# Middleware 11.23

# Funktionen

- Whitelist-Updates
  - Implementierung der Möglichkeit, eine Ausnahme mit dem übergeordneten Programmpfad und den Argumenten zu erstellen
  - Implementierung der Möglichkeit, eine Ausnahme zu erstellen, die Erpressungsantworten abgleicht, wenn nur vertrauenswürdige Zertifikate vorhanden sind, nur dann übereinstimmt, wenn keine zugehörigen Injektionen vorliegen, und nur dann übereinstimmt, wenn kein modifizierter Speicher vorhanden ist
  - Implementierung der Möglichkeit, eine Ausnahme zu erstellen, die bestimmte Dateizugriffsauslöser abgleicht
- Implementierung einer Gruppeneinstellung zur automatischen Freigabe von Lizenzen für inaktive Agenten
  - Aktualisierung des Gruppenmodells um eine Einstellung, wann Lizenzen von inaktiven Agenten in der Gruppe freigegeben werden sollen. Optionen sind 30/60/90 Tage oder die Deaktivierung dieser Einstellung
  - Aktualisierung des Agentenmodells um einen neuen Inaktivitätsstatus
  - Implementierung eines Dienstes zur automatischen Freigabe von Lizenzen inaktiver Agenten gemäß ihrer Gruppeneinstellung
- Aktualisierung des Endpunkts zum Abrufen von Erpressungsantworten, um den übergeordneten Programmpfad und die Argumente einzuschließen
  - Der übergeordnete Programmpfad und die Argumente sind nun auch in den eindeutigen Erpressungsantwort-Zählungen für die Webanwendung, die Sicherheitsbenachrichtigungen und die Executive Summaries enthalten
- Aktualisierung unserer Executive-Summary-Berichte, um die Lizenzen-Folie in separate Folien für Desktop- und Server-Lizenzen aufzuteilen
- Aktualisierung des E-Mail-Sicherheitsbenachrichtigungsmodells und des Sicherheitsbenachrichtigungsdienstes um zwei neue Alarmtypen
  - Verhaltensmodell angepasst
  - Neue Agentenversion
    - Wenn die verwalteten Update-Einstellungen einer Gruppe so geändert werden, dass automatische Updates deaktiviert sind, wird automatisch eine Benachrichtigung über eine neue Agentenversion für die Gruppe erstellt
- Aktualisierungen der Benutzerrollen/-berechtigungen
  - Aktualisierung der Berechtigungen des Rollenmodells „Incident Manager“, sodass nun nur noch Ansicht/Bearbeitung für Whitelists und stille Reaktionsregeln vorhanden sind
  - Gruppen verfügen nun über 3 Standardrollen, die von Benutzern nicht bearbeitet werden können:

    - Admin
    - Nur Lesen
    - Gast
  - Benutzer, die einer Gruppe hinzugefügt werden, erhalten standardmäßig die Rolle „Gast“
- Implementierung von Endpunkten für das Modal zur Abstimmung von Browser-Hilfsprozessen der Webanwendung, um einfach verwalten zu können, wie Agenten in Gruppen auf Chrome-Hilfsprozesse reagieren sollen
- Aktualisierung des Endpunkts für das Diagramm der Agenten-Seite, um Zählungen auf Agenten beschränken zu können, die sich in den letzten 30/60/90 Tagen gemeldet haben
- Aktualisierung der E-Mail-Benachrichtigung „Ransomware-Aktivität“ der Sicherheitsbenachrichtigung, um einen Link einzuschließen, der Benutzer automatisch zur Seite „Erpressungsantworten“ weiterleitet, mit einem Filter, der die Antworten anzeigt, auf die sich die Benachrichtigung bezog
- Implementierung einer Gruppeneinstellung, ob Agenten in einer Gruppe im abgesicherten Modus ausgeführt werden oder nicht
- Implementierung einer PowerShell-Skriptoption zur Installation von Agenten
- Aktualisierung unseres Spring Boot auf die neueste Version
- Verschiedene Aktualisierungen unserer Liste von Standarddaten-, Identitäts- und Zertifikats-Whitelists für Antivirenprogramme

---

Revision #1
Created 2026-07-24 04:07:10 UTC by Dennis Underwood
Updated 2026-07-24 04:07:10 UTC by Dennis Underwood