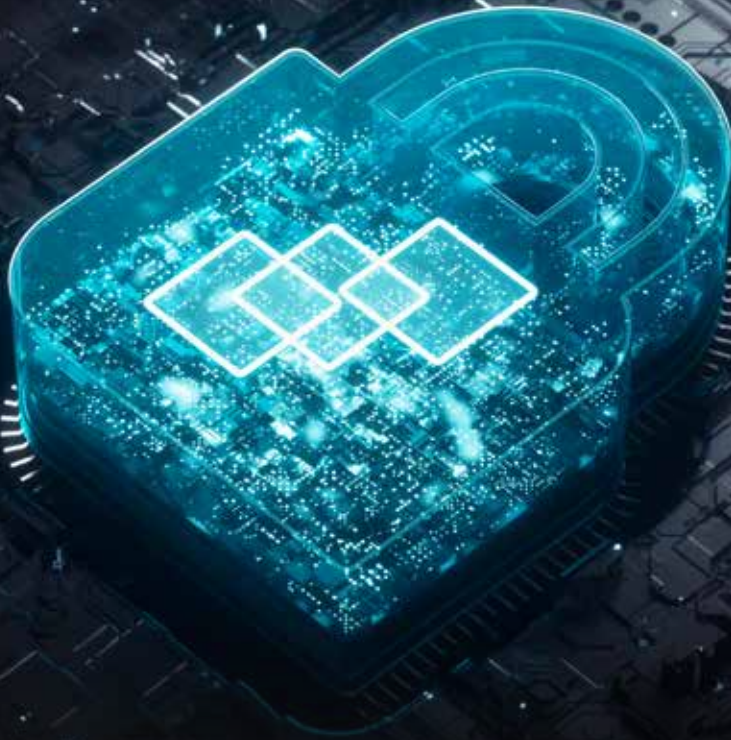


DIE WELTWEIT
**SICHERSTEN UND
LEISTUNGSSTÄRKSTEN
WORKSTATIONS¹**



EIN UMFASSENDE LEITFADEN ZU SICHERHEIT MIT Z BY HP



DIE WAHL EINER WORKSTATION IST EINE ENTSCHEIDUNG FÜR SICHERHEIT

Die weltweiten Investitionen in Cybersicherheit werden sich bis 2023 auf schätzungsweise 5,2 Billionen US-Dollar belaufen², da die Bedrohungen für die Informationssicherheit in ihrer Häufigkeit, Vielfalt und Reichweite weiter zunehmen.

Hardware-gestützte Sicherheit in jedem Gerät ist für den Gesamtschutz ihres Unternehmens von entscheidender Bedeutung. Unsere Z Workstations sind auf Widerstandsfähigkeit ausgerichtet und verfügen über selbstüberwachende und selbstheilende Sicherheitsfunktionen. Maßnahmen zum Schutz der Geräte und sensiblen Daten Ihres Unternehmens sind unterhalb, im und oberhalb des Betriebssystems eingebettet.

**ALLE
4 SEKUNDEN**
TAUCHT EINE NEUE ART
VON MALWARE AUF³

**5,2 MILLIARDEN
US-DOLLAR**
GESCHÄTZTE WELTWEITE
CYBERSICHERHEITSKOSTEN
BIS 2023²

4X TÖDLICHER
ZERO-DAY-ANGRIFFE SIND FÜR UNTERNEHMEN GEFÄHRLICHER⁶

**FANGEN SIE ZERO-DAY-
ANGRIFFE AB,
BEVOR SIE AUFTRETEN**

Tagtäglich werden mehr als 350.000 neue Malware-Varianten entwickelt. Damit Sie und Ihre Geräthenutzer sicher sind, statten wir unsere Z Workstations und Laptops mit zahlreichen Sicherheitsfunktionen aus, darunter HP Sure Sense, ein urheberrechtlich geschützter Deep-Learning-Algorithmus und eine hoch entwickelte neuronale Netzwerktechnologie zur Erkennung von Malware und zum Schutz vor neuartigen Angriffen.

**12 % ANSTIEG
DER KOSTEN FÜR
SICHERHEITS-
VERLETZUNGEN**
IM JAHRESVERGLEICH⁴

ÜBER 350.000
NEUE MALWARE-VARIANTEN
PRO TAG⁵

KI
WIRD ZUNEHMEND VON
HACKERN GENUTZT⁷



SCHÜTZEN SIE SENSIBLE DATEN UND GEISTIGES EIGENTUM MIT HARDWARE-GESTÜTZTER SICHERHEIT

Eine Sicherheitsverletzung kostet durchschnittlich 3,6 Millionen US-Dollar.⁸ Jedes Jahr steigen die Kosten von Datenschutzverletzungen, und in einem nicht enden wollenden Wettrüsten steigen die Ausgaben für Sicherheit parallel dazu.

Der Wert der Sicherheit übersteigt den Preis bei weitem und umfasst den Schutz der sensiblen Daten Ihres Unternehmens, ihrer Reputation und – was vielleicht am wichtigsten ist – den Schutz Ihres wertvollen geistigen Eigentums. Unsere unübertroffenen Hardware-gestützten Steuerungen umfassen:

HP ENDPOINT SECURITY CONTROLLER

HP Security Endpoint Controller ist die Hardware-Komponente, auf der die Sicherheitsarchitektur von Z by HP PCs basiert. Die getrennte, kryptografisch geschützte Hardware schafft die Basis des Vertrauens und ermöglicht Hardware-gestützte, selbstheilende und verwaltbare Sicherheitslösungen wie HP Sure Start, HP Sure Run und HP Sure Recover.

150 US-DOLLAR

DURCHSCHNITTS-
KOSTEN FÜR EINEN
GESTOHNENEN
DATENSATZ¹²

HP SURE START GEN6

HP Sure Start ist das weltweit erste selbstheilende BIOS.⁹ Es überprüft fortlaufend das System-BIOS und heilt sich automatisch selbst, wenn das BIOS durch Malware, Rootkits oder Angriffe beschädigt wurde. Darüber hinaus stellt es den BIOS-Code aus einer geschützten „Gold-Kopie“ wieder her.

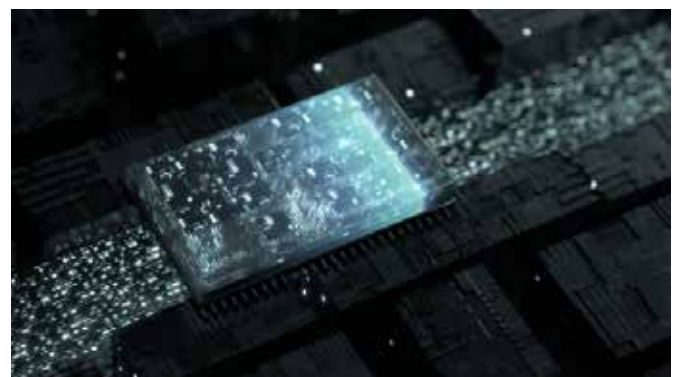
HP Sure Start stellt sicher, dass nur der vertrauenswürdige BIOS-Code ausgeführt wird und somit Ihren PC oder Ihre Workstation auf der grundlegendsten Ebene schützt. Zudem bietet Sure Start Gen6 Echtzeit-Überwachung der „Root of Trust“ der Hardware und DMA-Schutz vor dem Systemstart.

HP SURE RUN GEN3

HP Sure Run Gen3¹⁰ hält Ihre Geräteflotte davon ab, sich gegenseitig zu infizieren. Dazu werden sie in Ihrem Netzwerk isoliert. Schutzmaßnahmen stellen sicher, dass kritische Prozesse weiterhin ausgeführt werden, selbst wenn Malware versucht, sie zu deaktivieren. HP Sure Run wird durch den HP Endpoint Security Controller gestützt und überwacht wichtige Prozesse, warnt Benutzer und die IT vor Änderungen und startet sie automatisch neu, falls sie gestoppt werden. Dank Dynamic Persistence, Abtrennung des Netzwerks und Kill Prevention bringt Sure Run Ihre PCs so schnell wie möglich wieder zum Laufen.

HP SURE RECOVER GEN3

HP Sure Recover Gen3¹¹ ist in die Systemhardware und -firmware auf eine schnelle, sichere und automatisierte Art und Weise integriert, sodass Ihre Benutzer ihre Rechner schnell und sicher auf das neueste Betriebssystem-Image zurücksetzen können. Dazu benötigen sie nur eine Netzwerkverbindung bzw. bei bestimmten Modellen einen eingebetteten Flash-Chip. Damit kann Ihre IT-Abteilung sogar das Reimaging für die gesamte Flotte planen.



SICHERHEIT, DIE IHRE GESAMTE GERÄTEFLOTTE SCHÜTZT

Allein in der ersten Hälfte des Jahres 2019 gab es mehr als 3.800 Datenschutzverletzungen, ein Anstieg von 54 %¹³ gegenüber dem gleichen Zeitraum des Vorjahres. Da sich der Arbeitsplatz ständig weiterentwickelt, mobiles Arbeiten immer einfacher wird und Mitarbeiter auf mehrere Standorte verteilt sind, steigt die Bedrohung.

Angriffe vollständig zu stoppen ist schwierig, die intelligentesten IT-Teams regenerieren sich jedoch am schnellsten. Die Sicherheitsprodukte von HP können Geräte ohne manuelles Eingreifen wiederherstellen, sodass Ihre IT-Abteilung die PC- und Workstation-Flotte in Ihrem Unternehmen einfach verwalten kann.

HP SURE CLICK

Web-Browser sind ein primärer Angriffsvektor für Malware und andere Online-Bedrohungen. HP Sure Click ist eine Hardware-gestützte Lösung für sicheres Browsen und schützt vor bösartigen Websites, Downloads und Anhängen. Die Lösung isoliert Web-Inhalte in einem CPU-gestützten mikrovirtuellen Rechner, wo Malware andere Registerkarten, Anwendungen oder das Betriebssystem nicht beeinträchtigen kann.¹⁴

HP SURE SENSE

Herkömmliche Antivirenprogramme können neue Angriffe nicht immer erkennen. HP Sure Sense macht sich die Leistung von Deep-Learning-KI zunutze und erkennt 99 % der neuartigen Angriffe. Sie werden unter Quarantäne gestellt, um Infektionen zu verhindern, bevor sie auftreten.¹⁵ Sure Sense arbeitet Hand in Hand mit Sure Click. Mithilfe eines leichten Agenten wird jede Datei, die auf Ihr Gerät gelangt, gescannt, um festzustellen, ob sie bösartig ist.

HP SURE VIEW

Selbst die beste Sicherheitssoftware kann visuelles Hacken nicht verhindern - d. h. unbefugte Benutzer, die vertrauliche Informationen auf einem unbewachten Bildschirm einsehen. HP Sure View aktiviert auf Knopfdruck einen integrierten Datenschuttschirm, der Daten nur für den direkt davor sitzenden Benutzer sichtbar macht.¹⁶

HP SECURE ERASE

Durch einfaches Löschen von der Festplatte sind Dateien nicht unwiederbringlich verloren. HP Secure Erase ist eine Funktion auf BIOS-Ebene, die sensible Daten von Festplatten und Solid-State-Laufwerken dauerhaft zerstört, so dass sie niemals wiederhergestellt oder beeinträchtigt werden können.¹⁷

HP PRO UND ENTERPRISE SECURITY

HP hat Sicherheitslösungen für kleine, mittlere und große Unternehmen entwickelt, um allen Kundenanforderungen gerecht zu werden. Dieses Sicherheitsportfolio beinhaltet die HP Pro Security Edition,¹⁹ HP Proactive Security²⁰ und HP Sure Click Enterprise.²¹ Der vielschichtige Ansatz, bei dem Schutz oberste Priorität hat, wird den besonderen Anforderungen größerer Unternehmen gerecht. Wir bieten modernste Schutzoptionen, u. a. Bedrohungsanalyse und -überwachung für Ihre gesamte Flotte. Diese Lösungen lassen sich einfach implementieren und haben eine vorkonfigurierte Verwaltbarkeit.

ZERTIFIZIERTE SELBSTVERSCHLÜSSELNDE FESTPLATTEN

Selbstverschlüsselnde Festplatten und Solid-State-Laufwerke verwenden hardwarebasierte Verschlüsselung, um ihren Inhalt auch dann zu schützen, wenn die Festplatte vom PC getrennt wurde. Dank des hardwarebasierten Datenverschlüsselungsverfahrens sind zudem keine oder nur minimale Auswirkungen auf die Leistung feststellbar.¹⁸



EINFACHE VERWALTUNG DER GESAMTEN IT-SICHERHEIT

HP integriert Sicherheit in die Z Workstations, um ein vollständiges, einfach zu verwaltendes Ökosystem zu schaffen. Dazu gehören auch der HP Endpoint Security Controller – das Herzstück der Sicherheitsinfrastruktur – sowie verschiedene Identitäts- und Management-Tools für einen nahtlosen täglichen Betrieb.

REMOTE-LÖSUNGEN:

HP ZCentral

HP ZCentral ist eine umfangreiche Hardware- und Softwarelösung aus einer Hand. Sie befähigt mobile Mitarbeiter und vereinfacht die Verwaltung und gemeinsame Nutzung zentralisierter Workstations durch mehrere Benutzer.

HP ZCentral Remote Boost²²

Eine Remote-Lösung aus einer Hand für eine vereinfachte Verwaltung und gemeinsame Nutzung von zentralisierten Workstations durch mehrere Benutzer. Weisen Sie Personen über eine Konsole und eine schlanke Benutzeroberfläche einfach eine Workstation zu, oder weisen Sie gemeinsamen Zugriff auf bestimmte Maschinen zu. Außerdem können Sie darauf vertrauen, dass die sensiblen Daten Ihres Unternehmens geschützt sind – wir übertragen nur verschlüsselte Pixel über das Netzwerk an Remote-Benutzer. Alle wichtigen Daten bleiben genau dort, wo sie hingehören – in Ihrem Datenschränk.

VERWALBARKEIT:

HP ZCentral Connect²³

ZCentral Connect ist eine vollständige Remote-Workstation-Lösung für eine vereinfachte Verwaltung und gemeinsame Nutzung von zentralisierten Workstations durch mehrere Benutzer. Weisen Sie Personen über eine Konsole und eine schlanke Benutzeroberfläche einfach eine Workstation zu oder weisen Sie Pools zu.

HP Manageability Integration Kit

Das HP Manageability Integration Kit (MIK) ist für die Einbindung in den Microsoft System Center Configuration Manager (SCCM) konzipiert und soll IT-Administratoren bei der Aktualisierung und Wartung von Software- und Sicherheitseinstellungen für die gesamte PC- und Workstation-Flotte unterstützen.²⁴

HP Image Assistant

HP Image Assistant unterstützt Ihre IT-Abteilung bei der Entwicklung und Wartung eines widerstandsfähigen Software-Image. Darüber hinaus stellt er sicher, dass Sie mit den neuesten Patches und Upgrades auf dem aktuellen Stand bleiben, und implementiert sie einheitlich auf allen Systemen in Ihrem Unternehmen.

IDENTITÄT:

HP Client Security Manager

HP Client Security Manager hilft Benutzern und IT-Fachleuten bei der Konfiguration und Steuerung einer Vielzahl von in HP PCs integrierten Sicherheitsfunktionen, u. a. HP Sure Run, SpareKey usw.



HP Multi-Factor Authenticate

HP Multi-Factor Authenticate hilft, Ihr Netzwerk und VPN vor unbefugtem Zugriff zu schützen, indem bis zu drei Authentifizierungsfaktoren für die Anmeldung gefordert werden – darunter ein optionales Fingerabdruck-Lesegerät und eine Kamera für die Infrarot-Gesichtserkennung. Dabei werden die Richtlinien auf Siliziumebene durchgesetzt.²⁵

HP SpareKey

Falls Benutzer ihr Windows-Passwort vergessen haben, kann HP SpareKey Passwörter zurücksetzen und den Zugriff auf gesperrte PCs wiederherstellen, ohne dass IT-Mitarbeiter eingreifen müssen. Dazu wird der Benutzer durch eine Reihe vorgegebener Sicherheitsfragen geführt.





IMMER EINEN SCHRITT VORAUSS MIT SICHERHEIT IN NEUE ARBEITSKONZEPTE

Die digitale Sicherheitslandschaft befindet sich im Wandel, vor allem da sich zahllose Mitarbeiter auf der ganzen Welt an eine neue vom mobilen Arbeiten geprägte Normalität gewöhnen. Da Fachleute im technischen und kreativen Bereich neue vernetzte Produkte und Dienstleistungen in ihr Leben integrieren, prüft HP Security Lab entstehende Sicherheitsgefahren ganzheitlich.

Dieses Lab ist Teil der berühmten HP Labs und soll HP darin unterstützen, die weltweit sichersten Workstations zu bauen. Seine Mitglieder sind führende Forscher, Ingenieure, White-Hat-Hacker und Sicherheitsexperten, die Erkenntnisse von der Front bereitstellen.

Durch eigene Forschung in der Systemsicherheit stellt HP Security Labs sicher, dass wir sichere und geprüfte Produkte, Dienstleistungen und Erfahrungen bereitstellen und der Branche damit stets das Tempo im Bereich der Cybersicherheit vorgeben.



QUELLANGABEN UND HAFTUNGSAUSSCHLÜSSE

1. Basierend auf den einzigartigen und umfassenden HP-Sicherheitsfunktionen ohne zusätzliche Kosten und der Verwaltung sämtlicher PC-Aspekte, u. a. Hardware, BIOS und Software, durch das Manageability Integration Kit von HP mithilfe des Microsoft System Center Configuration Manager auf HP Elite PCs und HP Workstations mit Windows und Intel® Prozessoren der 8. Generation und höher oder AMD Ryzen™ 4000 Prozessoren und höher.
2. https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50
3. AV-TEST, Security Report 2018/2019, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf
4. Ponemon, 2019, The cost of cybercrime, https://www.accenture.com/_acnmedia/pdf-96/accelenture-2019-cost-of-cybercrime-study-final.pdf
5. AV-TEST Institute
6. Ponemon, 2018, Endpoint Security Risk Report, <https://www.ponemon.org/news-2/82>
7. DataCenter Knowledge, Juni 2019, Why It's Time to Prepare for AI-Wielding Hackers, <https://www.datacenterknowledge.com/machine-learning/why-its-time-prepare-ai-wielding-hackers>
8. <https://newsroom.accenture.com/news/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture.htm>, Seite 16
9. HP Sure Start Gen6 ist auf ausgewählten HP PCs verfügbar.
10. HP Sure Run Gen3 ist auf ausgewählten HP Pro, Elite und Workstation PCs mit Windows 10 und ausgewählten Intel® oder AMD Prozessoren verfügbar.
11. HP Sure Recover Gen3 ist auf ausgewählten HP PCs verfügbar und erfordert eine offene Netzwerkverbindung. Sie müssen wichtige Dateien, Daten, Fotos und Videos etc. vor der Verwendung von HP Sure Recover sichern, um Datenverluste zu vermeiden.
12. IBM, 2019 Cost of a Data Breach Report, https://www.ibm.com/security/data-breach?cm_mc_uid=21400672026815717196148&cm_mc_sid_50200000=99136091571719614838 TechRepublic, August 2019, Data breaches increased 54% in 2019 so far, <https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/>
13. HP Sure Click erfordert Windows 10 Pro oder Enterprise und unterstützt Microsoft® Internet Explorer, Google Chrome und Chromium™. Unterstützte Anhänge umfassen Microsoft Office- (Word, Excel, PowerPoint) und PDF-Dateien im Lesemodus, wenn Microsoft Office oder Adobe Acrobat installiert ist.
14. HP Sure Sense erfordert Windows 10 Pro oder Enterprise. Verfügbarkeit siehe Produktspezifikationen.
15. HP Sure View ist auf ausgewählten mobilen Workstations verfügbar und auf Querformat ausgelegt. Konfiguration beim Kauf erforderlich.
16. HP Secure Erase entspricht den Methoden, die in der Sonderveröffentlichung 800-88 „Clear“ Sanitation Method des National Institute of Standards and Technology dargelegt sind.
17. Selbstverschlüsselnde Laufwerke sind auf ausgewählten HP PCs optional verfügbar.
18. HP Pro Security Edition ist bereits geladen auf ausgewählten HP PCs verfügbar und beinhaltet HP Sure Click Pro und HP Sure Sense Pro. 3-Jahres-Lizenz erforderlich.
20. HP Proactive Security ist separat erhältlich. Die Leistungen von HP unterliegen den geltenden Allgemeinen Geschäftsbedingungen von HP, die dem Kunden beim Kauf bereitgestellt oder angezeigt werden. Kunden haben womöglich weitere gesetzliche Rechte gemäß den geltenden lokalen Gesetzen, und diese Rechte werden durch die Allgemeinen Geschäftsbedingungen oder die mit Ihrem Produkt bereitgestellte beschränkte Garantie von HP in keiner Weise beeinträchtigt. Die vollständigen Systemanforderungen sind unter folgender Adresse nachzulesen: www.hpdaas.com/requirements.
21. HP Sure Click Enterprise erfordert Windows 8 oder 10, und Microsoft Internet Explorer, Google Chrome, Chromium oder Firefox werden unterstützt. Unterstützte Anhänge umfassen Microsoft Office- (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office oder Adobe Acrobat installiert ist.
22. HP ZCentral Remote Boost ist auf Z Workstations nicht vorinstalliert, kann jedoch ohne Erwerb einer Lizenz heruntergeladen und auf allen Z Desktop und Laptops ausgeführt werden. Für Nicht-Z-Sendergeräte ist der Erwerb einer unbefristeten Einzellizenz oder einer unbefristeten Floating-Lizenz pro gleichzeitig ausgeführter Version und der Erwerb von ZCentral Remote Boost Software Support erforderlich. RGS erfordert das Betriebssystem Windows, RHEL (7 oder 8), UBUNTU 18.04 LTS oder HP ThinPro 7. Das Betriebssystem MacOS (10.13 oder neuer) wird nur auf Empfängerseite unterstützt. Erfordert Netzwerkzugang. Die Software steht unter folgender Adresse zum Download bereit: hp.com/ZCentralRemoteBoost.
23. HP ZCentral Connect Software erfordert den Erwerb einer unbefristeten Floating-Lizenz pro gleichzeitig ausgeführter Verbindung und den Erwerb von ZCentral Connect Software Support Service für ein Jahr. Sie muss unter folgender Adresse heruntergeladen werden: hp.com/ZCentral. Erfordert HP ZCentral Remote Boost Software, die unter hp.com/ZCentralRemoteBoost heruntergeladen werden kann, das Betriebssystem Windows 10, Windows Server 2016 oder neuer, Microsoft Active Directory und Intel Active Management Technology für ausgewählte Funktionen.
24. HP Manageability Integration Kit kann unter folgender Adresse heruntergeladen werden: hp.com/go/clientmanagement.
25. HP Multi-Factor Authenticate Gen2 erfordert Windows, einen Intel Core™ Prozessor der 7. oder 8. Generation, integrierte Intel Grafikleistung und Intel WLAN. Microsoft System Center Configuration Manager ist für den Einsatz erforderlich. Die Drei-Faktor-Authentifizierung erfordert Intel vPro™.

© 2020 HP Development Company, L.P. Die hierin enthaltenen Informationen können ohne Vorankündigung geändert werden. Die einzigen Garantien für Produkte und Dienstleistungen von HP sind in den ausdrücklichen Garantieerklärungen zu diesen Produkten und Dienstleistungen dargelegt. Nichts hierin sollte als eine zusätzliche Garantie ausgelegt werden. HP haftet nicht für hierin enthaltene technische oder redaktionelle Fehler. Intel, das Intel-Logo, Core und Xeon sind Warenzeichen oder eingetragene Warenzeichen der Intel Corporation bzw. ihrer Tochtergesellschaften in den USA und anderen Ländern. Microsoft und Windows sind eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. NVIDIA und Quadro sind Warenzeichen oder eingetragene Warenzeichen der NVIDIA Corporation in den USA und anderen Ländern.

4AA7-7957ENW, Juli 2020

