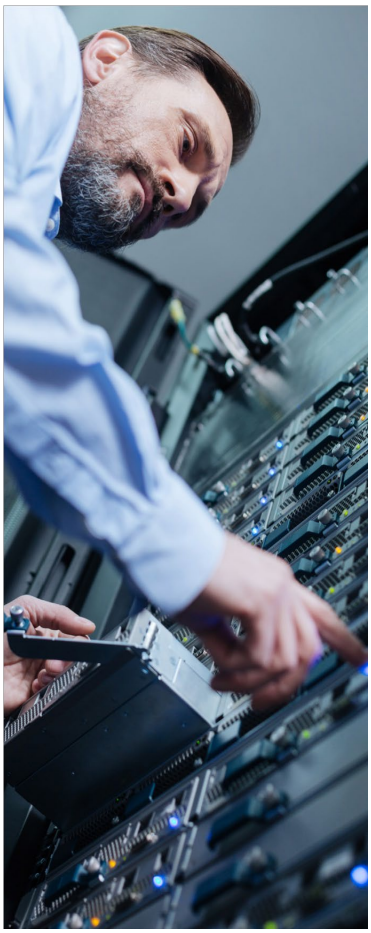
Monitoring SSL Certificates With Argent Omega At No Cost

White Paper

ARGENT

Why Are SSL Certificates So Critical?



SSL certificates are used to verify to users that your website is legitimate.

They also provide encryption of the internet traffic between the user's browser and your website.

When an SSL certificate expires, **all traffic between the user's browser and your website will no longer be encrypted** -- sensitive customer data such as credit card and home address information will be exposed in plaintext to hackers.

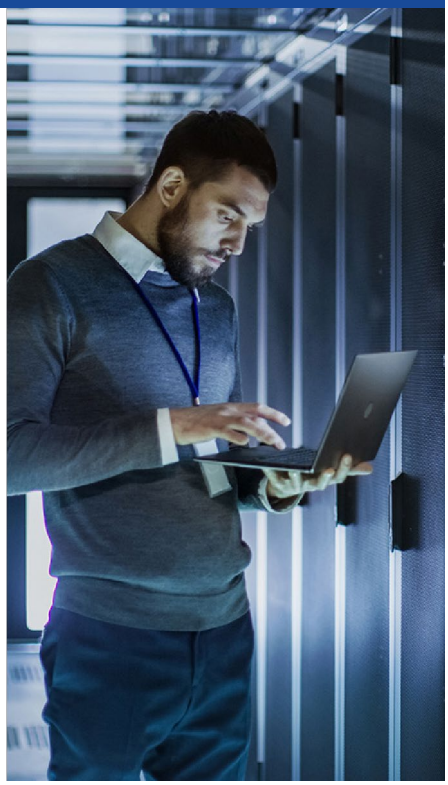
Hello Class Action lawsuits.

Monitoring expired SSL certificates is an essential but often overlooked job.

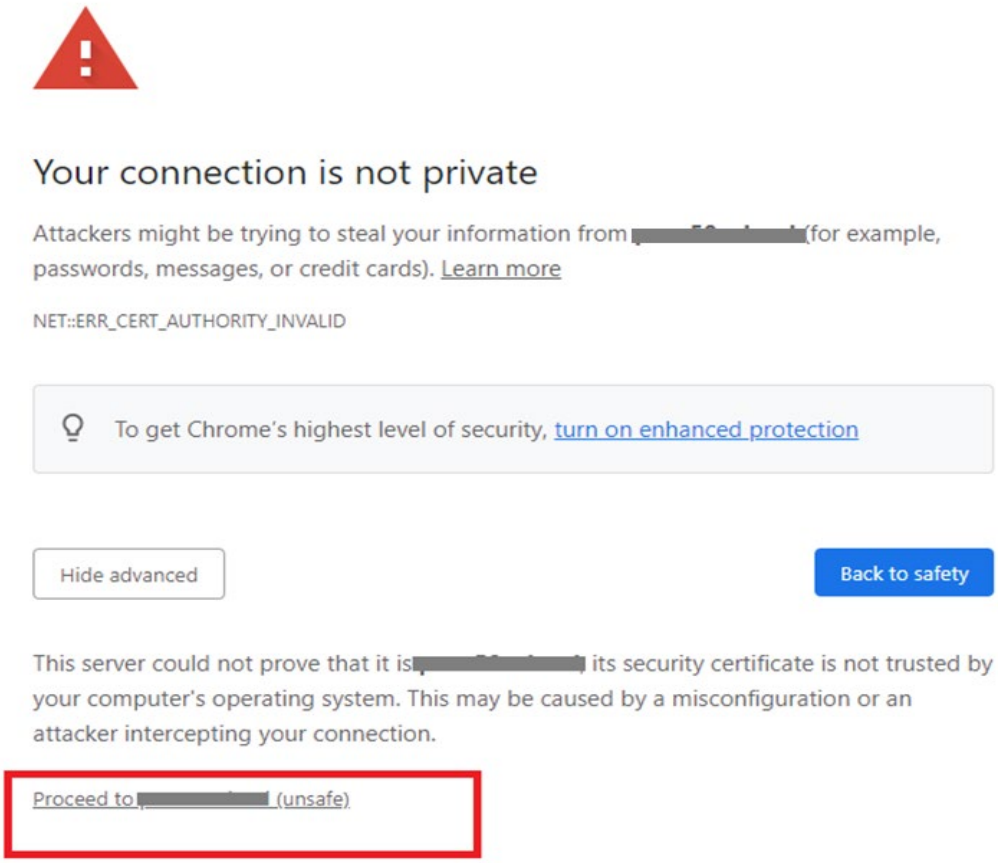
An expired SSL certificate needlessly creates panic.

Panic because your critical website is offline.

Needlessly because Argent can stop this at no cost to you.



The web browser will immediately warn any visitor trying to access the website that the site is unsafe and that hackers might be trying to steal their information (See example warning message below from the Google Chrome browser).



And…

Using an expired certificate also results in failed audits and regulatory fines.

Why Do SSL Certificates Expire?

The SSL regulatory body for the SSL/TLS industry requires that SSL certificates do not last longer than one year; can be shorter.

This ensure your website's authenticity is validated on a regular basis.

But for IT this is a new nightmare to ensure all your company's SSL certificates are both up-to-date and will not shortly expire.

How Argent Can Help

Argent Omega provides an easy way to **automate monitoring** the validity and expiration dates of all company's SSL certificates.

Argent Omega customers can start monitoring their SSL certificates within minutes using the built-in SSL Certificate monitoring Rules.

All at no cost to you.

Learn more by speaking to an Argent consultant today simply email

Support@Argent.com

We'll do all the heavy lifting for you.