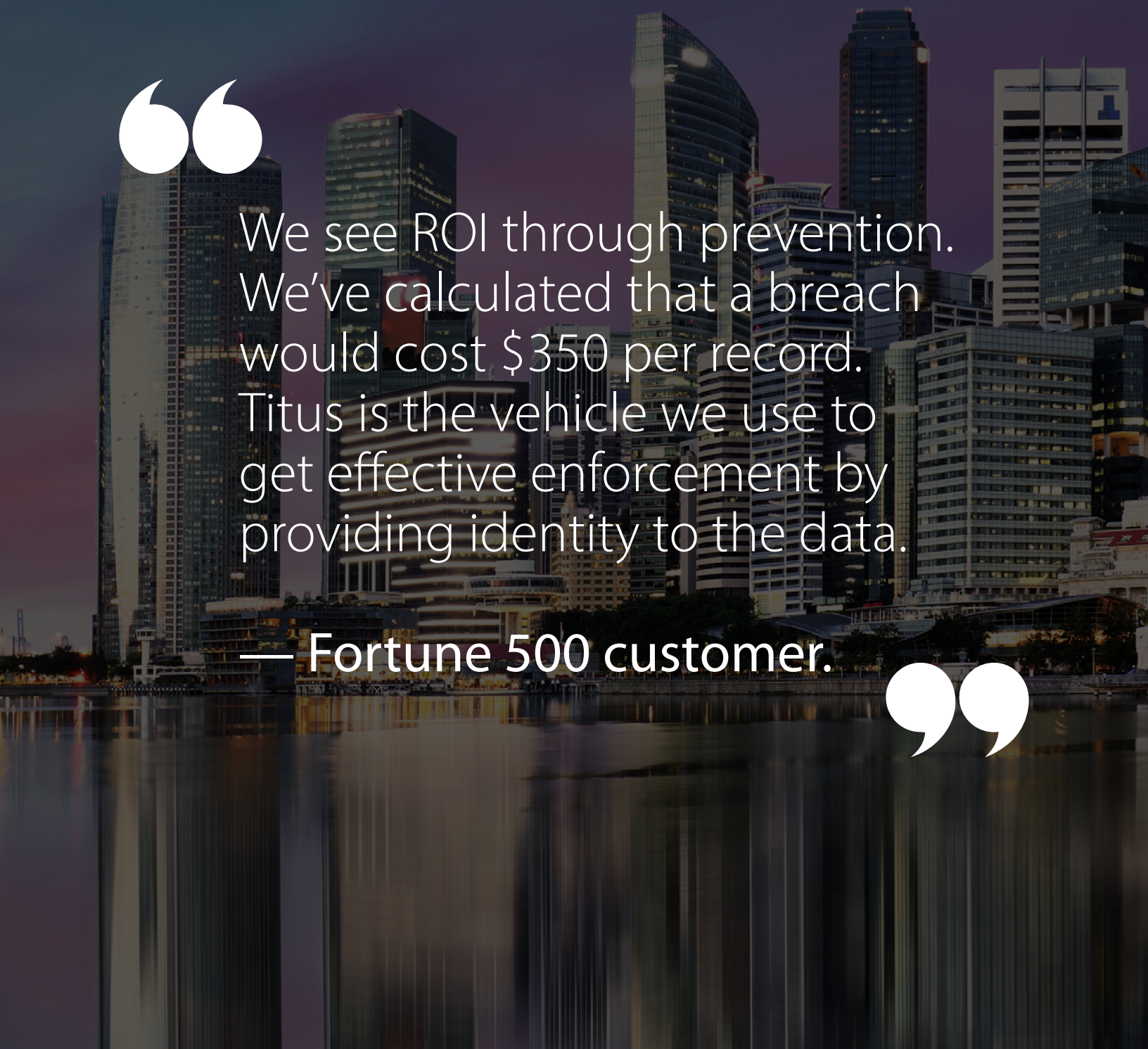
titus
by HelpSystems

Working towards the **Technical Measures for a Smart Nation**

Maintaining the confidentiality, integrity and availability of customer data while safeguarding against increasingly sophisticated cyberthreats is an evolving concern. The Public Sector Data Security Review Committee is deploying measures to help you more confidently protect your customers' assets by creating a common approach to cybersecurity across the public sector and nation.

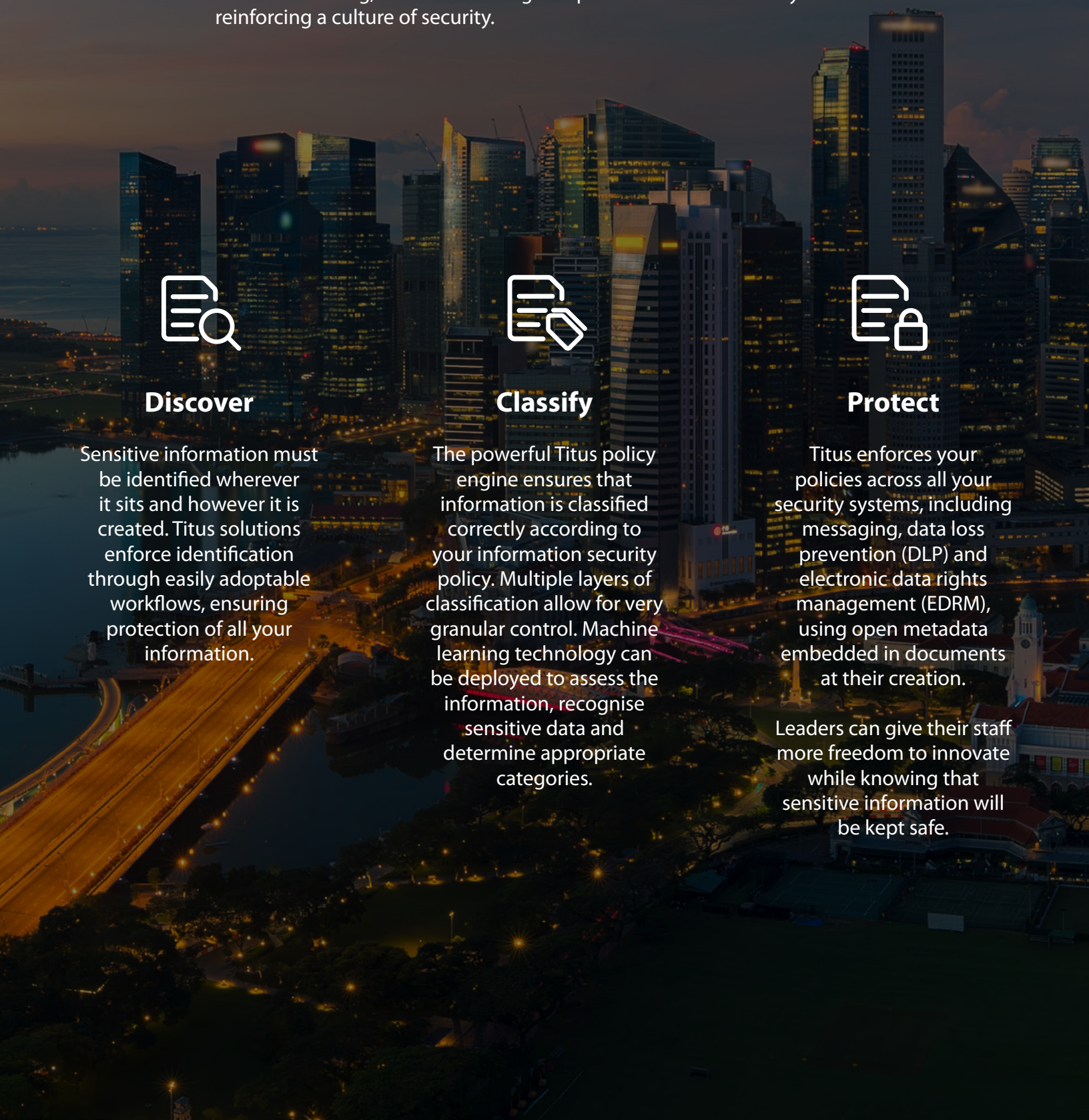
Titus will help you achieve the desired outcomes that the measures address by complementing and strengthening your existing cybersecurity infrastructure.



> We see ROI through prevention. We've calculated that a breach would cost $350 per record. Titus is the vehicle we use to get effective enforcement by providing identity to the data.
>
> — Fortune 500 customer.

How Titus supports your **compliance**

Titus works in concert with your existing cybersecurity infrastructure to help you achieve end-to-end cybersecurity compliance. The open, configurable, policy engine enables your organisation to enforce detailed data identification and information handling policies with award-winning machine learning, while monitoring compliance and continuously reinforcing a culture of security.



Discover

Sensitive information must be identified wherever it sits and however it is created. Titus solutions enforce identification through easily adoptable workflows, ensuring protection of all your information.

Classify

The powerful Titus policy engine ensures that information is classified correctly according to your information security policy. Multiple layers of classification allow for very granular control. Machine learning technology can be deployed to assess the information, recognise sensitive data and determine appropriate categories.

Protect

Titus enforces your policies across all your security systems, including messaging, data loss prevention (DLP) and electronic data rights management (EDRM), using open metadata embedded in documents at their creation.

Leaders can give their staff more freedom to innovate while knowing that sensitive information will be kept safe.

Titus supports you in the implementation of data protection measures recommended by Singapore's Smart Nation and Digital Government Office. Titus' cybersecurity controls complement your existing security infrastructure, ensuring protection of commercially sensitive and personal data throughout your organisation and wider ecosystem.

The Titus platform is open by design, integrating seamlessly with your existing security stack. As your partner in deploying your security strategy, Titus implements our proven methodology built with over 10 years of experience in data identification and security. Our solution set is designed to support compliance with the technical, people and process data protection measures as they are finalised and deployed.

Technical **Measures**

Strengthen the whole security infrastructure

After data classification by Titus, users and other systems (e.g. DLP, messaging) are triggered to apply the necessary restrictions for the data. E.g. salted hashing, tokenisation, encryption, obfuscation, masking and dataset partitioning. Under this process, the whole security infrastructure becomes compliant.

Watermarking

Identify the source of data files and their classification. Titus can mark documents with physical watermarks and metadata that identify the classification and individual responsible for setting the classification.

Email data protection

Prevent accidental disclosure of confidential data. Users are prompted to confirm they are aware of the value and sensitivity of data they are about to send by email. All emails are scanned for confidential data and users are challenged or warned, if necessary, before sending. Safe recipient checking can prevent classified emails from being sent to the wrong people.

Data Loss Prevention

Prevent the loss of confidential information on end-points, laptops, phones, etc. Titus marks all datafiles with a metadata classification that will trigger DLP systems to act to stop data loss and unauthorised file transfers.

Automatic identity and access management tools

As users change roles and departments and eventually leave the organisation, their access control rights must keep up with their status. Titus allows multiple classifications to strengthen control of the information that users can access.

Time limited data access

Restrict the length of time that users have access to confidential data. Titus can flag documents for deletion when a user's allocated time has expired.

Enhanced logging and active monitoring of data access

Be warned of immediate and long term threats. Titus can log all sensitive user activity and will scan for anomalous behaviour, flagging it to authorities. E.g. behaviours such as repeated down-classifying and downloads at unexpected times of day.

People

Security is a continuous process. By using Titus in their everyday work, users are always reminded of security policies and to protect valuable information. Titus suggests classifications by understanding the content, thereby continuously training users to recognise its value.

Process

Governance of cybersecurity requires effectively implementing a security policy across the whole organisation and its partners, monitoring for compliance and investigating non-compliance. Titus puts in place the foundations for achieving all this by orchestrating the data security policy across all the security infrastructure so that the entire organisation can remain safe.

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

(tt-sb-0722-db)