DATA SHEET

TANIUM
Public Sector

Managing Digital Certificates in the Public Sector

Gain real-time and detailed visibility to keep essential services open.

> A recent study showed 39% of organizations failed their certificate audits, and 27% of certificates found had weak encryptions.[1]

Don't let a weak, unknown, or expired certificate ruin your day. Modernize your certificate management with Tanium's Converged Endpoint Management (XEM) platform.

Digital transformation shouldn't be jeopardized by expired certificates

Public sector organizations rely on current and secure certificates to enable communications, and provide essential services. But with digital transformation efforts in full swing, there is a growing number of certificates to manage.

Studies have shown that the average organization manages more than 50,000 certificates. With an abundance of legacy tools to meet the challenge, public sector organizations are often stuck manually maintaining their certificate inventory in spreadsheets, and don't have access to real-time data and visibility into several parts of the network.

Not being able to manage certificates at scale can lead to service outages or compromises, resulting in a loss of productivity and reputation.

Common challenges of managing certificates for public sector organizations include:

- Tedious, manual processes required to manage tens or hundreds of thousands of certificates cause expired certificates to be missed.
- Lost reputation and disruption to digital services when expired, weak or unknown certificates are left unnoticed.
- Threat of compromise when weak cryptography is used to secure communications, particularly with future quantum computing advances.
- Legacy tools used to manage certificates are laborious, slow and don't integrate with other tools used for cybersecurity or IT operations management.

With Tanium XEM, you can inventory your certificates, gain automated insight into when they will expire, and find vulnerable cipher keys and certificates with weak security in real time.

- Get real-time visibility on location, health and status of your digital certificates across your environment.
- Avoid essential service disruptions with automated digital certificate expiry reporting.
- Identify your most easily compromised certificates to mitigate risks.
- Reduce manual workload on IT operational and security teams.
- Prevent man-in-the-middle (MITM) data theft by finding unauthorized certificates.
- Avoid point tools by leveraging a single XEM platform across IT, risk and security teams.
- Protect sensitive data by reducing entry points into critical systems due to weak ciphers.

> "A typical modern organization requires support for multiple certificate authorities (CAs), diverse certificate discovery mechanisms, detailed reporting and alerting, and a wide set of out-of-the box integrations for life cycle management. CAs often need to be complemented by certificate management tools to be able to meet all needs."
>
> Gartner

Tanium XEM can help prevent service downtime and save hundreds of hours of operational work by discovering your certificates, sending alerts when they are expiring, and identifying where you are most vulnerable.

- **Get complete visibility on the location, health and status of your certificates from across your IT environment.** Large parts of your operations cannot work if the certificates expire – not to mention disruption to critical services for constituents if your public website is shuttered. Know the certificates you have in your endpoint environment, and when they are about to expire in real time with the XEM platform.
- **Identify where your certificates are being stored.** Have a view of your certificates across your endpoint estate faster and more accurately to know if they're from authorized Certificate Authorities (CAs). Instead of guessing which networks and ports to scan for, you will have visibility to identify certificates wherever they are across your endpoint environment.
- **Ensure strong secure communication and future-proof your certificate management.** Find non-compliant certificates that need to be replaced, such as those with short key lengths or weak hash algorithms that could compromise the connection and allow traffic to be decrypted.
- **Keep essential services open, and protect sensitive data.** Maintain mission-critical operations internally, and keep your external services open and uphold public trust.

SEE TANIUM IN ACTION

Experience visibility, control and remediation with the industry's only Converged Endpoint Management (XEM) platform.

Schedule a demo

ENDNOTES

[1] https://academic.oup.com/cybersecurity/article/7/1/tyab025/6470936

Tanium, the industry's only provider of converged endpoint management (XEM), protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. State and local governments, educational institutions, federal civilian agencies and the U.S. Armed Forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. Visit us at www.tanium.com.