

it-sa 2024: Who is attacking your infrastructure and how?

Simulating the vulnerability of your infrastructure with HCL BigFix.





Jens NEHMER Diplom-Kaufmann Product Sales Specialist HCL BigFix Senior Area Sales Director DACH HCL Software DACH +49-173-5749713 Jens.Nehmer@hcl-software.com

HCLSoftware

Copyright © 2023 HCL Software Limited | Confidential

HCL BigFix

Industry-leading software solutions with proven reliability & trust to supercharge digital programs for enterprises of all sizes.

20K+ Global clients

50% Global 500 clients

75+ Software products



4.5K+



FERRARI TEAM PARTNER

45+

Global presence in countries

Employees

\$1.4B Enterprise software business



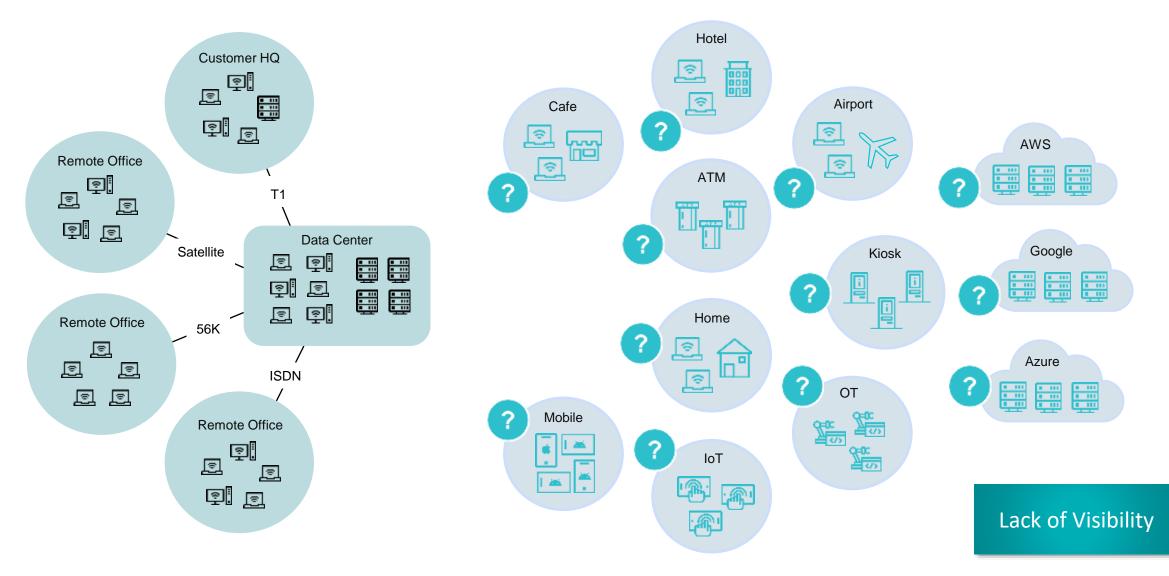
Endpoint Management Platform



Copyright © 2023 HCL Software Limited | Confidential

Maintaining All Endpoints Remains Complex

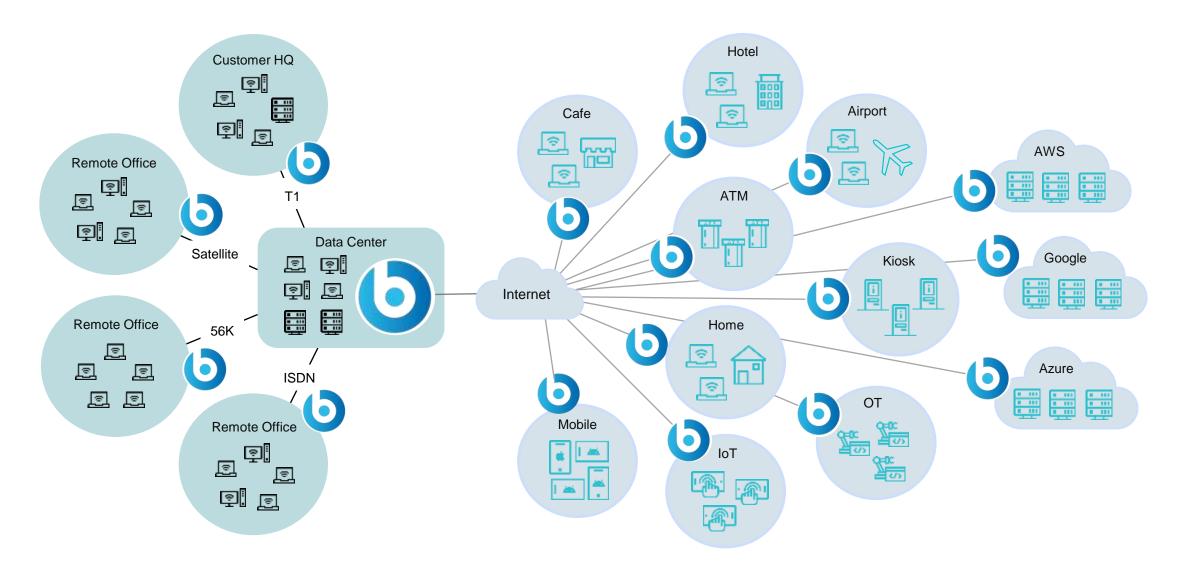
Vulnerable, unpatched, susceptible to configuration drift



4

BigFix Endpoint Management

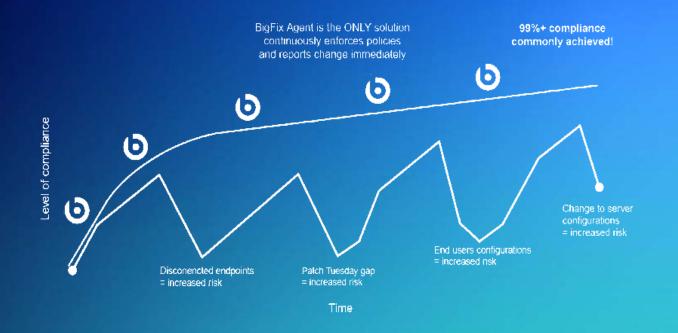
Secure and manage *all* endpoints



Continuous Compliance & Policy Enforcement

Continuous compliance puts rules enforcement at the endpoint & continuously loops through all assigned policies & configurations, ensuring that the endpoint is always in a compliant state.

- Providing near real-time assessment
- Automatic remediation of configuration drift
- Track, analyze & report on compliance status & historical trends





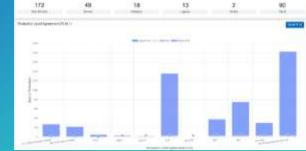
CyberFOCUS

"The first vulnerability remediation solution that helps teams to collaborate to <u>prioritize</u> vulnerabilities, <u>prescribe</u> the most effective remediation strategies, <u>protect</u> through remediation, and <u>prove</u> better cyber security outcomes."









Your Exposure to Known Attackers? Your Exposure to Known Vulnerabilities? Your Exposure to Discovered Vulnerabilities?

Proven Cyber Risk Reduction to C-Suite?

What's new in CyberFOCUS 1.1?

Prescriptive remediation guidance for MITRE APT simulator to help organizations more quickly and effectively reduce their attack surface against APT groups

Better understand your exposures by being able to drill-down to the details of the affected devices

More out of the box Protection Level Agreement (PLA) definitions enabling you to more quickly and easily understand the organization's effectiveness in remediating issues

× CVE to impact the most MITRE APTs Completely mitigating CVE-2017-0199 will reduce the attack surface of correlated MITRE APT groups by: 23.3% . This cye has been correlated to 10 APT groups. Total Exposure Count:60 X MITRE correlated CVE with the most exposures The cve with the most exposures (regardless of group affinity) is CVE-2018-8174. This cve has 4 exposures. This cve has been correlated to 2 APT groups. #TRE Advanced Persistent Threat Groups () AFT Groups (19 1 2 of Equipments by DVE) Color 2 Minute CV And in case of ADD DOT A

Insights for Vulnerability Remediation

Use your existing vulnerability scanning tool and match the found vulnerabilities to BigFix remediation

Quickly execute the suggested remediation actions on your schedule for the fastest vulnerability remediation loop.

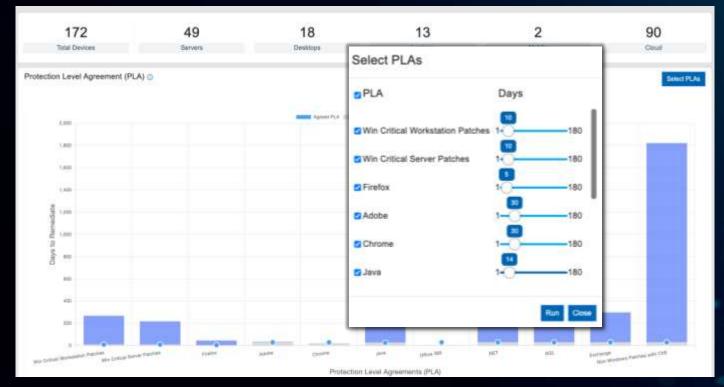
| To | p 1D Critical VPR Exposures By | + DIE | Great | kdown by | CVSE V | Enerability Priority Ratiog | Top 10 Vulr | | | | | | |
|----|---|---|----------------------------|--|------------------------|-----------------------------|--|------------------|-------|------|-----------|--------|---------------------------|
| | OVE-John-olde | | | | | | | | | | | | |
| | CVE-atao-seat | | | | | | | | | | | | |
| | CVE-max-max- | | | | | | 100 | | | | | | |
| | CVE 2020 9014 4 | | | | | | and showing the | | | | | | |
| | CVE-2020.xeri 4 | | | | - | | × . | | . I | | | | |
| | cive anazi-mon 4 | | | | | | | | | | | | |
| | OVE-adda-autor | | | | | | - | | | | | | |
| | CVE-8018-12207 | | 0.0 | | | | | 11-50-000 | 1.000 | 1144 | 00-91-000 | 0.1100 | 1000-13 m |
| | CVE-2020-15998- | | 100pt | fwe : | - 48 - 5 | | | 8 1 | 1 | R | R (| n R | 10 |
| | | | 1.04 | | | | | | | | | | |
| | CVE-Jené-H138- | | | | | | | | | | | | |
| 69 | suiterabilities as of Jul 12, 2023 🍙 | - 13 | | | | | | ńew. | 20 • | 1 | 3. • | • > | 1sf4pages |
| 69 | | H Recodule (1) | VPR - 1 | VPR | cvss 7. | CVEIDs | Patone S | | 20 • | | | | |
| 69 | varberebildies as of Jul 12, 2029 . S ma Extended . Yow Extend only | Remediate (3) | | | evisi % | CVE IDs | | , | | | | | |
| 69 | valterabilities as of Jul 12, 2023 ma Deleting View Distance any Tenable Valterability 1, | Remediate (3) | | VPR | | | Published 12 | , | | | | | Esposure ① |
| 69 | Valiterabilities as of Jul 12, 2023 . The Deletion of Mark Scheme and Schem | Remediate (3) | VPR - 1, | ¥P8 • | • | 1000 for 64 million | Published 1/2 minutely, • | , | | | | | Esposare ① · |
| 69 | valterabilities au of Jul 12, 2023 Tenable Valverability 1, Type Int anoth, Windows Epeculative Execution Configur. | Remediate (2) (8) 1/2 132303 | VPR = 7; 2.2 | yee • | • Nedure | 1924 for second | Published 1/2 mm/2007, • Jan 4, 2018 | 1 | | | | , | Exposure (1) |
| 69 | Valiberabilities as of Jul 12, 2023 Valiberabilities as of Jul 12, 2023 Valiberabilities as of Jul 12, 2023 Valiberabilities as a constrained and a constrained and a constrained as a constra | 1000022000(2) 60 % 102300 102300 102906 | VPR = 1, 23 9 | VPR + High Concel | • Nedum High | 11 CVEs 45 CVEs | Published 1/2 men/abby - Jan 4, 2018 New 12, 3016 | 1 | | | | 7 | Exposure (1) |
| 69 | Valheesbilles as of Jul 12, 2023 Tenable Valvesbilly 1, Tenable Valvesbilly 1, Yes hit seech. Wedays Epeculative Execution Configur. K645252356 Windows 10 Versen 1607 A. K64525258 Windows 11 and Windows E. | Rome2ator (2) (2) 192107 130906 | V94 - 1; 23 9 1 | VPR VPR High Critical Critical | Medum Nedum High | 1300 for Sec. 10. | Published % mm/dbly, - Jan 4, 2018 New 12, 3016 New 12, 2019 | 1 1 1 1 | | | | 7 | Exposure ① N 0 8 |

Remediate Vulnerabilities

| 0 | Salact contact | | Defect ante | | 0 bite | t hargetiv | | 0 | Configure | | | Deployment Summary |
|------|----------------------------|-------|------------------|------------------|--------------|------------|----------|--------|--------------|------------|--------|--|
| eget | by dealers Target by | prave | Target for price | erties Target by | class) refer | **1.0 | | | | | | Deployment Name * Multiple Action Group |
| 3 64 | nies 💎 # | | | | 4 | at w | ur 20 | • 1 | 1.4.1 | Tellipe | qia | - 9 Vulnerability Conte |
| 110 | na Selected 🛛 🖬 Ven | Seter | *** **** | | | | | | | | | ~ 3 Targets |
| | Computer Name | | Critical Patches | Applicable P., 1 | Depinge | nertis | Desize T | (press | 95 | | Sine | PHLICIGARITIE |
| | Spinity models. | | | | _ | | | | | ÷ | _ | privati halocat |
| 8 | affrication and the second | 0 | No | (440) | | 29 | Server | | fiel the los | ingrise. | MAG-R | Data |
| | PHL00546179 | ø | Pau | 408 | | 364 | Server | | Red that the | terprise. | MAC 6 | Bas |
| - | REAR STORES AND | 0 | Test | 22 | | 12 | farser. | | Mindows 3 | Training T | IAAC 4 | |

Protection Level Agreements

- Manage the SLA around patching by providing accurate reporting on patching times. Set an agreement on patching timeline for each category and then view the adherence to policy in one view.
- Provides the best way to balance cybersecurity risk, downtime, and patching efforts in one decision making roundtable approach



Jana PLE Charden has not facer and

Jan 8

ALT:

SQL

Office 365

Rose Windows Patches with CWT

Scope Definition

Application

Application

Application

Application Non Vischum

PLA Definition Tris PCA defines that all critical and high severity content for JADA be patched within 15 days of the machine being stansard as relevant. This PCA applies to all Windows systems estimothed to the Updates for Windows Application Stat. Centert Scope All Jaca critical and high severity contact within the Updates for Windows Applications There are 252 Contant Barry in scope of this PLA Tree Barger Officiance in time from when the machine was first downood applicable (first percarks, relevant) and other the machine was patched to the timeleane calculation The larget limit and is 30. The actual limitants is: 145. Machine Scope Ad Windows Systems askecified to the Updates for Windows Application Site are in acops There are 36 Machines in scope of this PLA. FLA THE Actual Contrast Strengt Machine Scope Californy Tarpet Wathence. Windows Weskplans Rên Crîtical Workstation Patishea #5 Days NT Days +24 12 100 Wedges Server We Critical Server Patcher 38 Days iil Dege 2016 23 Fished 15 Days 30 Days 4.55 36 Application 200 Application Adulta 30 Days 33 Oays 211 Overse 100.000 & Clays. - 10 37 Application

30 Days

30 Days

30 Days

33 Days

30 Days

145 Days

T Days

35-Days

254 Days

10 Days

1712

+

1264

-01

253

122

343

221

2344

36

55

14

36

44

Where can you find as on it-sa 2024? Hall 9 - Booth 9-325

Who will be onsite from HCL?

-Management HCL Software
-Product Sales Specialists HCL BigFix
-Technical Advisors for deep dives and simulating BigFix and it's console
-Business Partner Manager

The next Panel discussions from the HCL BigFix Team:

-Wednesday

-Thursday

What else will be at the HCL booth?

-An original F! race car (a red one) -A racing Simulator for everybody to try.



HCLSoftware

hcltechsw.com