

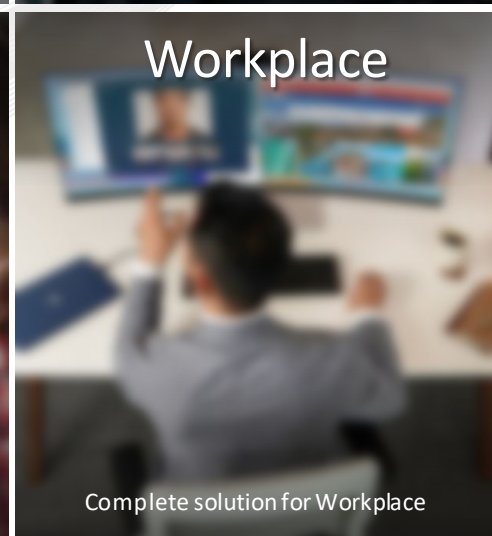
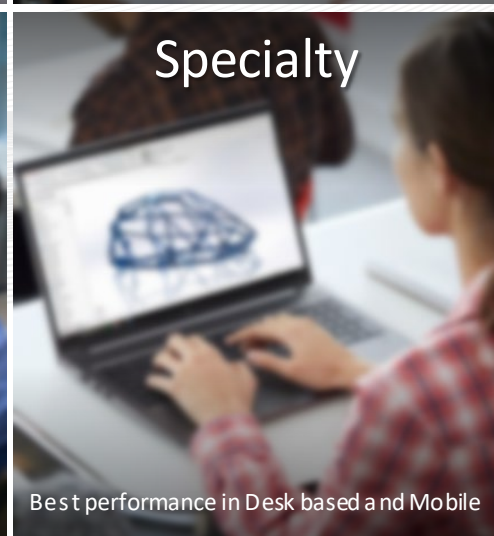
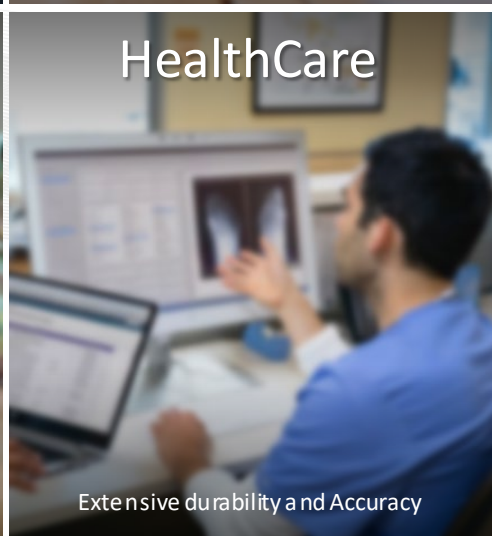
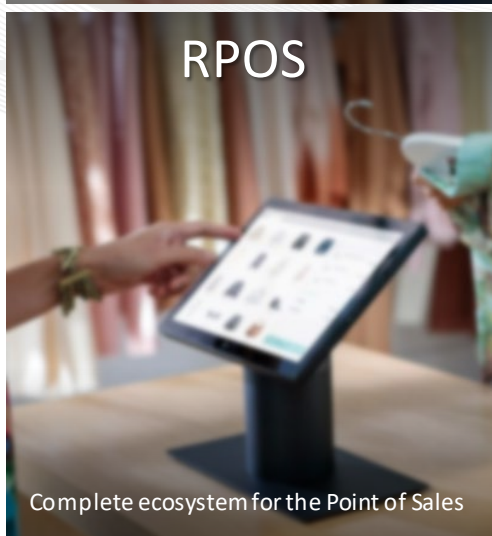
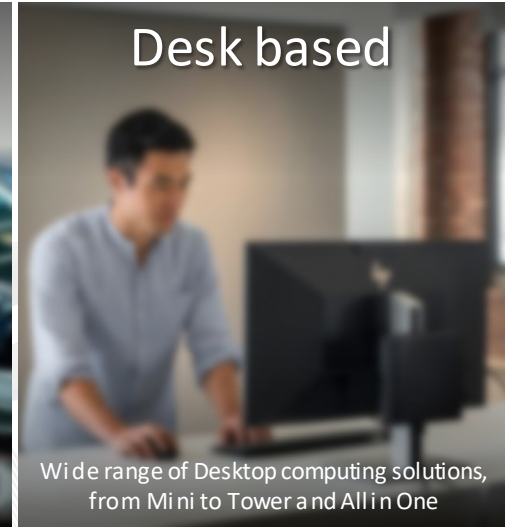
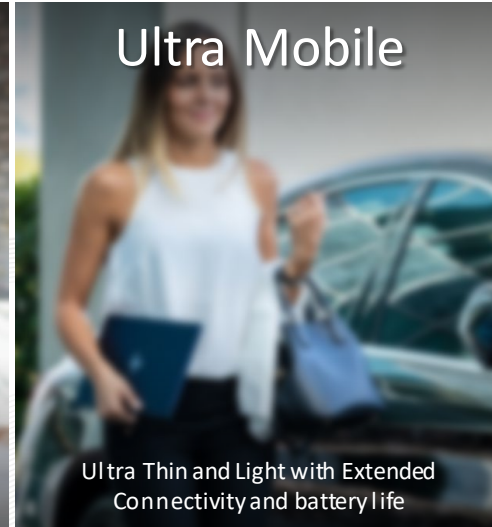
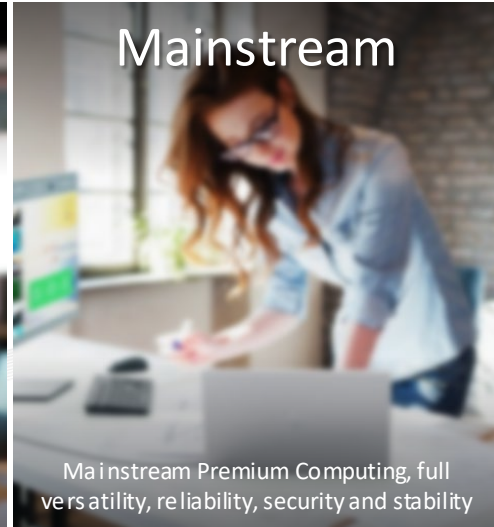
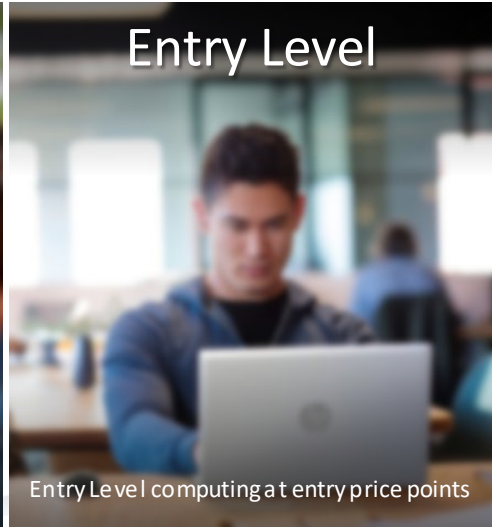
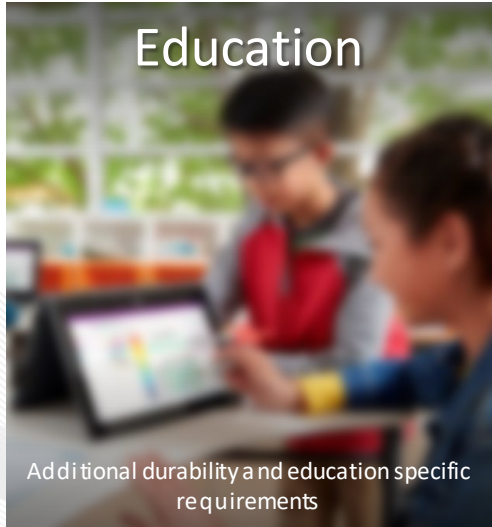
# CHANGE

## Bechtle IT-Forum 2021. HPI - Modern und sicher Arbeiten.

Silvio Defuns | HP Business Development Manager | ARP Schweiz AG  
Gilbert Benkert | Service Sales Consultant | HP Schweiz AG



# HP Commercial Computing Portfolio.



# The Reality Today.

**+75%**

of Fortune 500 CEOs  
say the pandemic  
will accelerate digital  
transformation<sup>4</sup>

**56%**

of IT Decision  
Makers will  
outsource more as a  
result of  
COVID-19<sup>2</sup>

**59%**

believe the buying  
model is shifting to  
IT as a Service  
because of  
COVID-19<sup>5</sup>

<sup>2</sup> HP Proprietary Research May 2020

<sup>4</sup> Fortune 500 2020 CEO Survey

<sup>5</sup> Remote work changing landscape, IT Leader View, May 2020

# HP Device as a Service.

Changed Definition to meet market's expectations.



---

Reduce the complexity of device lifecycle management with Device as a Service (DaaS), a solution that combines hardware, services and analytics into a predictable payment\*.

---

# Modern Management.

A workplace IT transformation where PC's are provisioned from the cloud, with zero or light touch, and security policies are automatically enforced



Un-box and log on  
off-the-shelf

instantly downloading  
needed apps, settings &  
policy

Device is ready for productive  
use

**Autopilot**



**Azure AD**



**Unified Endpoint  
Management (UEM)**

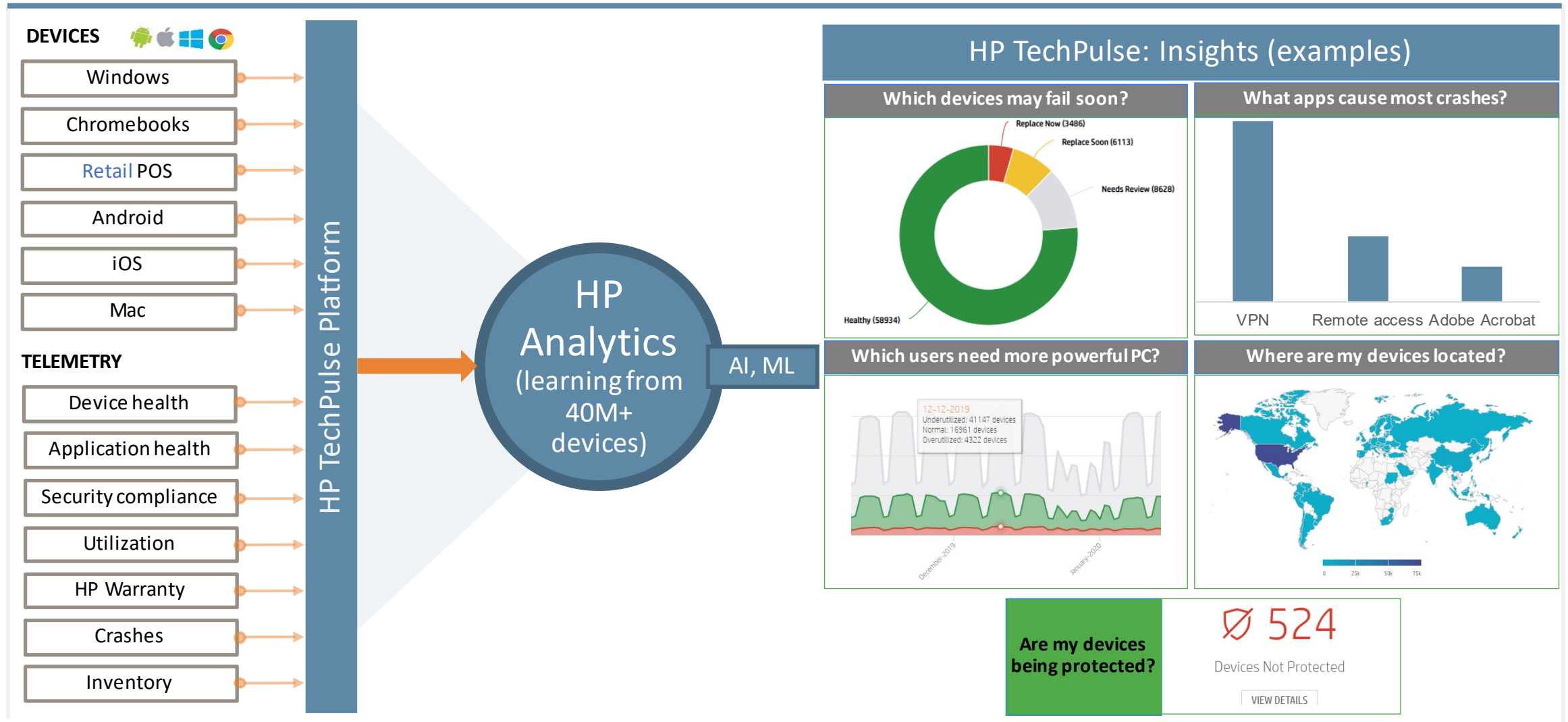


**Modern Management**

 **Microsoft  
Intune**

 **vmware**  
Workspace™ ONE™

# How it works – data collection and insights.







HP WOLF SECURITY

# HP Wolf Security

Gilber



Home > Security > Business-IT > Schweiz verzeichnet deutlich mehr Attacken auf Remote-Desktop-Verbindungen

Seit dem Umzug ins Homeoffice 23.09.2020, 10:32 Uhr

## Schweiz verzeichnet deutlich mehr Attacken auf Remote-Desktop-Verbindungen

Seit dem Corona-bedingten Umzug ins Homeoffice stieg in der Schweiz die Zahl der Hackerangriffe auf Remote-Desktop-Verbindungen massiv an. Das zeigt eine Untersuchung der IT-Sicherheitsexperten von Eset.



(Quelle: Christian Bouvier / Unsplash)

Während der Corona-bedingten Homeoffice-Zeit im Frühjahr sind die Hackerangriffe auf Fernverbindungen zu Firmensystemen sprunghaft angestiegen. Laut dem IT-Sicherheitshersteller Eset waren es in der Schweiz im Januar täglich rund 30'000 Angriffe – bis im Juni stieg der Höchstwert auf 220'000. Den Angreifern gehe es dabei sowohl um das Absaugen von Daten als auch um das Einschleusen von Schadsoftware. Dies teilte Eset am Mittwoch mit.



### Immer mehr Hackerangriffe auf KMU

Aus Schweiz aktuell vom 29.08.2019.

News > Schweiz >

### Vermehrte Cyber-Angriffe

## Schweizer Firmen im Visier von Hackern

Der Bund warnt nach wiederholten Hackerangriffen in den letzten Wochen vor allem KMU davor, die Gefahr zu unterschätzen.

Daniel Glaus  
Donnerstag, 29.08.2019, 22:10 Uhr



Dieser Artikel wurde 1-mal geteilt.

Diese Woche ein Busbetrieb und Fahrzeugausrüster, Ende Juli ein Gebäudetechnik-Unternehmen: Nur zwei Fälle von Schweizer Unternehmen, die in den letzten Monaten via Internet angegriffen und deren IT-Systeme massiv gestört wurde.

NEWS

Was IT-Security-Experten den Schlaf raubt

## US-Militär legt riesiges Botnetz Trickbot lahm - zumindest für einen Moment

Mo 12.10.2020 - 12:10 Uhr  
von Coen Kaat

Komisch, spannend und beängstigend. Jeden Tag kommen neue Meldungen zu DDoS-Attacken, Ransomware, Cryptominern und Co. Die Redaktion bloggt an dieser Stelle über alles rund um Cybercrime und IT-Security.



netzwoche NEWS STORYS DOSSIERS VIDEO SPECIAL

NEWS

Nachgefragt bei Nicolas Mayencourt

## Cybersecurity in Coronazeiten: Es braucht ein radikales Umdenken

Mo 11.05.2020 - 11:20 Uhr | Aktualisiert 11.05.2020 - 11:20  
von Joël Orizet

Cyberkriminelle beuten die Angst vor dem Coronavirus aus. Und die Angriffsfläche reicht bis ins Homeoffice. Nicolas Mayencourt, CEO und Gründer von Dreamlab Technologies, spricht darüber, wie die Coronakrise unseren Umgang mit IT-Sicherheit und Datenschutz verändert, wo die grössten Gefahren lauern und was dagegen zu tun ist.







## Today's Challenges.

---

Inadequate endpoint security

---

Limited resources dedicated to endpoint security

---

Advanced anti-malware solutions can be complex

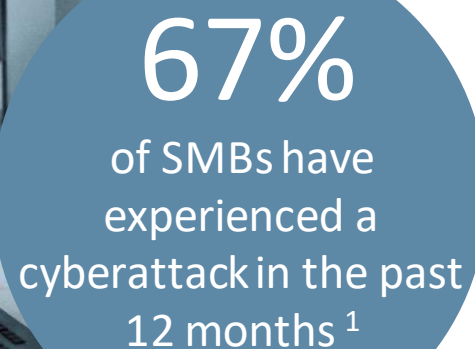
---

Many security solutions negatively impact employee productivity

---

Lack of visibility into details of attempted attacks

---



67%  
of SMBs have  
experienced a  
cyberattack in the past  
12 months <sup>1</sup>

1. Source: Ponemon Institute (2019 Global State of Cybersecurity in Small and Medium-Sized Businesses <1000 employees)



# Why current security approaches are inadequate.



Email is an enormous risk

**94%**

of infections originate from email attachments.

Source: 2019 Data Breach Investigations Report, Verizon



Anti-virus falls short

**60%**

of attacks are missed by anti-virus.

Source: Ponemon Institute 2020 State of Endpoint Security Report sponsored by Morphisec, January 2020



Zero-day threats

**4x**

more likely to compromise organizations.

Source: Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018



Lack of visibility

**96%**

of breaches aren't discovered until months afterwards.

Source: 2018 Data Breach Investigations report 11th Edition, Verizon, 2018;



Shortage of expertise

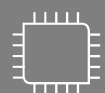
**53%**

reported a shortage of cyber security skills.

Source: ESG Global IT Survey 2018-2019  
<https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse>



# HP Security Solutions.



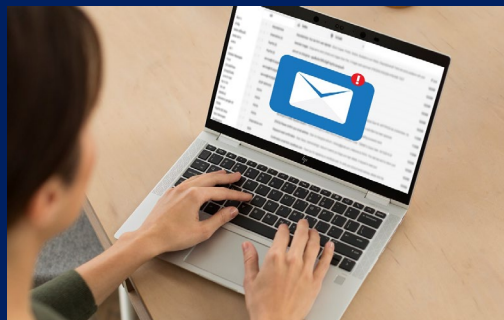
## HP PC Hardware *Sure Security Suite*



- HP Endpoint Security Controller
- HP Sure Start
- HP Sure Run
- HP Sure View
- HP Sure Recover
- HP Wolf Security for Business
- Multifactor authentication, biometrics



## HP Wolf Enterprise Security *former "Bromium" (SCE)*



### Threat isolation technology

- Isolate Office files in Secure Micro VM
- Give Malware no chance to infect your PC
- Work in isolated Browsers
- Isolate files from USB-Sticks

**Customer Self Managed**

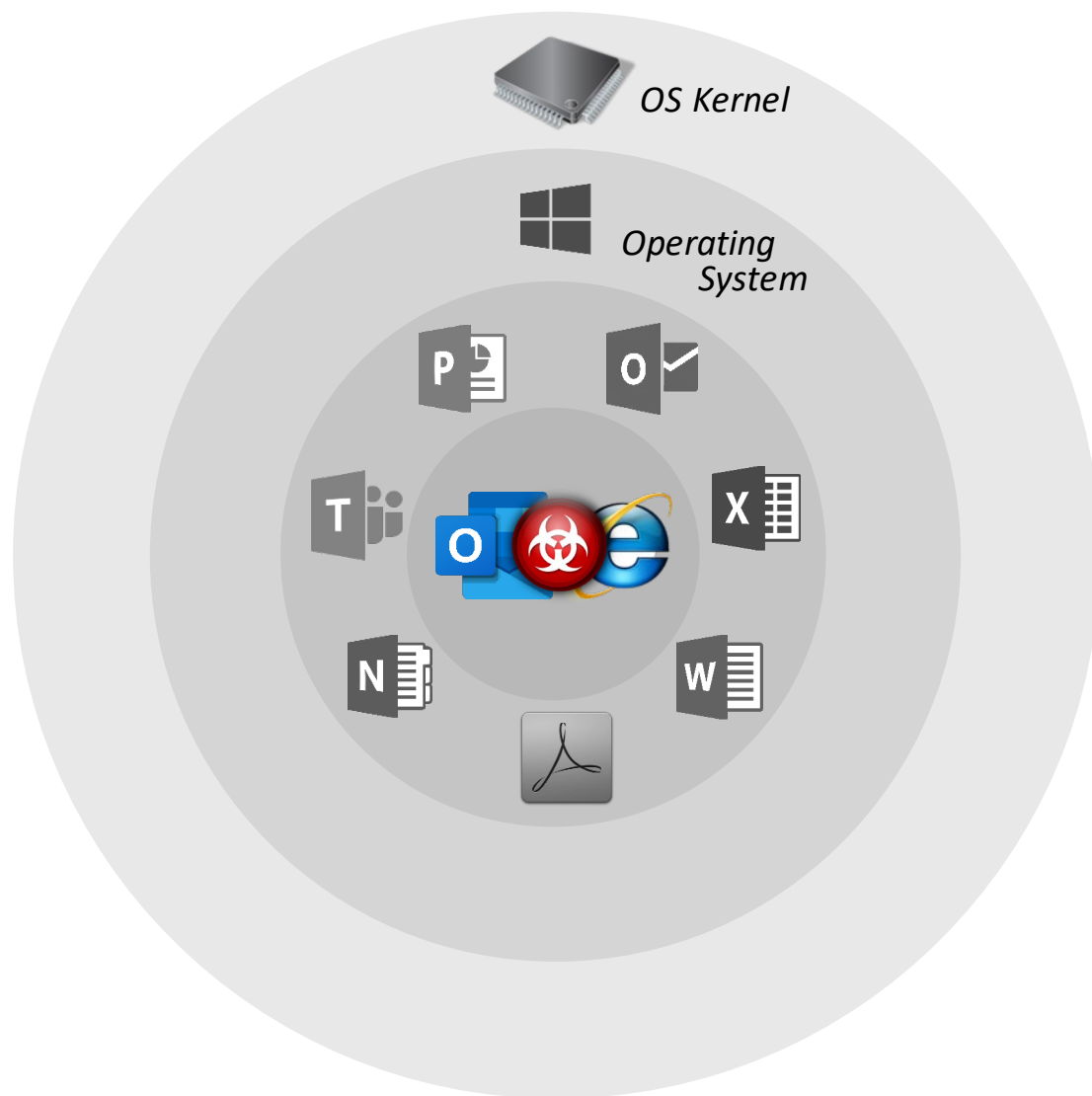


## HP Wolf Pro Security



- Sure Sense - Deep Learning/AI protection
- Threat Assessment
- Compliance reporting
- Device find / lock / wipe
- Patch policy management

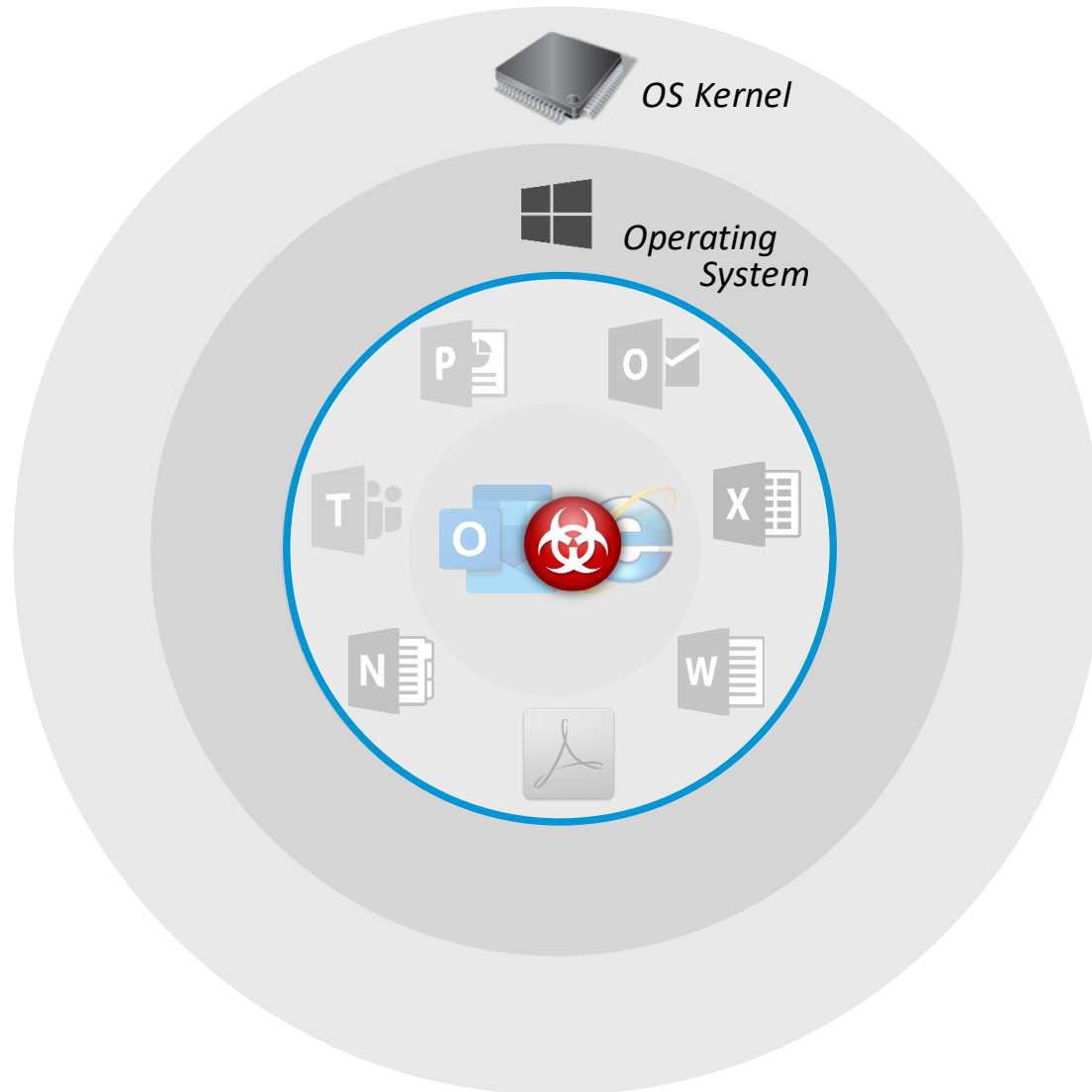
**HP / Partner Managed**



One click on a malicious file from a USB stick, email, URL-link can cause damage to your company



# HP Security Solutions.



One click on a malicious file from a USB stick, email, URL-link can cause damage to your company

Works in a virtual machine, isolated from the complete system

- No performance-impact
- Threats disappear once browser/mail/file is closed
- It get visibility thanks to a dashboard



Recycle Bin



Type here to search



10:13 PM  
4/13/2020







# HP Wolf Security.

## Malware dashboard.

Threat - HP Sure Controller

bec-hpdaas-na.gui.bromium-online.com/gui/threats/3611/

Sure Controller - HP North America Production DaaS

Dan Allen

Microsoft Word **Detection: Isolation 4.2.1.3242** **True Positive**

Threat UUID: 94889af1-2f7a-4701-8819-e93323ee0552

**SUMMARY** GRAPH FILES BEHAVIORAL NETWORK EMAIL INFO

SEVERITY **High** TOTAL EVENTS **5,958** HIGH SEVERITY EVENTS **1,117**

ALLEND7 AUTH\allend

Threat triggered for Microsoft Word because 17 different suspicious activities were detected. The triggering event was reported because of the 'loads a modified dll file' behavior. This event occurred after the micro-VM had been running for 9 seconds.

Initiated By: User Action  
Threat Response: Isolated

Detected: June 8, 2020 12:33 p.m.  
Received: June 8, 2020 12:34 p.m.  
Updated: June 8, 2020 12:34 p.m.

TOTAL DURATION  
00:02:25  
ATTACK DURATION  
00:02:16

Threat Indicators

Threat Intelligence Service Response

Win32.Ransomware.Crypt	1
Win32.Trojan.Wannacrypt	7
Win32.Trojan.Npe	17
Win32.Trojan.Ransomnote	9
Win32.Trojan.Filecoder	2
Win32.Trojan.Wanna	1
daniella_jones_cv	?

MITRE ATT&CK™

TA0001 - Initial Access	1
T1193 - Spearphishing Attachment	
TA0002 - Execution	2
T1106 - Execution through API	
T1129 - Execution through Module Load	
TA0003 - Persistence	3
T1060 - Registry Run Keys / Startup Folder	
T1037 - Logon Scripts	
T1137 - Office Application Startup	
TA0004 - Privilege Escalation	0
TA0005 - Defense Evasion	2
T1107 - File Deletion	

Capacity\_Run\_at\_Ra....xls

Show all

HP Confidential. For use by HP Internal Sales and Channel Partners under HP CDA for training purposes only  
©Copyright 2021 HP Development Company, L.P. The information contained herein is subject to change without notice.





# HP Wolf Security.

## Sophisticated Customer rely on HP Security.



Excellence in Government Security 2017



#### 4 InfoSec Awards 2018:

- Cutting Edge in the Anti-Phishing
- Best Product in the Application Security
- Hot Company in the Email Security Management
- Editor's Choice in the Endpoint Security



Bundesamt für Ausrüstung,  
Informationstechnik und  
Nutzung der Bundeswehr



POLIZEI  
Nordrhein-Westfalen



UNISYS



INTERPOL



Informations  
Technik  
Zentrum Bund



Bundesamt  
für Sicherheit in der  
Informationstechnik



HP Confidential. For use by HP Internal Sales and Channel Partners under HP CDA for training purposes only  
©Copyright 2021 HP Development Company, L.P. The information contained herein is subject to change without notice.





# Be Part of IT.

Vielen Dank für Ihre Teilnahme.

HP Schweiz AG  
Gilbert Benkert, Service Sales Consultant  
[Gilbert.benkert@hp.com](mailto:Gilbert.benkert@hp.com)

ARP Schweiz AG  
Silvio Defuns, HP Business Development Manager  
[silvio.defuns@arp.com](mailto:silvio.defuns@arp.com)