Web Attack Surface Management

Gain Deeper Visibility into Your Web Application Inventory to Secure Your Attack Surface

Problem

Accelerated digital transformation has made it difficult for your security operations center (SOC) and application security (AppSec) teams to keep tabs on your external web attack surface. Your web attack surface spans everything from a single source of truth for your web inventory to being able to monitor software supply chain risks due to third-party technologies or dependencies attributed to an organization's web artifacts.

Lack of visibility into these dependencies and their outdated artifacts creates serious cracks in your web attack surface, putting your organization and customers at risk. Legacy solutions are manual and require frequent updates. However, it's a problem that your teams can solve with automation.

Solution

Get complete, current, and accurate visibility into your public-facing web infrastructure without any manual intervention from your security teams with Cortex Xpanse. With the Web Attack Surface Management (Web ASM) Module, your security teams can:

- Continuously discover and monitor your website inventory and web technologies.
- Identify insecure and misconfigured websites in your environment.
- Identify sites failing security best practices and putting users at risk.
- Track and measure the risk due to third-party libraries or dependencies attributed to an organization's web artifacts.
- Identify websites serving sensitive content such as personally identifiable information (PII) and payment forms using insecure protocols.

Xpanse empowers your security teams with continuous visibility for managing public-facing web infrastructure, continuously reducing the critical security gap your organizations face. With Web ASM, organizations see not only a continuous and updated view of their web attack surface but also discover insecure content running on their managed and unmanaged web assets to highlight critical security gaps.

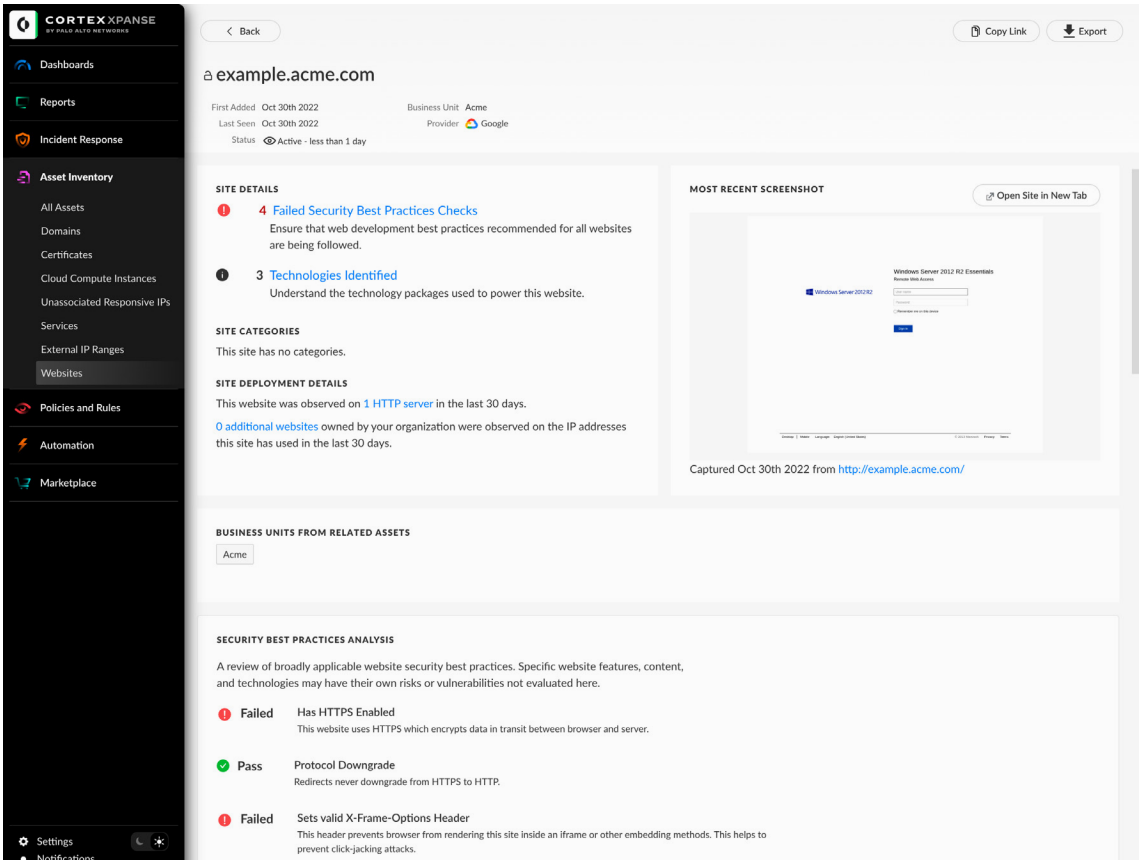

Figure 1: Complete, current, and accurate visibility into your public-facing web infrastructure

The Web ASM Module helps your client-side security teams defend against the following types of attacks:

- Payment skimming/E-skimming
- Hijacking website forms/CSS injection
- Supply chain attacks—dependencies within dependencies

How It Works

Cortex Xpanse scans your known and unknown assets to discover websites that belong to your organization. Web ASM then crawls these individual webpages to discover and classify the different web technologies used to build that particular web asset. Once this continuously updated web inventory is created for your organization, Web ASM performs a security best practice analysis to identify misconfigurations and potential vulnerabilities. Web ASM then enriches incidents with additional business context to help your security teams resolve issues faster and at scale.

Use Cases

- Inventory of backend/frontend web technologies (i.e., Apache, Drupal, ReactJS, Angular).
- Identify pages that deal with payment card forms.
- Discover insecure login forms susceptible to credential skimming.
- Identification of sensitive websites—webforms/payment forms on HTTP (potential PII leaks).
- Discover accidentally exposed websites (e.g., shadow dev/marketing).
- Continuous server software discovery. Discover server software running in your network and automatically evaluate if they are exposed to CVEs.
- Third-party software risk. Distributing web dependencies (e.g., WordPress plugins, Google Analytics, Pendo, Marketo, etc.).

Customer Outcomes

Bank Eliminates Insecure Login Pages

A large North American bank used Web ASM to discover all of its websites with insecure login pages and quickly resolved them.

Insurance Provider Reduces Software Supply Chain Risk

A major insurance provider used Web ASM to identify third-party libraries to help manage risk from supply chain vulnerabilities.

Travel Company Takes Down Shadow Web Assets

A large travel company used Web ASM to identify unsanctioned websites being spun up by marketing/shadow developers and remediated them.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com