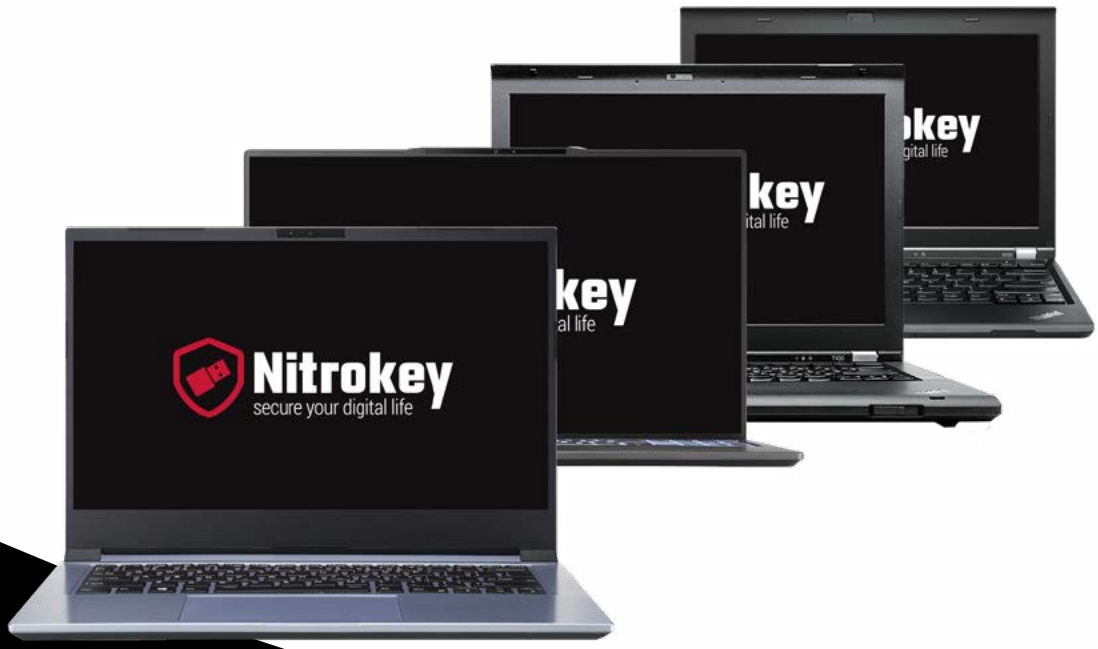


NitroPad

Sicheres Arbeiten in unsicheren Umgebungen dank einzigartigem Hardware-Schutz

Glauben Sie, dass Ihre Computerhardware sicher ist? Können Sie ausschließen, dass in Ihrer Abwesenheit niemand Ihren Computer manipuliert hat?

In einer Welt, in der die meisten Benutzer keine wirkliche Kontrolle über ihre Hardware haben und blind auf die Sicherheitsversprechen der Hersteller vertrauen müssen, ermöglicht NitroPad ein erfrischend neues Sicherheits-erlebnis. NitroPad ist deutlich sicherer als normale Computer. Mit NitroPad behalten Sie mehr als jemals zuvor die Kontrolle über Ihre Hardware und Daten, bei gleichzeitig einfacher Bedienbarkeit.

Nitrokey
secure your digital life

VORTEILE

Manipulationserkennung durch Measured Boot

Dank der Kombination aus den Open-Source-Lösungen Coreboot, Heads und Nitrokey USB-Hardware können Sie überprüfen, ob Ihr Laptop während des Transports oder in Ihrer Abwesenheit manipuliert wurde (sogenannte Evil Maid Attack). Dabei wird effektiv die Integrität des TPM, der Firmware und des Betriebssystems durch einen separaten Nitrokey USB-Schlüssel überprüft. Schließen Sie einfach während des Bootvorgangs Ihren Nitrokey an das NitroPad an und eine grüne LED des Nitrokeys zeigt an, dass Ihr NitroPad nicht manipuliert wurde. Sollte die LED jedoch einmal rot leuchten, weist dies auf eine Manipulation hin.

Deaktivierte Intel Management Engine

Verwundbare und proprietäre Low-Level-Hardwareteile werden deaktiviert, um die Hardware robuster gegen fortgeschrittene Angriffe zu machen.

Die Intel Management Engine (ME) ist eine Art separater Computer innerhalb aller modernen Intel Prozessoren (CPU). Die ME fungiert als Master-Controller für Ihre CPU und hat weitgehenden Zugriff auf Ihren Computer (Systemspeicher, Bildschirm, Tastatur, Netzwerk). Intel kontrolliert den Code der ME und es wurden bereits schwere Schwachstellen in der ME gefunden, die lokale und entfernte Angriffe ermöglichen. Daher kann ME als Hintertür betrachtet werden und ist im NitroPad deaktiviert.

Vorinstalliertes Ubuntu Linux mit Festplattenverschlüsselung

NitroPad wird mit einem vorinstallierten Ubuntu Linux LTS mit vollständiger Festplattenverschlüsselung ausgeliefert. Ubuntu ist eine der beliebtesten, stabilsten und am einfachsten zu bedienenden Linux-Distributionen. Der Umstieg von Windows auf Linux war noch nie so einfach.

Optional: Vorinstalliertes Qubes OS für höchste Sicherheitsanforderungen

Qubes certified*

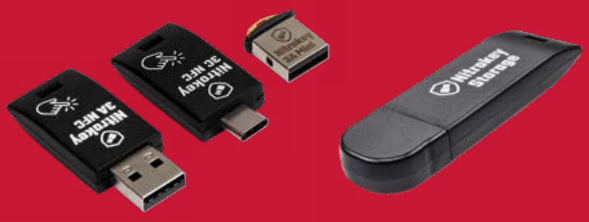
Anstelle von Ubuntu Linux erhalten Sie auf Wunsch Ihren NitroPad mit vorinstalliertem Qubes OS und vollständiger Festplattenverschlüsselung.

Qubes OS ermöglicht stark abgeschottetes Arbeiten mittels virtueller Maschinen (VM). Für jede Anwendung bzw. jeden Arbeitsbereich wird eine eigene VM gestartet. Dieser Ansatz isoliert Anwendungen und Prozesse wesentlich stärker als herkömmliche Betriebssysteme. Qubes OS hält Ihr System sicher, auch wenn eine Schwachstelle in einer der verwendeten Software ausgenutzt wurde. Beispiel: Wenn Ihr PDF-Anzeigeprogramm oder Webbrowser erfolgreich angegriffen wurde, kann der Angreifer den Rest des Systems nicht kompromittieren und wird ausgesperrt, sobald die VM geschlossen wird.

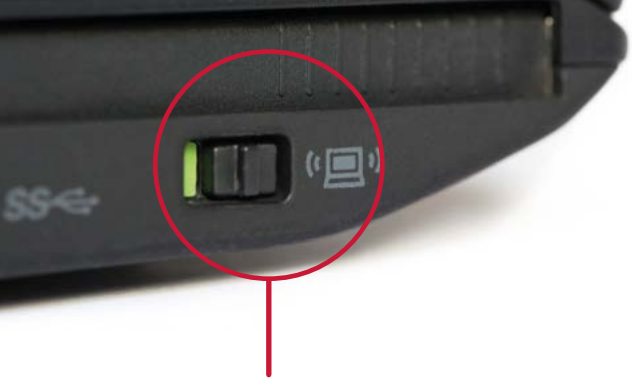
Zudem können getrennte virtuelle Arbeitsumgebungen verwendet werden, z.B. eine Offline-Arbeitsumgebung für vertrauliche Daten und eine Online-Arbeitsumgebung zur Kommunikation. NitroPad mit Qubes OS ist technisch ähnlich wie SINA Clients (für Behörden), bleibt dabei aber transparent dank Open Source. Qubes OS ist für Benutzer, die maximale Sicherheit wünschen.

*Für ausgewählte Modelle

Inklusive Nitrokey USB-Schlüssel



Das NitroPad wird mit einem Nitrokey ausgeliefert. Die Sicherheitsfunktionen des Nitrokey 3 umfassen Passkeys zum passwortlosen Login, Zwei-Faktor-Authentifizierung mittels FIDO2 und Einmalpasswörtern (OTP), E-Mail-Verschlüsselung (PGP, S/MIME), sichere Server-Administration (SSH). Der Nitrokey Storage 2 enthält einen verschlüsselten Massenspeicher mit versteckten Volumen.



Air Gap (nur X230, T430)

Flugmodus-Schalter ermöglicht Air Gap.

Schlüssel unter Ihrer Kontrolle

Alle individuellen kryptografischen Schlüssel werden ausschließlich während der Installation direkt auf dem NitroPad generiert und nicht von uns gespeichert. Trotzdem können alle individuellen Schlüssel von Ihnen ersetzt werden. Anders als bei „Secure Boot“ bleiben die Schlüssel zur Absicherung des Betriebssystems unter Ihrer Kontrolle und hängen nicht von der Zustimmung des Herstellers ab.

Sicherheitsbewusster Versand

Um das Abfangen und Manipulieren Ihres NitroPads zu erschweren, werden das NitroPad und der Nitrokey USB-Schlüssel auf Wunsch in zwei separaten Lieferungen verschickt.

Sofort startklar

Mit NitroPad müssen Sie sich nicht darum kümmern, das Gehäuse zu öffnen um den BIOS-Chip zu flashen, Linux zu installieren und zu konfigurieren oder den Nitrokey einzurichten.
Wir erledigen das für Sie. Der Nitrokey ist bereits mit Ihrem NitroPad konfiguriert, so dass er ohne weiteren Konfigurationsaufwand zur Manipulationserkennung verwendet werden kann.

Professionelle ThinkPad-Hardware (nur X230, T430, T480)

Basierend auf Lenovo ThinkPad erfüllt die Hardware-Verarbeitung und -Robustheit professionelle Qualitäts-Ansprüche. Die berühmte ThinkPad-Tastatur mit Hintergrund-Beleuchtung (optional) und TrackPoint erlaubt komfortables Arbeiten. Die gebrauchten Laptops wurden generalüberholt.

ANWENDUNGSFÄLLE

Für jeden

Mit dem NitroPad können Sie Manipulationen an der Hardware erkennen. Wird Ihr Laptop beispielsweise beim Grenzübertritt kontrolliert oder lassen Sie Ihr Gerät unbeaufsichtigt im Hotel oder während Reisen, können Sie die Integrität Ihres NitroPads mit Hilfe des Nitrokeys überprüfen.

Für Behörden

Behörden können sich mit dem NitroPad vor Advanced Persistent Threats (APT) schützen, ohne sich auf fremde proprietäre Technologien verlassen zu müssen.

Für Unternehmen

Das NitroPad kann als gehärteter Arbeitsplatz für Zertifizierungsstellen (Certificate Authorities) und andere Anwendungsfälle dienen, die Hochsicherheits-Rechner erfordern. Auf Geschäftsreisen schützt das NitroPad vor Evil-Maid-Angriffen während der Computer unbeaufsichtigt im Hotel oder im Reisegepäck ist.

Für Journalisten

Wenn Sie es als investigativer Journalist mit dem Schutz Ihrer vertraulichen Quellen ernst meinen, hilft Ihnen NitroPad dabei.

NITROKEY IST BESSER

Besser als gewöhnliche Laptops

Im Gegensatz zu herkömmlichen Laptops sind NitroPads mit Manipulationserkennung und deaktivierter Intel Management Engine ausgestattet. Dies macht das Gerät wesentlich widerstandsfähiger gegen fortgeschrittene Angriffe.
Die Hardware-Verarbeitung und -Robustheit erfüllt professionelle Qualitäts-Ansprüche.

Besser als gewöhnliche Betriebssysteme

Anders als Windows, macOS und die meisten Linux-Standardinstallationen, ist NitroPad wahlweise mit einem gehärteten Linux oder dem hochsicheren Qubes OS vorinstalliert.

Besser als Secure Boot

Anders als bei „Secure Boot" bleiben bei Measured Boot die Schlüssel zur Absicherung des Betriebssystems unter Ihrer Kontrolle und hängen nicht von der Zustimmung des Herstellers ab.

Sicherheit erfordert Open Source

Die Firmware (BIOS/UEFI), das Betriebssystem und der Nitrokey USB-Stick sind Open Source und freie Software, was unabhängige Sicherheitsaudits ermöglicht. Flexibel anpassbar, keine Herstellerabhängigkeit, keine Schein-Sicherheit durch Verschleierung, keine versteckten Sicherheitslücken und Hintertüren.

Made in Germany

Nitrokeys und NitroPads werden in Deutschland hergestellt. Zugunsten höherer Qualität und Sicherheit verzichten wir auf eine billige Produktion im Ausland.

Nachhaltigkeit

Das Aufarbeiten von gebrauchten ThinkPads zu NitroPads trägt zu einer nachhaltigen Umwelt und Gesellschaft bei. Bei Defekt lässt sich NitroPad einfach reparieren.

www.nitrokey.com

Unsere Kunden

Stand: 07/2025