

Palo Alto Networks and Fortra

With data growing exponentially, data loss has become a major concern for organizations around the world. It can severely impact an organization's brand as well as have potential financial and legal implications, especially for organizations in highly regulated sectors. Non-compliance with regulations can result in significant fines. With an increased reliance on cloud services and storage, mobile devices, and bring-your-own-device (BYOD) programs, coupled with concerns over intentional or accidental insider threat actors, organizations are looking for new ways to secure, use, and share data at the speed of their business.

Fortra's Data Classification Suite (DCS)

Fortra offerings enable organizations to adopt a data protection strategy that is open, intelligent, and flexible, enabling them to secure, govern, identify, classify, and confidently share information on their own terms. Using an intelligent policy engine to classify emails, documents, and other file types, DCS identifies sensitive data so that security teams can optimize prevention policies and focus on the highest-risk areas. From automated classification to user-driven classification built into the user's regular workflow, DCS provides the most advanced and flexible ways to meet enterprise requirements. As organizations look to enhance their cultures of security, DCS enforces security policy and provides targeted, interactive education for the user so that security becomes everyone's responsibility. In addition, DCS provides an open ecosystem that integrates with a range of data protection offerings, giving organizations the freedom to leverage current and future technologies that help solve their business challenges.



BENEFITS OF THE INTEGRATION

- Prevent data loss via email with data classification from DCS and datafiltering from Palo Alto Networks.
- Safely enable access to critical information in your data center.
- Prevent access to sensitive data on unsecured systems with DCS and Palo Alto Networks GlobalProtect.
- Protect sanctioned cloud applications against data leakage and regulatory noncompliance.

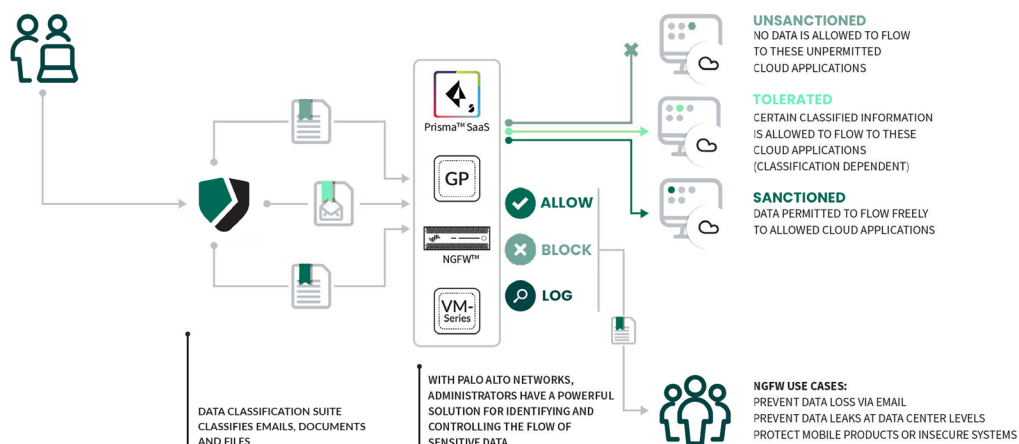


Figure 1: Palo Alto Networks integration with DCS

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyberattacks. Tight integration across the platform and with ecosystem partners delivers consistent security across your network, cloud, and mobile devices, natively providing optimized capabilities across all stages of the attack lifecycle.

Palo Alto Networks and DCS

The Security Operating Platform integrates with DCS to enable secure sharing of sensitive information throughout your enterprise. With DCS, you can designate document classifications (e.g., confidential or internal). Once a document has been classified, metadata filtering is applied to it. With the data filtering features of the Palo Alto Networks Next-Generation Firewall, VM-series GlobalProtect™ network security for endpoints, and Prisma™ SaaS, administrators have a powerful means of identifying and controlling the flow of sensitive data within their networks and to the cloud, based on the email and document classification provided by DCS. Next-Generation Firewalls leverage this data classification to prevent data loss via email, at the data center, in cloud applications, and on unsecured systems and unmanaged devices.

Use Case No. 1: Prevent Data Loss via Email

Problem: Data loss over email, whether accidental or malicious, can have a serious impact on an organization. Users need ways to classify sensitive data and prevent data loss when sending email, especially if they are using an unsanctioned email client.

Answer: Using DCS, Palo Alto Networks App-ID™ technology and the data-filtering profile, joint customers can identify Fortra-classified documents that are being sent outside the network as email attachments. Using Fortra, organizations can identify and classify sensitive data at creation on the desktop (emails, documents, and files) at rest in the cloud,

and in file on-premises repositories, so security teams can optimize prevention policies and focus on the highest-risk areas. Together with Next-Generation Firewall and VM-series data-filtering features, administrators have a powerful means of identifying and controlling the flow of sensitive data.

Use Case No. 2: Prevent Data Leaks at the Data Center Level

Problem: Sharing sensitive materials or information with teams that don't need it introduces unnecessary risks. Preventing unauthorized access to sensitive materials reduces the risks of both intentional and accidental insider threats.

Answer: The DSC and Palo Alto Networks integration allows employees in any department to access certain confidential materials based on rules or policies put in place for each department, role, or region. On the Next-Generation Firewall VM-series with User-ID™ technology enabled, two rules are created for data moving from the trust zone to the DMZ or server zone: one to allow employees within the department and a second to deny all other users.

Use Case No. 3: Protect Mobile Devices or Unsecured Systems

Problem: The increasingly mobile workforce needs to access sensitive data on the go. However, many mobile devices are not secure, which causes security challenges for CISOs forced to compromise between mobility and security.

Answer: With DSC Classification Suite and Palo Alto Networks GlobalProtect, you can mitigate the risks of mobile information-sharing by extending the benefits of classification to your mobile workforce. With GlobalProtect Host Information Profile checks, you can set rules to ensure users can only access sensitive material based on classification over encrypted devices. For example, if a user is trying to download documents that have been classified with a sensitive business value to an unsecured device, GlobalProtect can read the DSC classification and prevent the download.

Use Case No. 4: Control the Flow of Information to Cloud Applications

Problem: The appeal of software-as-a-service (SaaS) applications— such as Office 365®, Box, and Salesforce®— is growing, but so are the hidden threats in SaaS offerings: accidental data exposure, malicious outsiders, promiscuous sharing, and so on. Even sanctioned SaaS adoption can increase the risk of breaches and noncompliance.

Answer: DSC and Prisma SaaS help eradicate risks. Prisma SaaS delivers complete visibility and granular enforcement across all user, folder, and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any additional hardware, software, or network changes. Prisma SaaS integrates with DSC for data-classification protection against data leakage and regulatory noncompliance, controlling the flow of documents to cloud applications—unsanctioned, tolerated, or sanctioned—based on the sensitivity of the data, surfaced through DCS metadata classification.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

FORTRA[™]

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.