SECURITY COMPASS WHITEPAPER

Controlling Shadow IT Projects

Copyright © 2019 Security Compass. Updated Sept 2019.

Security Compass

Security teams have their work cut out for them. As the application and IT environment become more complex, the adoption of DevOps and container technologies, like Docker, create the need for more frequent change.

Attackers have grown more sophisticated in their attacks and more adept at attacking soft targets, like poorly managed IoT devices. According to Symantec's 2019 Internet Security Threat Report, IoT devices experience an average of over 5,000 attacks each month, with routers and connected cameras accounting for over 90% of the attacks.

While understaffed teams struggle to secure the environment they manage and control, additional risk comes from IT projects launched by others in their organizations without the knowledge or supervision of IT. "Shadow IT" projects include unapproved software, web applications, servers, IoT devices, and services run by marketing, engineering, and other functional areas of the organization.

Why Shadow IT Happens

Shadow IT is not necessarily deployed by malicious actors. In most cases the users are unaware of the risk shadow IT project pose to the organization; they often begin because users are trying to do their jobs better. Marketing may need to update the organization's website frequently and find that creating their own Joomla instance is faster than waiting for IT to schedule the project. Individual users may bring in devices and add them to the organization's network. Others may find software that is more effective for their use case than that officially approved by the organization, and they may license software or launch a server without notifying IT.

Risks from Shadow IT

It is obvious that security teams cannot protect applications and devices about which they have no knowledge. Since shadow IT projects are administered by teams that are not trained to maintain secure systems, they are often poorly deployed and managed. Many are "orphaned" after a short time, leaving an attack vector into the organization long after the organization stopped using the asset. The vulnerabilities in and risks from shadow IT projects include:

- **Missed Patches** – Thousands of new vulnerabilities are disclosed each year in software, including hundreds in common shadow IT projects like WordPress, Joomla, and Drupal. Often sample exploits are published to validate the vulnerability, providing a simple attack vector for "script kiddies" as well as skilled adversaries. If IT is unaware of the existence of these vulnerable applications, they will obviously not schedule them for patching and updates.

- **Missing Security Controls** – The developers of shadow projects may not understand the requirement for security controls. For example, failing to validate input properly in a login page or order form can result in successful SQL injection and cross-site scripting attacks. While many of these can be discovered in routine security testing, shadow projects outside of security's visibility will not be subject to those tests.

- **Vulnerable Components** – Open source frameworks, like Struts and Spring, are frequently used to simplify building new applications. Publicly disclosed vulnerabilities in these frameworks can be exploited easily by criminals, as seen in the 2017 Equifax breach. With shadow projects, IT will not know that an updated component is required.

- **Vulnerable Devices** – IoT devices, including internet cameras and wireless routers, often have default administrative passwords. Shadow projects may not follow corporate policies requiring that the default password be changed to a strong, random password.

- **Uncontrolled Data Leakage** – Employees may use shadow services to move data to their home computers for convenience, including customer information, product plans, and other sensitive data, presenting an "under the radar" channel that can result in data loss.

- **Regulatory Non-Compliance** – Good security policies and regulatory standards, including Sarbanes-Oxley Act and ISO 19770, require organizations to maintain Software Asset Management…etc.

Shedding Light on Shadow IT

The solution to shadow IT projects is two-fold. First, IT and security require visibility to all assets on the organization's network. Second, appropriate controls are required to minimize risk across all assets.

Visibility Across Your Infrastructure

SD Elements integrates with tools, like Bit Discovery, to provide visibility to all web assets. Bit Discovery crawls your domains to identify all internet-facing assets including web servers, mail servers, software, IoT devices, and web pages, and continuously monitors your domains for changes and new assets. The result is an inventory of anything an external attacker could access – those you know about and shadow projects that were previously invisible to IT. SD Elements automatically captures software metadata including programming language, software frameworks, communication protocols, and authentication mechanisms. If marketing set up a landing page for a long-forgotten demand generation campaign using WordPress or engineering installed an Ubuntu-based test server for a new product, you will know about it.

Actionable Controls

With visibility to your assets, SD Elements automatically translates and tracks policies into actionable tasks and controls. Controls can be mapped to your policies, security standards and frameworks such as ISO 27001, PCI-DSS, and NIST 800-53, or from our knowledgebase of security controls curated by our own security experts.

For example, controls generated for a newly identified web server might include ensuring that the communications channel is encrypted and that sessions time out after 5 minutes of inactivity. A Ruby on Rails application may require controls to test for proper session management and input validation, and Joomla instances will have controls to ensure deployments follow the "Least Privilege" principle for running PHP.

SD Elements prioritizes the identified risks and integrates with popular ticketing systems, like Jira, so the controls can be assigned to developers, security, and IT to remediate vulnerabilities and mitigate risk. Controls can test plans to confirm controls were successfully implemented.

Control and Auditable Compliance

With SD Elements, organizations can quickly gain control over shadow IT projects. Risks are identified and prioritized automatically, and controls generated from Security Compass' knowledgebase. With over 150 standard reports and a centralized repository for all risk data with an auditable record of changes, teams can more easily provide evidence of compliance with internal and external policies and standards.

SecurityCompass

Security Compass believes in a world where people can trust technology, and it is our mission to help customers proactively manage cybersecurity risk, without slowing down business. Our holistic program offerings are tailored to your organization's needs. Through advisory services, training, and SD Elements, our award-winning policy-to-execution platform, we set you up with all of the resources and tools your organization needs to develop secure software. Security Compass serves some of the world's largest enterprises, including 16 of the largest financial institutions in North America, South America, and Asia, as well as 4 of the largest tech companies in the world.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001

Copyright © 2019 Security Compass. Updated Sept 2019.