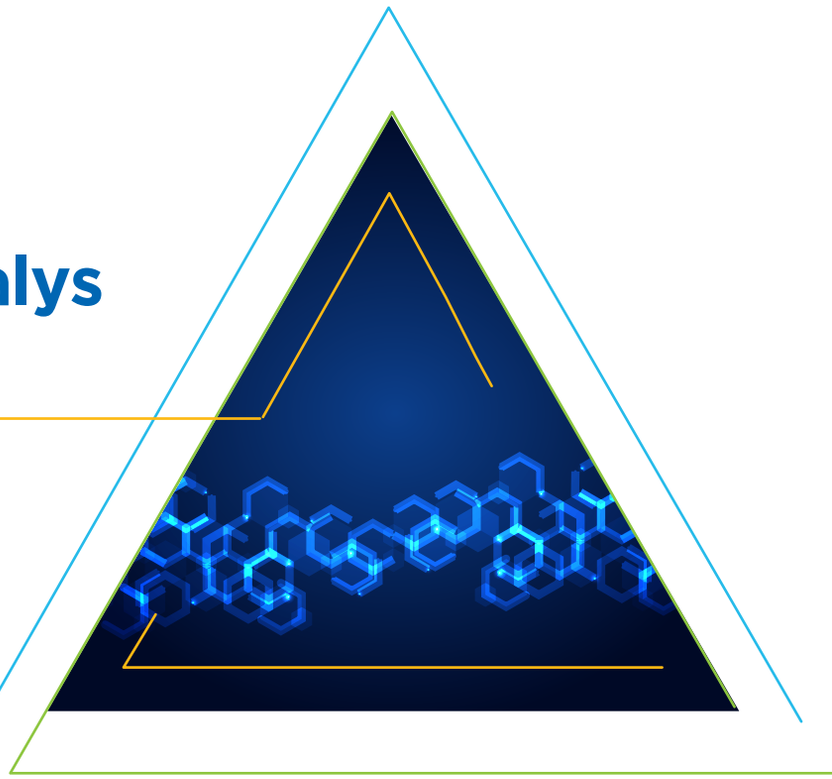
BigFix Insights for Vulnerability Remediation Integration mit Qualys



Verbessern Sie die Zusammenarbeit zwischen Sicherheitsteams, die Qualys® verwenden, und dem IT-Betrieb, der BigFix einsetzt, um die Zeit für die Behebung von Schwachstellen drastisch zu verkürzen.

Heutzutage kann es Tage oder Wochen dauern, bis der IT-Betrieb die von der IT-Sicherheit gefundenen Schwachstellen behebt, wodurch Unternehmen potenziellen Angriffen ausgesetzt sind. Daher steht die Minderung des Risikos von Cyberangriffen weiterhin ganz oben auf der Liste der Anliegen von CIOs und CISOs.

Unternehmen, die Schwachstellen mit Qualys® aufspüren, konzentrieren sich auf die Suche nach Sicherheitslücken im gesamten Unternehmen. Mit BigFix® findet der IT-Betrieb systematisch den richtigen Patch für jede einzelne, von Qualys identifizierte Schwachstelle und setzt ihn ein. In vielen Fällen besteht eine Kommunikationslücke zwischen den beiden Organisationen, was zu übermäßigem manuellem Aufwand, zu Fehlern in Excel-Listen und zu langen Zeitfenstern für potenzielle Sicherheitsrisiken führt. Tatsächlich zeigen aktuelle Studien, dass bis zu einem Drittel aller erkannten Schwachstellen nach einem Jahr noch offen sind und mehr als ein Viertel nie behoben werden.

BigFix Insights for Vulnerability Remediation kann die Zeit, die der IT-Betrieb für die Behebung der von der IT-Sicherheit gefundenen Schwachstellen benötigt, von Tagen oder Wochen auf Minuten oder Stunden reduzieren. BigFix Insights for Vulnerability Remediation korreliert automatisch die von Qualys entdeckten Schwachstellen mit den am besten geeigneten Patch- und Konfigurationseinstellungen, so dass Unternehmen schnell Prioritäten bei der Behebung setzen und die Angriffsfläche des Unternehmens reduzieren können. Im Gegensatz zu anderen Lösungen. BigFix verfügt über das breiteste Spektrum an Reparaturmöglichkeiten, sowohl in Bezug auf die unterstützten Betriebssystemplattformen als auch in Bezug auf zertifizierte Abhilfemaßnahmen, die sofort einsatzbereit sind.

Die Anwendung BigFix Insights for Vulnerability Remediation wurde speziell für Unternehmen entwickelt, die BigFix Lifecycle und BigFix Compliance einsetzen und zusätzlich Qualys für das Schwachstellenmanagement nutzen.

Highlights

- Verringern Sie die Lücke zwischen Sicherheit und IT-Betrieb drastisch und verbessern Sie das Bewusstsein dafür, welche Korrekturmaßnahmen erforderlich sind, um entdeckte Schwachstellen zu schließen
- Korreliert automatisch die von Qualys gefundenen Schwachstellen mit den empfohlenen BigFix Fixlets unter Verwendung von vier separaten Korrelations-Engines und liefert gleichzeitig die Daten, die Sie für eine effektive Priorisierung der Korrekturmaßnahmen benötigen
- Verkleinert Angriffsflächen und schließt den Kreislauf zwischen Schwachstellenerkennung und -beseitigung
- Erfordert keine zusätzlichen Agenten oder Relays und hat keine Auswirkungen auf die Leistung des Endgeräts oder des Netzwerks

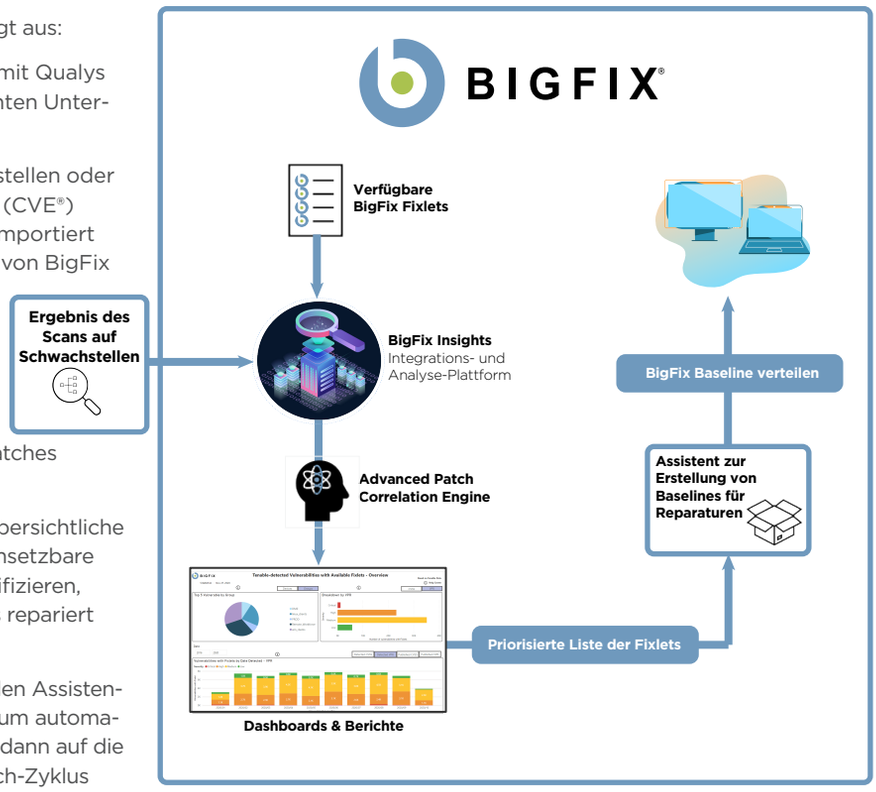
Beschleunigte Behebung von Schwachstellen – so funktioniert die Lösung.

BigFix Insights for Vulnerability Remediation beschleunigt die Behebung von Schwachstellen durch die Automatisierung manueller Prozesse, die in Unternehmen häufig vorkommen. Die automatisierte Korrelation der Ergebnisse des Scans mit Qualys mit den verfügbaren Fixlets von BigFix beschleunigt die Absicherung von Endgeräten im gesamten Unternehmen.

Der übliche Arbeitsablauf sieht dann wie folgt aus:

1. Ein Security Operator führt einen Scan mit Qualys durch, um die Schwachstellen im gesamten Unternehmen zu identifizieren.
2. Die von Qualys identifizierten Schwachstellen oder Common Vulnerabilities and Exposures (CVE®) werden automatisch in BigFix Insights importiert und mit den umfassenden Patch-Daten von BigFix kombiniert.
3. BigFix Insights for Vulnerability Remediation nutzt dann unsere Advanced Patch Correlation Engine, um die Scan-Daten der Qualys-Analyse automatisch mit den neuesten BigFix-Patches zu korrelieren.
4. BigFix-Benutzer können verschiedene übersichtliche Dashboards und Berichte nutzen, um umsetzbare und priorisierte Schwachstellen zu identifizieren, die sofort mit verfügbaren BigFix Fixlets repariert werden können.

   Ein BigFix-Benutzer im IT-Betrieb kann den Assistenten zur Erstellung von Baselines nutzen, um automatisch Reparaturen zu erstellen und diese dann auf die Zielgeräte zu verteilen, wodurch der Patch-Zyklus abgeschlossen wird.



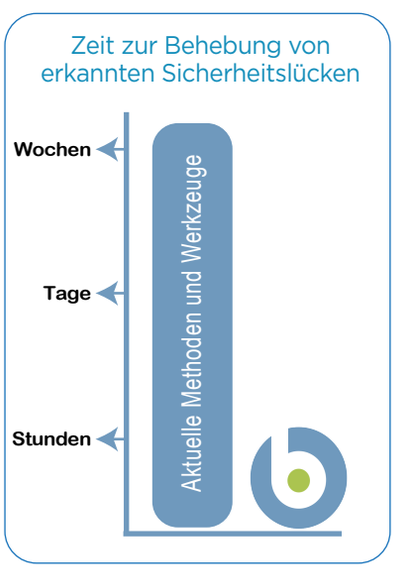
BigFix Insights for Vulnerability Remediation Arbeitsablauf

Mit diesem Arbeitsablauf können Unternehmen, die bereits Qualys einsetzen, zusätzlich BigFix Insights for Vulnerability Remediation nutzen, um die Zeit für die Behebung von Schwachstellen, und damit die Angriffsfläche, drastisch zu reduzieren.

BigFix Insights for Vulnerability Remediation – Eine Fallstudie

Normalerweise verbringt ein IT-Betriebs- oder Sicherheitsspezialist 2-3 Minuten mit der Suche nach der richtigen Abhilfemaßnahme für jede Schwachstelle. Bei potenziell Hunderten oder Tausenden von Schwachstellen ist das ein großer Zeitaufwand. BigFix Insights for Vulnerability Remediation automatisiert diesen Prozess mit nicht weniger als 4 Korrelations-Engines:

1. Korrelieren Sie die Endpunkt-ID mit der Qualys-Endpunkt-ID
2. Korrelieren Sie die gefundene Sicherheitslücke mit einem BigFix Fixlet
3. Identifizieren und weisen Sie die aktuellste Fehlerbehebung zu
4. Korrelieren Sie den BigFix-Endpunkt mit dem neuesten Fixlet



Was bedeutet das in der Praxis? Ein Unternehmen mit 1.000 aktiven Schwachstellen verbringt bis zu 50 Personenstunden pro Scanzyklus mit der Recherche und dem Zuordnen der verfügbaren Korrekturen zu den richtigen Geräten. Mit BigFix Insights for Vulnerability Remediation kann diese Zeit auf weniger als 2 Stunden reduziert werden, indem manuelle Prozesse automatisiert und Fehler und damit verbundene Nacharbeit reduziert werden. Jetzt ist eine IT-Organisation in der Lage, Korrekturen schnell zu implementieren und die Konformität gegenüber Auditoren und Führungskräften effektiv nachzuweisen. Mit BigFix Insights for Vulnerability Remediation sind die Teams für IT-Sicherheit und IT-Betrieb in der Lage, effektiv zusammenzuarbeiten, um die von Qualys entdeckten Schwachstellen schnell zu beheben, was dem CIO und CISO einen erheblichen betrieblichen und organisatorischen Nutzen bringt. Dieser Mehrwert wird realisiert durch:

- **Abstimmung von Sicherheits- und Betriebsteams mit intelligenter Automatisierung**
- **Drastische Verkürzung der Zeit für die Behebung von Sicherheitslücken**
- **Reduzierung des Sicherheitsrisikos im Unternehmen**

BigFix-Korrelations-Dashboard für Schwachstellen

Das Qualys-Vulnerability Correlation Dashboard bietet handlungsorientierte Ansichten der korrelierten Daten von Qualys und BigFix. Jede Ansicht hilft IT- und Sicherheitsmitarbeitern, das Ausmaß und den Schweregrad der Schwachstellen auf unterschiedliche Weise zu verstehen, um eine effektive Priorisierung von Abhilfemaßnahmen zu ermöglichen. Das interaktive Dashboard ermöglicht es den Anwendern, weitere Details zu den korrelierten Schwachstellen und Geräten aufzurufen.

Vier Granularitätsebenen

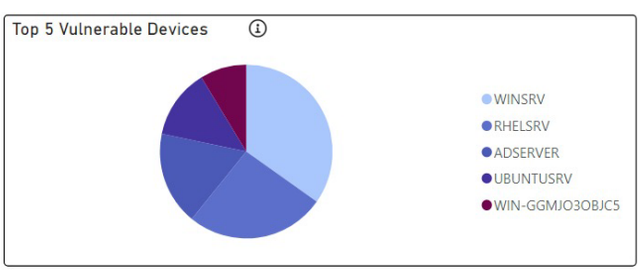
Das Dashboard bietet vier Reiter, um die korrelierten Schwachstellendaten von Qualys und BigFix in verschiedenen Granularitätsstufen darzustellen:

1. **Grafische Übersicht** – umfasst drei Graphen oder Diagramme für einen visuellen Überblick auf übersichtlichem Niveau, um eine sehr schnelle Priorisierung über mehrere Kontexte hinweg zu ermöglichen.
2. **Datenansicht** – zeigt Schwachstellen und die zugehörigen Fixlets zusammen mit der Anzahl der betroffenen Geräte in einem Tabellenformat an.
3. **Schwachstellenansicht** – zeigt an, welche Geräte eine bestimmte Schwachstelle aufweisen, und das empfohlene Fixlet zur Behebung.
4. **Geräteansicht** – zeigt alle Schwachstellen und die empfohlenen Fixlets zur Behebung, die mit einem bestimmten Gerät oder Endpunkt verbunden sind.

Die grafische Ansicht enthält die drei unten abgebildeten Diagramme. Einige nutzen den Schweregrad-Score von Qualys, der eine Priorisierung der Schwachstellen ermöglicht. Einige Diagramme bieten auch die Möglichkeit, Daten nach CVSS (Common Vulnerability Scoring System) zu betrachten, einem Industriestandard für die Bewertung des Schweregrads von Sicherheitsschwachstellen.

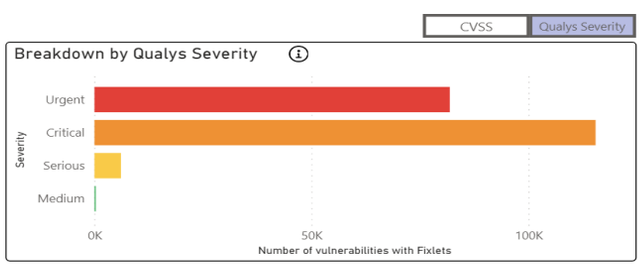
Top 5 der gefährdeten Geräte

Das erste Diagramm zeigt die fünf Geräte mit der höchsten Summe der Schweregrade von Qualys in Verbindung mit gefundenen Schwachstellen, die durch BigFix behoben werden können.



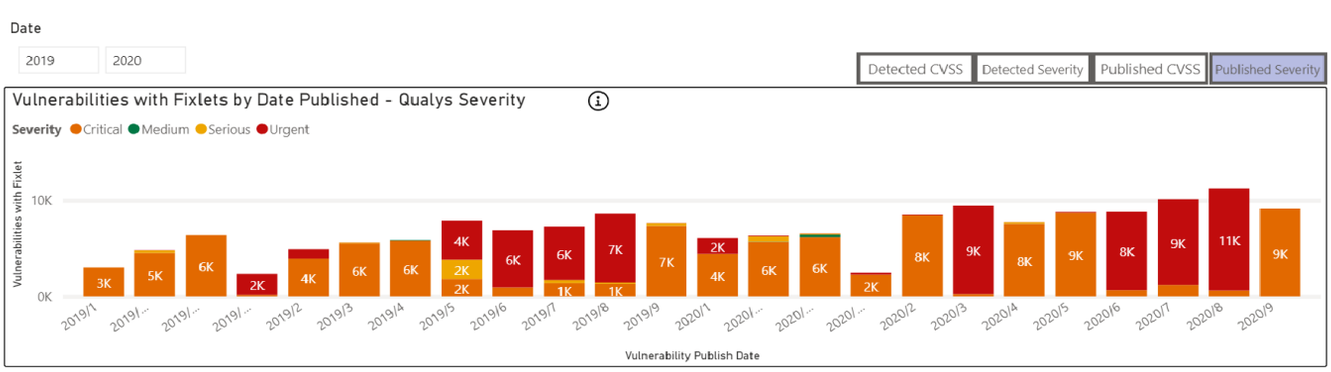
Schwachstellen nach Schweregrad

Das zweite Diagramm stellt Schwachstellen mit verfügbaren BigFix Fixlets nach Qualys-Schweregrad oder nach CVSS dar.



Schwachstellen nach Entdeckungsdatum und Schweregrad

Das dritte Diagramm ergänzt die Details aus dem Diagramm „Sicherheitsrisiken nach Schweregrad“. Insbesondere werden in diesem Diagramm das Entdeckungsdatum und das Veröffentlichungsdatum hinzugefügt. Das Entdeckungsdatum ist das Datum, an dem eine bestimmte Sicherheitsanfälligkeit zum ersten Mal von Qualys entdeckt wurde, während das Veröffentlichungsdatum das Datum ist, an dem der Datensatz der Sicherheitsanfälligkeit zum ersten Mal zur CVE-Liste hinzugefügt wurde. Es kann auch ein Datumsbereich nach Jahr angegeben werden.



Die Vorteile von BigFix

BigFix basiert auf einer einzigartigen, hoch skalierbaren Infrastruktur, welche die Entscheidungsfindung auf die Endpunkte verlagert. Dies bietet außergewöhnliche Funktions- und Leistungsvorteile für die gesamte BigFix-Lösungsfamilie und reduziert gleichzeitig die Kosten für die Endpunktverwaltung und die Komplexität der Infrastruktur.

- **Ein einziger intelligenter Agent –** Der BigFix-Agent führt mehrere Funktionen aus, darunter eine kontinuierliche Prüfung und die Durchsetzung von Richtlinien. Er initiiert Aktionen auf intelligente Weise, indem er Nachrichten an den zentralen Management-Server sendet und Patches, Konfigurationen oder andere Informationen in Echtzeit an den Endpunkt weiterleitet. Der BigFix-Agent drosselt sich selbst auf 2% CPU, führt eine dynamische Bandbreitendrosselung durch, um unterschiedliche Grade der Netzwerkbandbreite an entfernten Standorten zu berücksichtigen, und läuft auf mehr als 90 Betriebssystemen unter Windows, Linux, UNIX und macOS.
- **BigFix Fixlets™ –** BigFix Fixlets sind kleine Automatisierungseinheiten, die es der IT-Abteilung ermöglichen, ihren täglichen Betrieb zu vereinfachen und sich auf komplexere Vorgänge zu konzentrieren. BigFix bietet mehr als 500.000 Out-of-the-Box Fixlets. Das BigFix-Team aktualisiert die Fixlet-Bibliothek kontinuierlich, mit über 130 Content-Updates pro Monat. BigFix-Benutzer, Business-Partner und Entwickler können Fixlets nutzen, um benutzerdefinierte Richtlinien und Dienste für von BigFix verwaltete Endpunkte zu erstellen. Eine Community-Bibliothek von Fixlets ist auf BigFix.me verfügbar.
- **Hoch-skalierbare Architektur –** Ein einziger BigFix-Management-Server kann bis zu 250.000 physische und virtuelle Computer über private oder öffentliche Netzwerke verwalten, und die meisten Implementierungen erfordern nur 1-2 Betreuende pro Server. Zu den verwalteten Endpunkten können Server, Desktops, Laptops, Endpunkte in der Cloud und spezielle Geräte wie POS-Geräte, Geldautomaten und Selbstbedienungskioske gehören.
- **Multicloud-Unterstützung –** Cloud-Endpunkte können mit BigFix einfach neben lokalen Endpunkten verwaltet werden. Die Multicloud-Unterstützung ermöglicht es Unternehmen, den BigFix-Agenten auf Cloud-Endpunkten einzusetzen, um vollständige Transparenz, Kontrolle und Sicherheit zu gewährleisten. Damit können selbst Endpunkte, die in mehreren Cloud-Umgebungen gleichzeitig laufen – wie Amazon Web Services, Microsoft Azure und Google Cloud Platform – zentral verwaltet werden.
- **Integrationen –** BigFix lässt sich mit den Lösungen der wichtigsten Partner aus den Bereichen Sicherheit und IT-Betrieb integrieren, um ein umfassendes Ökosystem für Unternehmen zu schaffen, dass eine Vielzahl von Funktionen zur Analyse, Optimierung, Gewinnung von Kontext und Ergreifung entscheidender Maßnahmen für alle Bereiche Ihres IT-Betriebs bietet, um die Compliance zu verbessern und Cyber-Risiken zu reduzieren. Zu unseren Partnern gehören ServiceNow, IBM, Tenable, Aruba, Intel, Forescout und andere.

Die BigFix Produktfamilie

Ihre Investition in BigFix kann das Management Ihrer Endgeräte verbessern, Softwarekosten reduzieren und eine ganzheitliche Sicht auf Ihre Infrastruktur ermöglichen. BigFix-Kunden haben IT-Tools und Endpunkt-Agenten drastisch konsolidiert und unterstützen gleichzeitig neue Arbeitsformen wie z. B. das Home Office. Die BigFix-Familie umfasst:

- **BigFix Lifecycle –** Ermöglicht es der IT-Sicherheit und dem Betrieb, Hunderttausende von Endpunkten mit einer einzigen Plattform schnell zu erkennen, zu schützen und zu verwalten. Es bietet einen automatisierten, vereinfachten Patch-Prozess, der über Windows-, UNIX-, Linux- und macOS-Plattformen hinweg eine Erfolgsquote von mehr als 98 % beim ersten Patch-Durchlauf erreicht - unabhängig von Standort oder Verbindung. BigFix Lifecycle umfasst auch Betriebssystembereitstellung, Softwareverteilung, Fernsteuerung, Serverautomatisierung, Energieverwaltung, BigFix Modern Client Management, BigFix Insights und BigFix Insights for Vulnerability Management.
- **BigFix Compliance –** Erzwingt kontinuierlich die Konformität der Endgerätekonfiguration mit Tausenden von vorkonfigurierten Sicherheitsprüfungen, die sich an branchenüblichen Sicherheitsbenchmarks von CIS, DISA STIG, USGCB und PCI-DSS orientieren. BigFix Compliance bietet einen automatisierten, vereinfachten Patch-Prozess, der bei Windows, UNIX, Linux und macOS eine Erfolgsquote von mehr als 98 % beim ersten Patch-Durchlauf erreicht - unabhängig von Standort oder Verbindung. BigFix Compliance umfasst auch BigFix Modern Client Management, BigFix Insights und BigFix Insights for Vulnerability Remediation.
- **BigFix Inventory –** Reduziert drastisch den Zeitaufwand für die Durchführung einer umfassenden Software-Bestandsaufnahme zum Lizenzabgleich oder zu Compliance-Zwecken. BigFix Inventory liefert wertvolle Informationen darüber, welche Software auf den Endgeräten installiert ist und wie diese Software genutzt wird. BigFix Inventory reduziert die jährlichen Softwareausgaben, mildert Strafen für die Nichteinhaltung von Lizenzbestimmungen und hilft bei der Identifizierung nicht autorisierter oder riskanter Software für eine mögliche Entfernung.
- **BigFix Modern Client Management –** Ermöglicht Unternehmen eine vollständige Übersicht und Kontrolle über Windows 10- und macOS-Endgeräte, indem sie entweder einen traditionellen BigFix-Agenten oder Mobile Device Management (MDM) APIs verwenden. Die Kombination beider Ansätze bietet IT-Teams die größte Bandbreite an Verwaltungs- und Automatisierungsmöglichkeiten. Zero Touch Provisioning beschleunigt und vereinfacht die Bereitstellung neuer Laptops für Remote-Benutzer. Mit BigFix Modern Client Management können Organisationen neuere Unternehmensplattformen einfacher und kostengünstiger verwalten.
- **BigFix Insights –** Ermöglicht es den Teams, die Bedrohungslage ihres Unternehmens schnell an die Führungskräfte zu melden und erweiterte Analysen durchzuführen, um die nächsten Schritte voranzutreiben. Dieses innovative Angebot bietet eine leistungsstarke Endpunkt-Integrationsplattform und Datenbank für tiefere Erkenntnisse über traditionelle On-Premises-, Cloud- und MDM-API-verwaltete Endpunkte. BigFix Insights nutzt Business Intelligence (BI)-Reporting-Tools, um sofort einsatzbereite und individuell anpassbare Berichte zu erstellen.

Für weitere Informationen

Wenn Sie mehr über BigFix erfahren möchten, wenden Sie sich an Ihren Ansprechpartner bei HCL Software, einen HCL Business Partner oder besuchen Sie **www.BigFix.com**.

Über HCL Software

HCL Software ist ein Geschäftsbereich von HCL Technologies, der ein Portfolio der nächsten Generation von softwarebasierten Angeboten für Unternehmen mit flexiblen Nutzungsmodellen für traditionelle On-Premises-Software, Software-as-a-Service (SaaS) und gebündelte Managed Services entwickelt und bereitstellt. Wir bieten unseren Kunden Geschwindigkeit, Einblicke und Innovationen (große und kleine), um Mehrwert zu schaffen. Die Lösungen von HCL Software umfassen DevOps, Sicherheit, Automatisierung, Anwendungsmodernisierung, Daten- und Integrationsinfrastruktur sowie verschiedene Geschäftsanwendungen. HCL nimmt die reale Komplexität der Multi-Mode-IT an, die vom Mainframe bis zur Cloud und allem dazwischen reicht, und konzentriert sich dabei auf den Kundenerfolg und den Aufbau von „Relationships Beyond the Contract".

04/2021