

SECURING LEGACY ESTATES:

Are you really protected?

Our digital world requires IT decision-makers to have a comprehensive understanding of the threat environment in which they operate.

However, there is no silver bullet fix that will magically protect you from all cyberthreats.



The trouble with patches

If you have used any custom code the OEM is not aware of, implementing a generic security patch could unintentionally break the system.

You can't defend what you don't know

A patch is only one element of a vulnerability management program. It's important to evaluate your overall cybersecurity in a broader context using a layered approach that includes the following steps:



Contextual

Analyze your organization's environments — including business, people, processes, technologies, threat, and regulatory — to develop the appropriate mitigating actions for each circumstance. This must be an ongoing process to be effective.



Risk-based

Actions to reduce the likelihood of an identified security vulnerability being exploited should be employed until your desired level of risk has been achieved.



Defense-in-depth

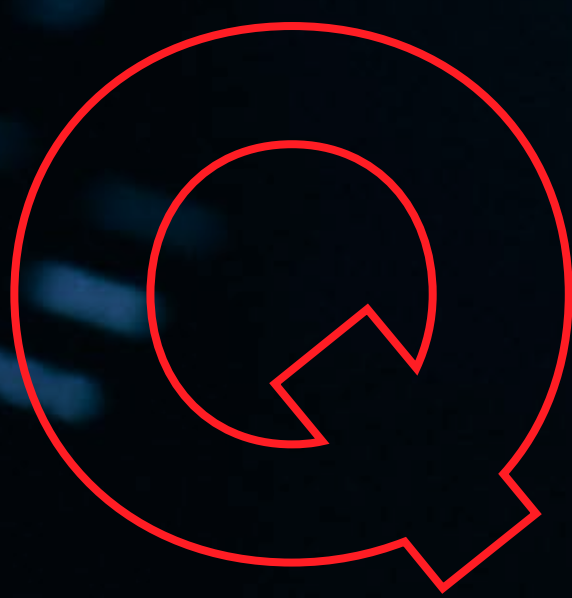
Apply multilayered defense actions across the environment in layers to secure the supported product and enhance your overall security posture.

Minimizing cybersecurity threats requires a layered, forward-thinking approach that limits exposure to vulnerabilities.



CYBERCRIME FORECASTED TO COST THE WORLD

\$10.5 TRILLION ANNUALLY BY 2025



ASK YOURSELF

Do we receive more than security patches as a line of defense?

Do I have a clear picture of potential vulnerabilities and mitigation solutions?

Am I alerted to potential cyberthreats in a timely manner?

Is our security solution tailored to our business?

Do we feel supported in our plan against cyberthreats?

Are you really protected?

Origina

Download our e-book

