos trabalhistas, previdenciários, sociais, fiscais e comerciais, gastos com transportes, prêmios de seguros e outras despesas decorrentes de exigência legal.

DECLARAÇÃO DE REGULARIDADE – ANEXO III

A Daten Tecnologia Ltda., inscrita no CNPJ 04.602.789/0001-01, nos termos das Resoluções 37/2009, nº 172/2017 e nº 241/2021 do Conselho Nacional do Ministério Público, e, ainda, nos termos do artigo

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

14 da Lei nº 14.133/2021, DECLARO, para fins de contratação e fornecimento junto a Procuradoria Geral de Justiça do Estado de Goiás, que:

- a) Os sócios desta pessoa jurídica, bem como seus, gerentes e diretores, não são cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, ou que estavam no exercício dos respectivos cargos e funções, nos últimos 6 (seis) meses, no Ministério Público do Estado de Goiás.
- b) A empresa, seus sócios, dirigentes, gerentes e diretores não se enquadram em nenhum dos impedimentos previstos no artigo 14, inclusive em seus incisos e parágrafos, da Lei nº 14.133/2021.

TERMO DE ANUÊNCIA – ANEXO IV

Contratada/Fornecedora: Daten Tecnologia Ltda

Objeto: Mini Desktops

CNPJ: 04.602.789/0001-01

E-mail: licitacao@daten.com.br / comercial@daten.com.br

Telefone (WhatsApp): (71) 99617-9557 / (71) 99617-9547

DECLARO que ACEITO RECEBER COMUNICAÇÕES PROCESSUAIS POR MEIO DO APLICATIVO WHATSAPP, no contato telefônico supra informado.

Declaro, ainda, que:

- I. Possuo o aplicativo de envio de mensagem eletrônica WhatsApp instalado em aparelho celular, tablet ou computador;
- II. Estou ciente de que o MPGO, em nenhuma hipótese, solicita dados pessoais, bancários ou qualquer outro de caráter sigiloso;
- III. Estou ciente de que, no ato da notificação, o servidor responsável encaminhará pelo aplicativo de mensagens eletrônicas o teor da comunicação relativa a procedimento administrativo decorrente de licitação ou contratação, com a identificação do processo e das partes;
- IV. Estou ciente que considerar-se-á realizada a notificação no momento em que os ícones de envio e entrega de mensagens eletrônicas forem disponibilizados, dispensada a confirmação de leitura, e que, no caso de insucesso da notificação por WhatsApp, será utilizado e-mail e publicação no Diário Oficial do MPGO para a devida comunicação;
- V. Quaisquer dúvidas e manifestações referentes à notificação deverão ser suscitadas exclusivamente nos autos do processo, por meio do protocolo eletrônico, não sendo admitidos questionamentos, dúvidas ou manifestações via WhatsApp;

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500

- VI. Estou ciente de que é proibido o envio por WhatsApp de petições, documentos, imagens ou vídeos;
- VII. Estou ciente, ainda, de que, se houver mudança do número do telefone ou e-mail acima indicados, deverei informar tal fato imediatamente ao MPMO, devendo assinar novo termo, reputando-se eficazes as intimações enviadas ao telefone ou e-mail anteriormente cadastrados na ausência de comunicação da mudança.

Ilhéus-Ba, 20 de maio de 2026



Documento assinado digitalmente
IGOR LEONARDO DE SANTANA CRUZ
Data: 20/05/2026 15:21:03-0300
Verifique em <https://validar.iti.gov.br>

Igor Leonardo de Santana Cruz
RG nº 100.176.46-17 SSP-BA
CPF nº 039.693.675-06
Lider Pré-venda - Comercial Governo

04.602.789/0001-01

DATEN TECNOLOGIA LTDA

Rodovia Ilhéus-Uruçuca, Km 3,5, s/nº - Galpão
Distrito Industrial de Ilhéus - CEP 45.658-335

ILHÉUS-BAHIA

Matriz

Rod. BA 262 - Km 3,5 - Sentido Uruçuca - Ilhéus
Distrito Industrial de Ilhéus.
Ilhéus/BA - Brasil - CEP: 45658-335
Tel: +55 73 3222.6200

Filial Salvador

Rua Frederico Simões, 125 - 6º andar
Edf. Liz Empresarial, Caminho das Árvores
Salvador/BA - Brasil - CEP: 41.820-774
Tel: +55 71 3616.5500