Intel® Active Management Technology: গোপনীয়তার বিবৃতি

সর্বশেষ আপডেট: 8/12/2021

Intel Corporation আপনার গোপনীয়তা. রক্ষা করার জন্য প্রতিশ্রুতিবদ্ধ। এই বিবৃতিটি বর্ণনা করে যে Intel® Active Management Technology (Intel® AMT) কী গোপনীয়তা-সংবেদনশীল ফাংশন এবং ক্ষমতা সক্ষম করে, Intel AMT আইটি অ্যাডমিনিস্ট্রেটরদের কী অনুমতি দেয় এবং কী করতে দেয় না এবং ব্যবহারকারীর সিস্টেমে Intel AMT কী ধরনের ডেটা সঞ্চয় করে তা নির্দেশ করে। এই বিবৃতি Intel-এর অনলাইন গোপনীয়তা বিজ্ঞপ্তির জন্য সম্পূরক এবং শুধুমাত্র Intel-এর AMT এর ক্ষেত্রে প্রযোজ্য।

Intel AMT কী?

Intel AMT অনুমোদিত আইটি অ্যাডমিনিস্ট্রেটরদের দ্বারা এন্টারপ্রাইজের নেটওয়ার্কযুক্ত কম্পিউটার সিস্টেমগুলোর আউট-অফ-ব্যান্ড (OOB) রিমোট সহায়তা এবং পরিচালনাকে সক্ষম করে।

Intel AMT দ্বারা উত্থাপিত সম্ভাব্য গোপনীয়তা সমস্যাগুলো কী কী?

রিমোট ম্যানেজমেন্ট ক্ষমতা সফটওয়্যার বিক্রেতাদের কাছে উপলভ্য এবং অনেক সংস্থার আইটি বিভাগ কর্তৃক যথেষ্ট সময় ধরে ব্যবহার করা হয়েছে।

তবে, Intel AMT আইটি অ্যাডমিনিস্ট্রেটরদের কোনো ব্যবহারকারীর কম্পিউটারকে রিমোট সহায়তা এবং পরিচালনা করার অনুমতি দেয়, এমনকি যদি ব্যবহারকারী উপস্থিত না থাকে বা কম্পিউটারটি বন্ধ করে দেওয়া হয়।

কিভাবে ব্যবহারকারী সিস্টেমটিতে Intel AMT সক্রিয় কি না তা বলতে পারেন?

Intel AMT-এর বর্তমান অবস্থা সম্পর্কে চূড়ান্ত ব্যবহারকারীকে স্বচ্ছতা এবং বিজ্ঞপ্তি প্রদানের জন্য Intel একটি সিস্টেম ট্রে আইকন তৈরি করেছে। বর্তমানে, স্ট্যান্ডার্ড Intel AMT সফটওয়্যারটিতে একটি Intel® Management and Security Status (IMSS) অ্যাপ্লিকেশন এবং সিস্টেম ট্রে আইকন রয়েছে যা ড্রাইভার এবং পরিষেবাগুলোর সাথে ইনস্টল করা হয়। IMSS সিস্টেম ট্রে আইকনটি সিস্টেমে (সক্রিয় বা নিষ্ক্রিয়) Intel AMT-এর বর্তমান অবস্থা প্রদর্শন করে এবং কীভাবে Intel AMT ক্ষমতাগুলো সক্রিয়/নিষ্ক্রিয় করতে হয় সে সম্পর্কে নির্দেশাবলীও প্রদান করে। Intel সুপারিশ করে যে প্রতিটি মূল সরঞ্জাম প্রস্তুতকারক (OEM) IMSS অ্যাপ্লিকেশনটি লোড করে। তবে, OEM-গুলো Intel-এর এই সুপারিশটি মেনে না চলার সিদ্ধান্ত নিতে পারে এবং এছাড়াও, চূড়ান্ত-গ্রাহক আইটি পরিচালকরা চূড়ান্ত ব্যবহারকারীদের Intel AMT-সক্রিয় সিস্টেম সরবরাহ করার আগে IMSS অ্যাপ্লিকেশনটি অপসারণ করতে বেছে নিতে পারেন। OEM বাস্তবায়নের উপর নির্ভর করে, ব্যবহারকারীরা তাদের কম্পিউটারের সিস্টেম BIOS-এ Intel AMT-এর অবস্থাও পরীক্ষা

করতে পারেন। তবে, এটি লক্ষ্য করা গুরুত্বপূর্ণ যে কিছু এন্টারপ্রাইজ আইটি বিভাগ ব্যবহারকারীদের সিস্টেম BIOS-এ প্রয়োজনীয় অ্যাক্সেস দিতে পারে না যা Intel AMT সক্রিয়/নিষ্ক্রিয় করতে বা Intel AMT-এর অবস্থা পরীক্ষা করার জন্য প্রয়োজনীয়।

Intel AMT ব্যবহারকারীর কাছ থেকে কোন ব্যক্তিগত তথ্য সংগ্রহ করে?

Intel AMT ব্যবহারকারীর কাছ থেকে কোনো ব্যক্তিগত তথ্য (উদাহরণস্বরূপ, নাম, ঠিকানা, ফোন নম্বর, ইত্যাদি) সংগ্রহ করে না।

Intel AMT কর্তৃক Intel Corporation কোন ধরনের তথ্য পাঠানো হয় এবং কিভাবে সেই তথ্য ব্যবহার করা হয়?

Intel AMT Intel Corporation কোনো তথ্য পাঠায় না।

Intel AMT কোন ধরনের তথ্য সংরক্ষণ করে?

Intel AMT সিস্টেমের মাদারবোর্ডে ফ্ল্যাশ মেমরিতে তথ্য সংরক্ষণ করে। এই তথ্যের মধ্যে ফার্মওয়্যার কোড, হার্ডওয়্যার ইনভেন্টরি ডেটা (উদাহরণস্বরূপ, মেমরির আকার, সিপিইউ এর ধরন, হার্ড-ডিস্কের ধরন), একটি ইভেন্ট লগ যা প্ল্যাটফর্ম ইভেন্টগুলো রেকর্ড করে (উদাহরণস্বরূপ, সিপিইউ হিট আপ, ফ্যানে ত্রুটি, BIOS পোস্ট বার্তা), Intel AMT সুরক্ষা ইভেন্টগুলো (উদাহরণস্বরূপ, Intel AMT পাসওয়ার্ড আক্রমণ ইভেন্টের সতর্কতা, বা সিস্টেম ডিফেন্স ফিল্টার ট্রিপিং), পাশাপাশি Intel AMT কনফিগারেশন ডেটা (উদাহরণস্বরূপ, নেটওয়ার্ক সেটিংস, অ্যাক্সেস কন্ট্রোল তালিকা এবং সর্বজনীন অনন্য শনাক্তকারী (UUID), প্রোভিশনিং ডেটা, ল্যান ম্যাক অ্যাড্রেস, কী, কীবোর্ড-ভিডিও-মাউস (KVM) পাসওয়ার্ড, ট্রান্সপোর্ট লেয়ার সিকিউরিটি (TLS) সার্টিফিকেট এবং আইটি কনফিগার করা ওয়্যারলেস নেটওয়ার্ক প্রোফাইল সহ)। সংবেদনশীল হিসাবে বিবেচিত সকল কনফিগারেশন ডেটা ফ্ল্যাশে একটি এনক্রিপ্ট করা আকারে সংরক্ষণ করা হয়। UUID-সমূহ সম্পর্কিত আরও তথ্য নীচের বিভাগে পাওয়া যাবে।

Intel AMT সংস্করণ 11.0 এবং পুরনো নিবন্ধিত স্বাধীন সফটওয়্যার বিক্রেতা (ISV) অ্যাপ্লিকেশনগুলোকে তৃতীয় পক্ষের ডেটা স্টোর (3PDS) নামে পরিচিত ফ্ল্যাশ মেমরি সংগ্রহস্থলের একটি এলাকায় ডেটা সংরক্ষণ করার অনুমতি দেয়। Intel AMT সংস্করণ 11.6 থেকে শুরু করে, এই বৈশিষ্ট্যটি ওয়েব অ্যাপ্লিকেশন হোস্টিং দিয়ে প্রতিস্থাপিত হয়েছিল যা Intel AMT-কে নন-ভোলাটাইল মেমরিতে (NVM) ওয়েব অ্যাপ্লিকেশন হোস্ট করতে দেয় যা Intel AMT ক্লায়েন্ট প্ল্যাটফর্মে স্থানীয়ভাবে পরিচালনা করে।

যদিও Intel তার ISV-গুলোতে দায়িত্বশীল ডেটা পরিচালনার জন্য যাকে তারা সর্বোত্তম গোপনীয়তা অনুশীলনবলে মনে করে সেগুলিই যোগাযোগ করে, তবুও শেষ পর্যন্ত Intel ফ্ল্যাশ মেমরির এই এলাকায় কোন ডেটা সংরক্ষণ করা যেতে পারে তা নির্ধারণ করে না এবং ISV ডেটার জন্য এনক্রিপশন পদ্ধতি সমর্থন করে না। সুতরাং ISV-গুলোকে ফ্ল্যাশে সংরক্ষণ করার আগে তাদের ডেটা এনক্রিপ্ট করতে উৎসাহিত করা হয় যদি তারা তাদের ডেটা সংবেদনশীল বলে মনে করে। এখানে

সঞ্চিত তথ্যের কারণে আপনার যদি সম্ভাব্য গোপনীয়তার ঝুঁকি সম্পর্কে উদ্বেগ থাকে তাহলে অনুগ্রহ করে NVM-এ তারা যে ধরনের তথ্য এবং ওয়েব অ্যাপ্লিকেশন সংরক্ষণ করছে এবং এটি কিভাবে সুরক্ষিত রয়েছে তা সম্পর্কে আরও বিস্তারিতের জন্য উপযুক্ত তৃতীয় পক্ষের সফটওয়্যার ডেভেলপারের সাথে যোগাযোগ করুন।

Intel AMT কিভাবে UUID ব্যবহার করে? Intel AMT-সক্ষম প্ল্যাটফর্মগুলোতে UUID-সমূহ কোন কার্যকারিতা সক্রিয় করে এবং সক্রিয় করে না?

ইউনিভার্সাল ইউনিক আইডেন্টিফায়ারস (UUIDs) হলো Intel AMT দ্বারা বিভিন্ন উদ্দেশ্যে ব্যবহৃত নিদর্শন, যার মধ্যে রয়েছে প্রভিশনিং প্রক্রিয়া, সিস্টেমের সুরক্ষা (উদাহরণস্বরূপ, পাসওয়ার্ড, কী এবং TLS সার্টিফিকেট), এবং আইটি অ্যাডমিনিস্ট্রেটররা কোনো এন্টারপ্রাইজের মধ্যে কোনো নির্দিষ্ট ব্যবহারকারীর সিস্টেমের সাথে সঠিকভাবে সংযোগ এবং পরিচালনা করতে সক্ষম কিনা তা নিশ্চিত করার জন্য।

Intel VPRO প্ল্যাটফর্মগুলো Intel® Unique Platform ID (UPID) নামে একটি স্থায়ী UUID সরবরাহ করে যা জিরো-টাচ প্রভিশনিংয়ের মতো অবিরাম UUID-এর প্রয়োজন এমন ক্ষেত্রে ব্যবহার সক্ষম করে। UPID এর কার্যকারিতা OEM বাস্তবায়নের উপর নির্ভরশীল। UUID-সমূহ কার্যত সকল আধুনিক পিসিতে উপস্থিত থাকে এবং সাধারণত Intel AMT-এর সাথে সম্পর্ক ছাড়াই সকল প্ল্যাটফর্মে OEM দ্বারা ইনস্টল করা হয়। প্রকৃতপক্ষে, UUID-সমূহ বর্তমানে প্রত্যাশিত কার্যকারিতা সরবরাহের জন্য অনন্য সিস্টেমের তথ্য পৃথক করতে অনেক পিসিতে পাওয়া অ্যাপ্লিকেশন দ্বারা ব্যবহৃত হয়, যেমন OS বা ভাইরাস নিয়ন্ত্রণ সিস্টেম আপডেট সরবরাহ। Intel AMT প্ল্যাটফর্ম UUID-সমূহ খুব অনুরূপভাবে ব্যবহার করে - প্রাথমিক পার্থক্যটি হলো Intel AMT-কে UUID-সমূহ OOB অ্যাক্সেস করতে সক্ষম করার জন্য, UUID ফ্ল্যাশ মেমরি সংগ্রহস্থলে কপি করা হয়।

এটি লক্ষ্য করা গুরুত্বপূর্ণ যে UUID সহ Intel AMT-সক্রিয় সিস্টেমগুলোতে UUID-সমূহ ব্যবহারকারীদের বা তাদের পিসিগুলো ট্র্যাক করতে Intel দ্বারা ব্যবহার করা যাবে না, বা তারা Intelকে প্ল্যাটফর্মের ব্যাক ডোরের মাধ্যমে ব্যবহারকারী সিস্টেমগুলো অ্যাক্সেস করার অনুমতি দেয় না, বা তারা ব্যবহারকারীর সম্মতি ব্যতীত প্ল্যাটফর্মে ফার্মওয়্যারকে জোর করার অনুমতি দেয় না। Intel AMT দ্বারা ফ্ল্যাশে সঞ্চিত যেকোনো UUID কেবলমাত্র একটি নির্দিষ্ট Intel AMT-সক্রিয় প্ল্যাটফর্মের জন্য অনুমোদিত আইটি অ্যাডমিনিস্ট্রেটরদের কাছে অ্যাক্সেসযোগ্য। অনুমোদিত আইটি অ্যাডমিনিস্ট্রেটরদের তালিকাটি এন্টারপ্রাইজ সার্টিফিকেট বা Intel AMT সিস্টেমে (BIOS মেনু বা USB কী এর মাধ্যমে) শারীরিক উপস্থিতি ব্যবহার করে একটি সুরক্ষিত প্রক্রিয়া চলাকালীন চূড়ান্ত গ্রাহক আইটি দ্বারা কনফিগার করা হয় এবং এইভাবে শেষ গ্রাহক আইটি দ্বারা মনোনীত বিশ্বস্ত সার্ভারগুলোতে বসবাসকারী কনসোলগুলোর সাথে সম্পূর্ণরূপে ঘটে। অন্য কথায়, UUID বা অন্য কোনো তথ্য Intel AMT-এর মাধ্যমে চূড়ান্ত গ্রাহকের বাইরের কোনো পক্ষের কাছে বা থেকে যোগাযোগ করা যাবে না যতক্ষণ না চূড়ান্ত গ্রাহক স্পষ্টভাবে এটি কনফিগার করে। কোনো নির্দিষ্ট সিস্টেমের জন্য অনুমোদিত অ্যাডমিনিস্ট্রেটরদের শনাক্ত করতে, https://software.intel.com/en-us/business-client/manageability উপলভ্য Intel AMT সফটওয়্যার ডেভেলপার কিট (SDK)

ডকুমেন্টেশন দেখুন যা ACL বা কেরবেরোস অনুমোদিত অ্যাকাউন্টগুলো পুনরুদ্ধার করার জন্য একটি API সরবরাহ করে।

Intel® Active Management Technology (Intel® AMT) নেটওয়ার্ক জুড়ে কী ধরনের তথ্য পাঠায়?

Intel AMT পূর্বনির্ধারিত IANA নেটওয়ার্ক পোর্টগুলোতে ডেটা প্রেরণ এবং গ্রহণ করে: SOAP/HTTP-এর জন্য পোর্ট 16992, SOAP/HTTPS-এর জন্য পোর্ট 16993, রিডাইরেকশন/TCP-এর জন্য পোর্ট 16994 এবং রিডাইরেকশন/TLS-এর জন্য পোর্ট 16995। ড্যাশ কমপ্লায়েন্ট সিস্টেমগুলো HTTP-এর জন্য 623 এবং HTTPS-এর জন্য 664 পোর্টে ডেটা প্রেরণ ও গ্রহণ করবে। কীবোর্ড-ভিডিও-মাউস (KVM) সেশনটি উপরের রিডাইরেকশন পোর্টগুলোতে (16994 বা 16995) বা প্রচলিত RFB (VNC সার্ভার) পোর্ট - 5900 এর উপরে চলতে পারে। নেটওয়ার্কে প্রেরিত তথ্যের ধরনের মধ্যে রয়েছে Intel AMT কমান্ড এবং প্রতিক্রিয়া বার্তা, রিডাইরেকশন ট্র্যাফিক এবং সিস্টেম সতর্কতা। 16993 ও 16995 পোর্টগুলোতে প্রেরিত ডেটা ট্রান্সপোর্ট-লেয়ার সিকিউরিটি (TLS) দ্বারা সুরক্ষিত হয় যদি সেই বিকল্পটি ব্যবহারকারীর সিস্টেমে সক্রিয় থাকে।

Intel AMT কোনো আইপিভি 4 বা IPV6 নেটওয়ার্কে ডেটা প্রেরণ করতে পারে এবং RFC 3041 গোপনীয়তা এক্সটেনশনগুলোর সাথে সামঞ্জস্যপূর্ণ।

Intel® Active Management Technology (Intel® AMT) নেটওয়ার্কে কী শনাক্তযোগ্য তথ্য প্রকাশ করে?

Intel® AMT সক্রিয় থাকাকালীন, ওপেন পোর্টগুলো এমন তথ্য উপস্থাপন করবে যা নেটওয়ার্কের অন্যদের কাছে কম্পিউটারটি শনাক্ত করতে ব্যবহার করা হতে পারে। এর মধ্যে রয়েছে HTTPS সার্টিফিকেট, HTTP ডাইজেস্ট রেলম, Intel AMT সংস্করণ এবং অন্যান্য তথ্য যা কম্পিউটারে ফিঙ্গারপ্রিন্ট করতে ব্যবহার করা যেতে পারে। Intel® AMT সমর্থিত প্রোটোকলগুলোর স্বাভাবিক ক্রিয়াকলাপের অংশ হিসাবে এই তথ্য দেওয়া হয়েছে। একটি অপারেটিং সিস্টেম ফায়ারওয়াল Intel® AMT পোর্টগুলোতে অ্যাক্সেস ব্লক করবে না, তবে অ্যাডমিনিস্ট্রেটররা Intel® AMT স্থানীয় পোর্টগুলো বন্ধ করতে এবং এই তথ্যে অ্যাক্সেস সীমাবদ্ধ করতে এনভায়রনমেন্ট ডিটেকশন এবং ফাস্ট কল ফর হেল্প (CIRA) ব্যবহার করতে পারেন।

Intel AMT একজন প্রমাণিত আইটি অ্যাডমিনিস্ট্রেটরকে কী করার অনুমতি দেয়?

- সমস্যা সমাধান ও মেরামতের জন্য সিস্টেমটি দূর থেকে চালু, পাওয়ার বন্ধ এবং রিবুট করা।
- হোস্ট OS বন্ধ বা ক্ষতিগ্রস্থ হওয়ার পরেও সিস্টেমটি দূর থেকে সমস্যার সমাধান করা।
- দূর থেকে সিস্টেমে BIOS কনফিগারেশন সেটিংস পর্যালোচনা ও পরিবর্তন করা। Intel AMT-তে কোনো আইটি অ্যাডমিনিস্ট্রেটরকে BIOS-এর পাসওয়ার্ডটি বাইপাস করার অনুমতি দেওয়ার বিকল্প রয়েছে, তবে সকল OEM এই বৈশিষ্ট্যটি প্রয়োগ করে না।

- সিস্টেমটি সুরক্ষিত করতে নেটওয়ার্ক ট্র্যাফিক ফিল্টারগুলো কনফিগার করা।
- সিস্টেমে সঞ্চালনের জন্য নিবন্ধিত অ্যাপ্লিকেশনগুলো নিরীক্ষণ করা (উদাহরণস্বরূপ, অ্যান্টিভাইরাস সফটওয়্যার চলছে কি না)।
- ব্যবহারকারীর সিস্টেমে Intel AMT ফার্মওয়্যার রিপোর্টিং ইভেন্টগুলো দ্বারা উৎপন্ন সতর্কতাগুলো পান যা প্রযুক্তিগত সহায়তার প্রয়োজন হতে পারে, যেমন: CPU হিট আপ, ফ্যানে ত্রুটি বা সিস্টেম প্রতিরক্ষা ফিল্টার ট্রিপিং। আরও উদাহরণ প্রকাশ্যে পাওয়া যায় www.intel.com/software/manageability।
- বুট প্রক্রিয়াটিকে একটি ফ্লপি ডিস্ক, সিডি-রম বা আইটি অ্যাডমিনিস্ট্রেটরের সিস্টেমে অবস্থিত কোনো চিত্রে পুনঃনির্দেশ করে ব্যবহারকারীর সিস্টেমের দূরবর্তী সমস্যার সমাধান করা।
- ব্যবহারকারীর সিস্টেমে কীবোর্ড ইনপুট এবং পাঠ্য-মোড ভিডিও আউটপুটকে আইটি অ্যাডমিনিস্ট্রেটরের সিস্টেমে পুনঃনির্দেশ করে সিস্টেমটি দূরবর্তীভাবে সমস্যার সমাধান করা।
- ব্যবহারকারীর সিস্টেম এবং আইটি অ্যাডমিনিস্ট্রেটরের সিস্টেম (KVM পুনঃনির্দেশ) থেকে কীবোর্ড, ভিডিও এবং মাউস পুনঃনির্দেশ করে সিস্টেমের দূরবর্তী সমস্যার সমাধান করা।
- কোন নেটওয়ার্ক পরিবেশে কনফিগার করা Intel AMT পরিচালনাযোগ্যতা কার্যকারিতা অ্যাক্সেসযোগ্য হবে (উদাহরণস্বরূপ, বিশ্বস্ত ডোমেনগুলো সংজ্ঞায়িত করে)।
- ফ্ল্যাশ রিপোজিটরিতে ডেটা লিখতে/মুছতে একটি নিবন্ধিত ISV অ্যাপ্লিকেশন ব্যবহার করা (যেমন, 3PDS অঞ্চল)
- নন-ভোলাটাইল মেমরিতে (NVM) ওয়েব অ্যাপ্লিকেশনগুলো হোস্ট করা যা Intel AMT ক্লায়েন্ট প্ল্যাটফর্মে স্থানীয়ভাবে পরিচালনা করে (Intel AMT 11.6 ও নতুন)।
- একটি UUID-এর মাধ্যমে এন্টারপ্রাইজ নেটওয়ার্কে ব্যবহারকারীর সিস্টেম শনাক্ত করা।
- Intel AMT আনপ্রভিশন করা এবং ফ্ল্যাশ সামগ্রী মুছে ফেলা।
- পূর্বনির্ধারিত ক্লায়েন্ট-ইনিশিয়েটেড-রিমোট-অ্যাক্সেস (CIRA) প্রোফাইলগুলো ব্যবহার করে এন্টারপ্রাইজ নেটওয়ার্কের বাইরেও রিমোটলি সিস্টেমগুলোর সাথে সংযোগ করা।

Intel AMT কি কোনো ব্যবহারকারীর স্থানীয় হার্ড ড্রাইভ (গুলো) অ্যাক্সেস করার জন্য একটি প্রমাণিত আইটি অ্যাডমিনিস্ট্রেটরকে অনুমতি দেয়?

একটি দূরবর্তী ব্যবস্থাপনা সেশনের সময়, আইটি অ্যাডমিনিস্ট্রেটরের ব্যবহারকারীর স্থানীয় হার্ড ড্রাইভগুলোতে অ্যাক্সেস থাকে। এর অর্থ হলো আইটি অ্যাডমিনিস্ট্রেটর ব্যবহারকারীর হার্ড ডিস্ক থেকে ফাইলগুলো পড়তে/লিখতে পারেন, উদাহরণস্বরূপ, ত্রুটিযুক্ত অ্যাপ্লিকেশন বা OS পুনরুদ্ধার বা পুনরায় ইনস্টল করে ব্যবহারকারীর সিস্টেমটি মেরামত করতে। Intel AMT দুইটি বৈশিষ্ট্য সমর্থন করে যা আইটি অ্যাডমিনিস্ট্রেটরদের এই ধরনের তথ্যে অ্যাক্সেস সরবরাহ করে উত্থাপিত সম্ভাব্য গোপনীয়তা ঝুঁকি হ্রাস করতে সহায়তা করে: IMSS ও অডিট লগিং। অডিট লগিং ক্ষমতাগুলো Intel AMT-এর মাধ্যমে ব্যবহারকারী সিস্টেমগুলোতে আইটি অ্যাডমিনিস্ট্রেটরের অ্যাক্সেসের উদাহরণগুলো লগ করে অ্যাডমিনিস্ট্রেটরের জবাবদিহিতার একটি স্তর প্রদান করে। যাইহোক, কোন ইভেন্টগুলো আসলে লগ করা হয় তা নিরীক্ষক দ্বারা সংজ্ঞায়িত করা হয়, যা এন্টারপ্রাইজে

সাধারণত হয় না। যদিও Intel তার গ্রাহকদের পরামর্শ দেয় যে Intel AMT সিস্টেমে রিমোট অ্যাক্সেস হলো এমন ধরনের তথ্য যা লগ করা উচিত, এটি সম্ভব যে এই তথ্যটি কিছু এন্টারপ্রাইজ পরিবেশে ব্যবহারকারীদের কাছে উপলভ্য হবে না। আইটি অ্যাডমিনিস্ট্রেটররা কিভাবে তাদের সিস্টেমে অ্যাক্সেস করেছেন এমন উদাহরণগুলোর বিজ্ঞপ্তিগুলো কিভাবে IMSS ব্যবহারকারীদের সরবরাহ করতে পারে তা সম্পর্কিত তথ্য অবিলম্বে নীচে প্রদান করা হয়েছে।

Intel AMT KVM রিডাইরেকশন কি কোনো প্রমাণিত আইটি অ্যাডমিনিস্ট্রেটরকে কোনো ব্যবহারকারীর পিসির রিমোট কন্ট্রোল নেওয়ার অনুমতি দেয় যেন তারা শারীরিকভাবে তাদের কীবোর্ডে বসে আছেন?

KVM রিডাইরেকশনসহ একটি দূরবর্তী ব্যবস্থাপনা সেশনের সময়, আইটি অ্যাডমিনিস্ট্রেটরের ব্যবহারকারীর পিসির নিয়ন্ত্রণ থাকে যেন তারা তাদের কীবোর্ডে বসে আছেন। KVM রিডাইরেকশন সেশনের ক্ষেত্রে, Intel AMT ব্যবহারকারীর স্পষ্ট সম্মতি ব্যতীত একটি KVM সেশন শুরু করা যাবে না, যা KVM ব্যবহারকারীর সম্মতি হিসাবে পরিচিত। রিডাইরেকশন সেশনে অপ্ট-ইন করার জন্য ব্যবহারকারীর সম্মতি প্রয়োগ করার জন্য, অন্য কোনো উইন্ডোর উপরে ব্যবহারকারীর স্ক্রিনে একটি সুরক্ষিত আউটপুট উইন্ডো ("স্প্রাইট") প্রদর্শিত হয়, যেখানে ব্যবহারকারীকে এলোমেলোভাবে উৎপন্ন নম্বরটি আইটি অ্যাডমিনিস্ট্রেটরের কাছে পড়তে বলা হয়। শুধুমাত্র যদি আইটি অ্যাডমিনিস্ট্রেটর সঠিক সেশন নম্বরে টাইপ করেন তবেই KVM সেশন শুরু হবে। একবার একটি বৈধ KVM সেশন আহ্বান করা হলে, ব্যবহারকারীর পুরো স্ক্রিনটি একটি ফ্ল্যাশিং লাল ও হলুদ সীমানা দ্বারা বেষ্টিত হবে - যা ইঙ্গিত দেয় যে একজন আইটি অ্যাডমিনিস্ট্রেটর KVM সংস্কার সেশনের প্রক্রিয়ায় রয়েছেন। এই ঝলমলে লাল ও হলুদ সীমানা যতক্ষণ সেশনটি সক্রিয় থাকবে ততক্ষণ অব্যাহত থাকবে। মনে রাখবেন যে Intel AMT সিস্টেমটি ক্লায়েন্ট কন্ট্রোল মোডে থাকলে KVM ব্যবহারকারীর সম্মতি বাধ্যতামূলক তবে অ্যাডমিন কন্ট্রোল মোডে থাকাকালীন ঐচ্ছিক।

OEM এর সেটিংস অনুযায়ী, Intel AMT-তে SOL/IDER বা KVM বৈশিষ্ট্যগুলো BIOS বা Intel® Management Engine BIOS Extension (Intel® MEBX) এ সক্রিয় বা নিষ্ক্রিয় করা হয়। KVM অপ্ট-ইনের প্রয়োজনীয়তা BIOS সেটিংস বা Intel AMT কনফিগারেশন সেটিংসের মাধ্যমে আইটি অ্যাডমিনিস্ট্রেটর দ্বারা পরিবর্তিত হতে পারে। Intel তার গোপনীয়তা বজায় রাখার জন্য ব্যবহারকারীর সম্মতির বাধ্যবাধকতা ব্যবহার করার পরামর্শ দেয়।

কিভাবে ব্যবহারকারী বলতে পারেন যেকোনো আইটি অ্যাডমিনিস্ট্রেটর Intel AMT-এর মাধ্যমে সিস্টেমটি অ্যাক্সেস করেছেন কি না?

IMSS সিস্টেম ট্রে আইকনটি বেশ কয়েকটি ইভেন্টের জন্য ব্যবহারকারীর বিজ্ঞপ্তিগুলো সক্রিয় করে এবং সমর্থন করে, যার মধ্যে কোনো আইটি অ্যাডমিনিস্ট্রেটর রিমোট রিডাইরেকশন সেশন (যেমন, SOL/IDER) খোলার/বন্ধ করার মাধ্যমে তাদের সিস্টেমটি অ্যাক্সেস করছেন কিনা বা অ্যাক্সেস

করেছেন কিনা, পাশাপাশি কোনো আইটি অ্যাডমিনিস্ট্রেটর দ্বারা ব্যবহারকারীর সিস্টেম ডিফেন্স অ্যাক্টিভেশন এবং সিস্টেমের রিমোট বুট অ্যাক্সেস করা হয়েছে কিনা। এছাড়াও, একটি সক্রিয় রিমোট রিডাইরেকশন সেশনের সময় স্ক্রিনের উপরের ডানদিকে একটি ফ্ল্যাশিং আইকন উপস্থিত হবে। তবে, এন্টারপ্রাইজ সেটিংয়ে IMSS দ্বারা প্রকৃতপক্ষে সক্রিয় ইভেন্টগুলো ব্যবহারকারী নয়, একজন আইটি অ্যাডমিনিস্ট্রেটর দ্বারা সংজ্ঞায়িত করা হয়। যদিও Intel সুপারিশ করে যে Intel AMT সিস্টেম স্থাপনকারী সংস্থাগুলো এই অনুচ্ছেদে উল্লিখিত IMSS বিজ্ঞপ্তিগুলো সক্রিয় করে, তবুও এটি সম্ভব যে Intel AMT সিস্টেমের দূরবর্তী সংযোগ সম্পর্কিত তথ্য সকল ব্যবহারকারীর কাছে অপরিহার্যভাবে উপলভ্য নাও হতে পারে।

একজন ব্যবহারকারী কিভাবে সমস্ত Intel AMT কনফিগারেশন এবং ব্যক্তিগত ডেটা সাফ করতে পারেন?

Intel AMT একটি Intel AMT সিস্টেমকে আংশিক/সম্পূর্ণরূপে আনপ্রোভিশন করার জন্য BIOS-এর বিকল্প সরবরাহ করে। Intel চূড়ান্ত ব্যবহারকারীদের পুনরায় বিক্রয়/পুনর্ব্যবহারের আগে একটি সিস্টেম সম্পূর্ণরূপে আনপ্রভিশন করার পরামর্শ দেয় এবং আপনি যদি ব্যবহৃত Intel AMT সক্রিয় সিস্টেম ক্রয় করেন তবে Intel AMT সম্পূর্ণরূপে অপ্রস্তুত কি না তা যাচাই করার পরামর্শ দেয়।

গোপনীয়তা বিবৃতির আপডেটসমূহ

আমরা মাঝে মাঝে এই গোপনীয়তা বিবৃতি আপডেট করতে পারি। আমরা যখন তা করি, তখন আমরা গোপনীয়তা বিবৃতির শীর্ষে সর্বশেষ আপডেটের তারিখটি সংশোধন করব।

আরও তথ্যের জন্য

আপনার যদি কোনো প্রশ্ন থাকে বা এই গোপনীয়তা পরিপূরক সম্পর্কে আরও তথ্য চান তাহলে অনুগ্রহ করে এই ফর্মটি ব্যবহার করে আমাদের সাথে যোগাযোগ করুন।

গোপনীয়তা বিজ্ঞপ্তির লিঙ্ক

- Intel-এর গোপনীয়তা বিজ্ঞপ্তি
- প্রার্থীর বিজ্ঞপ্তি