Que é a diferença entre as quarentena da manifestação e do vírus?

Índice

Pergunta:

Que é a diferença entre as quarentena da manifestação e do vírus?

Resposta:

As quarentena de AsyncOS incluem duas quarentena incorporados que não podem ser suprimidas: Manifestação e vírus.

A quarentena da manifestação é usada somente por filtros da manifestação do vírus (se permitida.)

As mensagens que encontram ou excedem o ponto inicial configurado do nível da ameaça do vírus na ferramenta de segurança do email de Cisco (ESA) são realizadas na quarentena da manifestação em vez do fornecimento. As mensagens podem ser liberadas ou suprimido da quarentena da manifestação na discreção do gerente da quarentena. As mensagens igualmente sairão da quarentena se o tempo ou os limites de tamanho configurados são excedidos, e estará segurado com o ajuste da política padrão da quarentena à supressão ou à liberação se estes limites são alcançados.

A liberação de seguimento da quarentena da manifestação, mensagens é tornada a varrer pelo módulo anti-vírus, e a ação é tomada de acordo com a política anti-vírus. Segundo esta política, uma mensagem pode ser entregada, suprimido, ou entregado com os acessórios virais descascados. Espera-se que os vírus estarão encontrados frequentemente durante a nova varredura após a liberação da quarentena da manifestação. Os arquivos ou o rastreamento de mensagem dos mail_logs ESA podem ser consultados para determinar se uma mensagem individual que seja notada na quarentena foram encontrados para ser viral, e se e como ele foi entregado.

A quarentena do vírus está disponível para receber as mensagens que Sophos classifica como vírus-contaminadas, cifrado ou un-scannable. Em cada um destes casos a mensagem é viral ou potencialmente viral. As mensagens enviadas à quarentena do vírus permanecerão lá até que o gerente da quarentena escolham as liberar ou suprimir d, ou o tamanho configurado ou os limites de tempo da quarentena está alcançado. A ação padrão quando os limites da quarentena são alcançados é configurável.

As mensagens liberadas da quarentena não são tornadas a varrer pelo módulo anti-vírus; contudo, quando na quarentena o gerente da quarentena puder fazer a varredura de uma mensagem individual para determinar se é viral de acordo com o grupo atual de vírus IDEs carregado no ESA.

Nota: Os vírus novos quarantined, mas as mensagens as mais velhas na quarentena são niveladas para fazer a sala para os novos. Isto é “primeiramente dentro, primeiramente para fora” política. Contudo, a disposição das mensagens as mais velhas é baseada em como a quarentena é configurada, significando que as mensagens estão suprimidas prematuramente ou liberadas prematuramente.

Embora as quarentena incorporados não possam ser suprimidas, a quantidade de espaço atribuída a elas pode ser reconfigurada. A quantidade de espaço disponível para quarentena varia pelo modelo ESA, e é indicada na página das quarentena de Monitor->Quarantines->Manage no GUI. O tamanho mínimo para uma quarentena é 250MB. Tendo um limite superior fixo às quarentena assegura que um aumento repentino na atividade da quarentena não pode impactar as filas do correio do ESA e afetar a entrega do mensagem normal.