IDC PERSPECTIVE

DreamWorks Animation Applies HP Inc.’s Expertise and Experience to Reinforce Print and Document Security

Robert Palmer          Allison Correia

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: DreamWorks Animation Partners with HP Inc. to Bolster Print and Document Security

Most organizations have made IT security a high priority. The 3rd Platform computing landscape, inclusive of mobility, big data, cloud, and social media, has accelerated the focus on security. Much of the IT security investment has traditionally emphasized certain technologies that reside on the network, but the print and document infrastructure is one of the most commonly overlooked elements for such initiatives. A large film production studio, DreamWorks Animation, partnered with HP Inc. to address its print security needs.

Key Takeaways

- HP assessed DreamWorks Animation’s print environment and provided recommendations to reduce the attack surface related to using network connected devices and to ensure that printers were secure.
- HP focused on ensuring that printers and multifunction printers (MFPs) have consistent security policies, that patches are deployed in a timely manner, and that all devices are configured to run the latest version of firmware.
- HP’s Print Security Advisory Services (PSAS) supported DreamWorks Animation’s ongoing security and corporate governance policies by enhancing the company’s print security posture.

Recommended Actions

- Enlist a trusted services and solutions provider to assess your environment and deploy a security program. It is important that the provider understand your business objectives and workflows.
- Define one or more print policies that work for your environment. You may need print policies that are specific to departments or different employees.
- Assess your print environment to ensure that printers and MFPs have consistent security policies, that patches are deployed in a timely manner, and that all devices are up to date with the latest security patches and system firmware.

Source: IDC, 2018
SITUATION OVERVIEW

This IDC Perspective looks at how an animation production studio partnered with HP Inc. to automate and standardize print security; assess, identify, and close security vulnerabilities within the print and document infrastructure; and put automated solutions in place to restrict security risks. Organizations that are currently engaged in or are evaluating managed print and document services (MPDS) programs, and are looking to further secure the print environment, can gain valuable insight from these experiences. This document examines the initial security assessment, the business objectives, the results achieved, and the lessons learned. Understanding these elements can help other organizations more effectively evaluate partners and aid in optimizing MPDS and print security programs and engagements.

Most organizations have made IT security a high priority. The 3rd Platform computing landscape, inclusive of mobility, big data, cloud, and social media, has raised the profile of an accelerated focus on security. Much of the IT security investment focus has traditionally emphasized certain technologies that reside on the network, but the print and document infrastructure is one of the most commonly overlooked elements for such initiatives.

Organization Overview

A part of the Universal Filmed Entertainment Group, DreamWorks Animation is a large CG animation production studio with a philosophy built on the idea that "great stories inspire great possibilities." DreamWorks Animation chose to work with HP to address its print security needs. The program is best viewed as an extension to what was already a strong partnership between the two companies. DreamWorks Animation had previously selected HP as its managed print services provider, partnering with the firm in a multiyear agreement that had already produced significant cost and productivity advantages. As part of a typical program review cycle, HP approached DreamWorks Animation to suggest an HP assessment of the overall print and document environment. HP completed an HP Print Security Advisory Services assessment of two of DreamWorks Animation's office locations, including its main campus in Glendale, California.

Challenges: Print as a Security Threat

The DreamWorks Animation management team has a long history of IT security as a top business priority. Over the years, DreamWorks Animation has developed and deployed a corporate information security program designed to predict, prevent, detect, and respond to events that might adversely affect the company's ability to achieve its business objectives. Through its own internal review processes, the DreamWorks Animation security management team had come to recognize the potential threat posed by printers and multifunction printers to the company's overall security posture. Like many organizations today, DreamWorks Animation was increasingly aware that a thorough examination of its print environment from a security perspective would provide an obvious benefit.

The company realized that today's printers and MFPs are more than just peripherals. Instead, these devices are complex computers, with features such as onboard processors, embedded web servers, embedded data storage, and cloud connectivity. Meanwhile, these connected machines often have access to the corporate network. DreamWorks Animation determined that threats posed from an unsecure print environment basically fall into two primary categories: data loss and use of the unprotected print device as an attack vector to pivot from a printer to the network environment.
As a key technology partner and MPS provider for many years, HP has worked with DreamWorks Animation to continuously evaluate its print environment to drive further optimization, improve productivity, and produce better business results. As part of the program review cycle for ongoing improvement, HP suggested an HP Print Security Advisory Services assessment to evaluate the current state of DreamWorks Animation's overall print and document infrastructure from a security perspective. Recognizing the importance of such an initiative, DreamWorks Animation welcomed the opportunity.

In conjunction with its existing MPS program, DreamWorks Animation agreed to work with HP to assess the print environment, provide recommendations to reduce the attack surface related to using network connected devices, and ensure that its printers and MFPs were secure. The assessment at DreamWorks Animation was part of the company's ongoing program to enhance its control environment and bolster its security posture related to printing.

The initial HP PSAS assessment covered process and technical controls within an HP framework designed to address key security elements, including:

- Access control
- Asset management
- Build and release
- Data and document security
- Login and security internet management
- Patching and antivirus
- Device security configuration
- Security governance

The initial review began with a comprehensive meeting and ongoing dialogue between the two security teams formed by both DreamWorks Animation and HP. Once guidelines and objectives were established, HP conducted a more detailed and hands on security assessment of DreamWorks Animation's print and document infrastructure. From an operational standpoint, the process was highly integrative with the HP MPS program and was coordinated between DreamWorks Animation management and the HP onsite administrators.

**Solutions: Consistency in Policy and Governance**

The DreamWorks Animation staff remained involved and engaged in all phases of the assessment, which took about a day and a half to complete. A final report and presentation was then given to the broader team so that stakeholders understood the current landscape as well as potential risks and opportunities for improvement. One of the most important conclusions to come from the assessment was within the context of its existing corporate security and governance policies.

DreamWorks Animation did have security policies deployed for its printers, but the application of those policies was done manually. HP's approach coming out of the assessment phase was to identify the details at every printer location and provide recommendations and best practices for standardizing policies throughout the fleet and closing any inconsistencies. The first recommendation was to focus on what was identified as the "low-hanging fruit": ensuring that printers and MFPs have consistent security policies, that patches are deployed in a timely manner, and that all devices are configured to run the latest version of firmware.
Working with HP, DreamWorks Animation manages operational risk and leverages the capabilities of various HP solutions to identify and restrict risks in a seamless manner for the operations team. HP Security Manager software was recommended as a prerequisite for conducting the assessment, and DreamWorks Animation agreed to deploy that software. HP Security Manager was instrumental in uncovering opportunities for improvement and is leveraged to establish and maintain security configuration settings. Settings may include closing ports, disabling access protocols, and auto-erasing files; automatically assessing security after reboots; and if necessary, automatically remediating device security settings to comply with pre-established company policies.

DreamWorks Animation also deployed printer embedded PIN printing to help employees with sensitive workflows set printing for PIN code entry at any device.

DreamWorks Animation recognized the value of what HP brings to the table, in terms of building consistent and automated support for enterprise-level security feature sets across the environment. This high-level support provides DreamWorks Animation with a comfort level that its attack surface and risk profile has been notably reduced with these incremental enhancements. Much of that comes from direct integration with the existing MPS program because HP is constantly auditing and monitoring the DreamWorks Animation print infrastructure to ensure that it has proper equipment and solutions in place and that the necessary updates are quickly identified and automatically deployed.

The same variables apply to securing the print ecosystem. From an operational perspective, DreamWorks Animation's security policies are easily and quickly created, and the autodiscovery features enabled through HP Access Control mean there is very little productivity impact to the company's operational team. DreamWorks Animation can upgrade and add printers to the fleet with a high degree of certainty that its security policies are all being brought forward.

Deployment of the software and implementation of the additional security initiatives were very straightforward. There were a few days of training, which the onsite administrators described as intuitive, low impact, and centrally administered. Ongoing management of the MPS program and additional security services are handled by HP’s onsite administrators.

**Results**

While it has achieved multiple benefits from the initial assessment and ongoing application of security policies and procedures, DreamWorks Animation notes that the real value of the overall program stems from HP's experience and expertise. From the beginning, HP reinforced that the best approach is not simply to identify and implement a standard set of best practices but instead to pursue a specific program that would work best for DreamWorks Animation within the context of its existing environment and corporate security policies.

DreamWorks Animation says that it has experienced significant benefits from the program across multiple vectors, and results were achieved almost immediately. In fact, DreamWorks Animation management says that it realized immediate value within the first 10 minutes of the initial review of printer policy settings. During this process, a setting that needed adjustment to comply with policies was quickly attuned and updated settings were pushed out to a number of devices. Again, having HP experts onsite during the initial assessment when discussing security control within the context of the DreamWorks Animation environment was crucial.

DreamWorks Animation says that it is difficult to quantify the value of its print security program, especially within the confines of its own existing security policies. Nevertheless, cyberattackers almost
always take the path of least resistance, and it only takes one misconfigured or unpatched device to wreak havoc. In that sense, DreamWorks Animation management says that its partnership with HP in general and the HP Secure MPS program more specifically have proven invaluable. As one security manager for DreamWorks Animation explains, people tend to underestimate the security risk as it relates to print, so minimizing that risk has significantly enhanced DreamWorks Animation’s overall security posture. HP helps DreamWorks Animation not only enhance print security but also save time and money, enabling the company to focus resources on filmmaking initiatives.

ADVICE FOR THE TECHNOLOGY BUYER

Lessons learned from this case study that technology buyers should consider include the following:

- Determine the level of complexity expected for print and document security over the next three years. Built-in features designed to provide endpoint security protection for printing devices will become more commonplace in the coming years. Nevertheless, organizations looking to develop a comprehensive print infrastructure security strategy should seek out solutions and services to extend protection well beyond the device.
- Integrate print security within the context of your overall IT security strategy. Develop a long-term plan that includes measures for ongoing monitoring and management of print and document security programs.
- Define one or more print policies that work for your environment. You may need print policies that are specific to different employees, such as print policies for individuals with sensitive content such as HR or legal, which differs from those for general employees. Also, consider existing guest printing policies.
- Ensure that print policies apply consistently to the printers in scope for those policies.
- Deploy firmware and other security updates in a timely manner.
- Assess your print environment and focus on patching your system and ensuring consistency in installation and configuration.
- Enlist a trusted services and solutions provider to assess your environment and deploy a security program. It is important that the provider understands your business objectives and workflows.

LEARN MORE

Related Research

- HP Inc. Sets Out to Reinvent the Power of Print Through Its Partners (IDC #EMEA43097817, September 2017)
Synopsis

This IDC Perspective looks at how an animation production studio partnered with HP Inc. to automate and standardize print security; assess, identify, and close any security vulnerabilities within the print and document infrastructure; and put automated solutions in place to restrict security risks. Organizations that are currently engaged in or are evaluating managed print and document services (MPDS) programs, and are looking to further secure the print environment, can gain valuable insight from these experiences. This document examines the initial security assessment, the business objectives, the results achieved, and the lessons learned. Understanding these elements can help other organizations more effectively evaluate partners and aid in optimizing MPDS and print security programs and engagements.

"Security of the print and document infrastructure is reaching top of mind for many security managers and IT professionals," said Robert Palmer, research vice president, IDC's Imaging, Printing, and Document Solutions. "This case study outlines a proven approach to addressing key security issues within the print environment, beginning with a holistic current-state assessment that should be viewed as foundational to the ongoing development of corporate governance and security policies."
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2018 IDC. Reproduction is forbidden unless authorized. All rights reserved.