

CODE GREEN NETWORKS NEXT-GENERATION TrueDLP™ 7.0
DATA LOSS PREVENTION (DLP)

FAQ

Q1. What are you announcing today?

- A. We have started shipping the next-generation TrueDLP 7.0, a complete data loss prevention solution that provides enterprise-class DLP without unnecessary complexity. This latest product release extends the TrueDLP architecture and adds significant new data discovery features that will appeal to any organization needing to protect employee, customer, or other information that is considered sensitive.

Q2. How is this new product different from your existing TrueDLP product?

- A. TrueDLP 7.0 improvements include a fully distributed solution architecture for easier scalability and support of geographically dispersed networks; management layer redundancy to ensure reliability; server discovery to locate and identify sensitive data residing on servers and in data centers; improved reporting (scheduled and auto-emailed); and additional administrator roles for managing incidents.

Q3. How will this new version benefit customers?

- A. There is tremendous amount of interest among organizations in finding and securing sensitive data before it is exposed. TrueDLP 7.0 offers enterprises the ability to locate and identify sensitive data by efficiently scanning large data repositories throughout the network, thereby greatly reducing risk of accidental exposure.

Additionally, customers are looking for a straightforward way to implement enterprise-class DLP without incurring complex rollouts, significant costs, and excessive administrative overhead. Most customers also require a solution that is scalable – one that offers comprehensive DLP capabilities and works at multiple offices and locations. TrueDLP 7.0 delivers a scalable, cost-effective enterprise DLP solution that can be implemented and deployed much more easily than many other solutions.

Server Discovery

Q4. Many organizations have large amounts of data residing on servers throughout the network. Is TrueDLP able to search servers to locate files with sensitive information?

- A. Yes. Locating and identifying files with sensitive information is critical to compliance and to protecting organizational assets. TrueDLP 7.0 supports discovery scanning of large server-based data repositories to locate and categorize sensitive data. Detailed reporting is provided so that remediation actions can be taken to secure discovered data.

Q5. What kinds of servers does TrueDLP support for discovery?

- A. The TrueDLP solution can discover and locate sensitive information on many different types of data repositories, including file servers, SharePoint servers, mail servers such as MS Exchange, web servers, FTP servers, even source code control systems that often contain intellectual property (IP). Data connectors are available to enable scanning of additional types of data repositories.

Q6. Discovery scanning of large data repositories can take a long time. How fast can TrueDLP discovery perform when inspecting files? Can it scale to handle discovery scanning of multiple terabytes (TB) of data?

- A. Depending on the Content Inspection appliance model and DLP policy definitions, a single CI appliance can scan and inspect approximately a terabyte of source files per day. Because the solution utilizes a fully distributed architecture, multiple inspection appliances may be applied to easily scale for inspection of multi-terabyte repositories.

Q7. Can the Code Green solution provide discovery scanning for a geographically dispersed network with multiple datacenters? Is there any network impact?

- A. TrueDLP is a fully distributed solution. Multiple appliances may be utilized, allowing discovery scanning to be performed locally at each location. This increases performance, eliminates WAN latency issues, and avoids impacting the network. The solution is centrally managed so that content detection rules and policies may be enforced across the solution. All logging, reporting, and management are centralized, allowing easy management of TrueDLP discovery across an enterprise.

Q8. Can Discovery scans be scheduled, for example to perform daily scans of sensitive public facing servers and monthly or quarterly scans of less sensitive servers?

- A. Yes, the TrueDLP discovery solution allows multiple scans to be configured and scheduled. Different content inspection rules may be applied for each scan, allowing separate DLP policies to be enforced for different data repositories.

Q9. How is TrueDLP discovery implemented? Does it require an agent on each server?

- A. Discovery scanning may be performed directly from the Content Inspection appliance by using agent-less scanning, or via a proxy agent hosted on a workstation. No agents are required on the servers that are the targets of the discovery scans. Separate from server discovery, the TrueDLP solution also offers endpoint discovery, which performs discovery scanning of endpoint devices using the endpoint CI Agent.

Architecture

Q10. How does the new version 7.0 improve the TrueDLP architecture?

- A. With version 7.0 Code Green TrueDLP now offers a fully distributed, modular, and scalable architecture. The solution is appliance-based, with each content inspection appliance offering the full capabilities of network DLP, endpoint DLP and discovery.

New in version 7.0 is capability for each CI appliance to perform its content inspection locally to identify sensitive data and enforce DLP policies. Local inspection and enforcement allows DLP functions to be distributed across multiple appliances, whether to address the DLP needs of geographically dispersed networks, to scale for performance, or to provide redundancy.

Q11. What benefits does this architecture provide to customers?

- A. The TrueDLP solution is the easiest enterprise DLP solution to deploy and manage. It offers complete DLP capability without the complexity introduced by multiple, special purpose DLP appliances. The scalability and performance requirements of large organizations, especially for server discovery, can be met by distributing DLP functions across multiple appliances. The entire TrueDLP solution is centrally managed, offering simpler management with low administrative overhead.

Q12. How many appliances and servers are necessary to implement TrueDLP 7.0?

- A. You can implement a complete DLP solution using a single TrueDLP appliance. Unlike other solutions, TrueDLP does not require additional servers or databases and is not built around multiple specialized appliances that each performs only a single DLP function. Many of our customers implement the three key enterprise DLP capabilities with a single CI appliance and add to the configuration as necessary.

Enterprise DLP versus Point Solutions

Q13. How is TrueDLP different from other DLP solutions? Don't they all do about the same thing?

- A. While there are common features and functionalities in many DLP solutions, in the last year or so the market has diverged into two types of DLP solutions¹. One type is enterprise DLP, often referred to as complete solutions, supporting data loss prevention at endpoints, on the network, as well as discovery of sensitive data at rest. Enterprise DLP solutions utilize sophisticated content detection technologies to ensure highly accurate identification of sensitive data. The other type of DLP solution delivers a point solution focused on just one potential leak path, such as email. These are sometimes referred to as channel DLP solutions. Channel DLP/point solutions are limited to protecting only a single leak path and don't protect against data leaks over other pathways. Channel DLP solutions typically have limited data detection capabilities that have low accuracy and can result in very high false positive rates.

Code Green's TrueDLP is a comprehensive enterprise DLP solution offering all of the cornerstone DLP capabilities. Yet it retains the simple deployment and low management overhead of less capable and less accurate single channel DLP solutions.

Q14. We have heard of some DLP solutions that focus on just email encryption or other single channels. How is TrueDLP different?

A. TrueDLP not only provides the basic email encryption function, but as a complete DLP solution we also provide network DLP, endpoint DLP, and discovery functions.

Ease of Deployment, Ease of Use

Q15. We've tried or heard about DLP, and it seems complex to set up and manage. What does TrueDLP 7.0 do to help?

A. In general, enterprise DLP solutions have been unnecessarily complex to deploy and manage, often requiring multiple appliances as well as management servers and databases. TrueDLP 7.0 is a very simple solution to implement. We offer a fully contained, appliance-based solution that provides all DLP capabilities. TrueDLP is managed via a web browser and doesn't require a separate server or database. Some organizations implement our DLP solution in phases, beginning with monitoring network traffic to detect if confidential data is being transmitted. They then often enable inspection of email and/or web traffic and in some cases choose to block traffic that might otherwise leak sensitive data. They may add server discovery to inspect data residing on servers. Finally, they may deploy CI Agent software on desktops and laptops to provide both endpoint DLP and endpoint discovery.

The advantage of the TrueDLP solution is that each of these capabilities may be enabled on the solution without requiring deployment of additional servers or appliances. Each Code Green TrueDLP appliance offers all of the enterprise DLP functionality needed.

Q16. How long does a typical installation take to get up and running?

A. We have had some users up and running in a few hours. One customer, Cascade Healthcare Community (CHC), installed TrueDLP for about 3,000 seats and was running in less than a day.

Q17. How many people are required for the ongoing management and maintenance of TrueDLP?

A. No extra people should be required just to manage your DLP solution. Our customers tell us they typically spend about a half hour a day with TrueDLP to assess the incident logs and various reports.

Q18. How is TrueDLP priced? Aren't these complete DLP solutions expensive?

A. They can be, but TrueDLP 7.0 is unique in its pricing. We have a low initial cost for the appliances, beginning at \$9,900, with user license fees additional. TrueDLP is unique in that user licenses are based on one-time purchase with no annual subscription fees, resulting in lower cost of ownership over time. Additionally, both monitoring and blocking capabilities are included with each DLP module (network, endpoint, and discovery). Many other solutions include only basic monitoring capability with the initial modules; blocking functionality requires additional purchase that increases the overall solution cost.

Operational costs are low with the Code Green Networks TrueDLP solution. It is easy to use and does not require full-time, dedicated staff members to administer the solution. The TrueDLP solution can be scaled to support additional seats or sites with the simple addition of low-cost appliances that plug-and-play and can be centrally managed.

Q20. How is TrueDLP distributed?

A. Code Green Networks solutions are primarily distributed through strategic channel and alliance partnerships.

Q21. What are future enhancements for TrueDLP?

A. We will continue to evaluate additional features around discovery and management capabilities. We also continue to evaluate appropriate industry relationships in order to expand our distribution and capabilities with complementary products.

Copyright © 2010 Code Green Networks, Inc. All rights reserved.

All products mentioned in the release are trademarks or registered trademarks of Code Green Networks. All other trademarks, trade names and product names are used solely for the purpose of identification and are the property of their respective owners.

¹ Gartner Group “Content-Aware Data Loss Prevention Evolves into Channel and Enterprise Offerings”, 2009