



April 12, 2018

Illumio and Qualys Integrate Their Solutions to Deliver the Industry's First Vulnerability-Based Micro-Segmentation

Integration enables organizations to visualize vulnerabilities across data centers and clouds through a real-time global vulnerability map

SUNNYVALE, Calif., April 12, 2018 /PRNewswire/ -- [Illumio](#) today announced new global vulnerability mapping capabilities on its Adaptive Security Platform[®]. For the first time, vulnerability and threat data from the Qualys Cloud Platform is integrated with Illumio application dependency mapping to show potential attack paths in real time. The integration between the Qualys Cloud Platform and Illumio delivers **vulnerability maps**, enabling organizations to see connections to vulnerabilities within and between applications. This new capability also includes an **East-West exposure score** that calculates how many workloads can potentially exploit vulnerabilities on applications. This integration can be used to generate micro-segmentation policies as compensating controls that reduce East-West exposure and to prioritize patching.

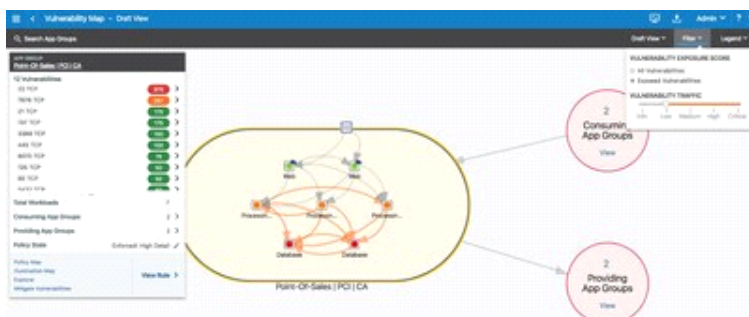
"Digital transformation leads to an explosion of connected environments where perimeter protection is no longer enough. The focus now needs to shift from securing network perimeters to safeguarding data spread across applications, systems, devices, and the cloud," said Philippe Courtot, CEO and Chairman of Qualys. "The new Illumio integration with Qualys helps enterprises get visibility across hybrid environments and implement appropriate controls to protect assets from cyber threats, whether on premises or in the cloud."

Software vulnerabilities in applications have been the cause of recent headline-grabbing attacks and data breaches around the world, including WannaCry, NotPetya, and Apache Struts. Meltdown and Spectre are among other recent examples of vulnerabilities where potential exploitation could give attackers access to an environment - or to move laterally within data centers and clouds. Due to the growing scale of infrastructure and software vulnerabilities, organizations are unable to patch every vulnerability and may be unable to patch many critical vulnerabilities due to production freezes or for fear of breaking their applications.

"Vulnerability management is an invaluable tool in every security team's arsenal. With our Qualys Cloud Platform integration, organizations can see a map of how active, exposed vulnerabilities can potentially be exploited by a bad actor," said Andrew Rubin, CEO and co-founder of Illumio. "By adding vulnerability maps to our Adaptive Security Platform, security teams can see potential attack paths in real time and immediately implement micro-segmentation to prevent the spread of breaches."

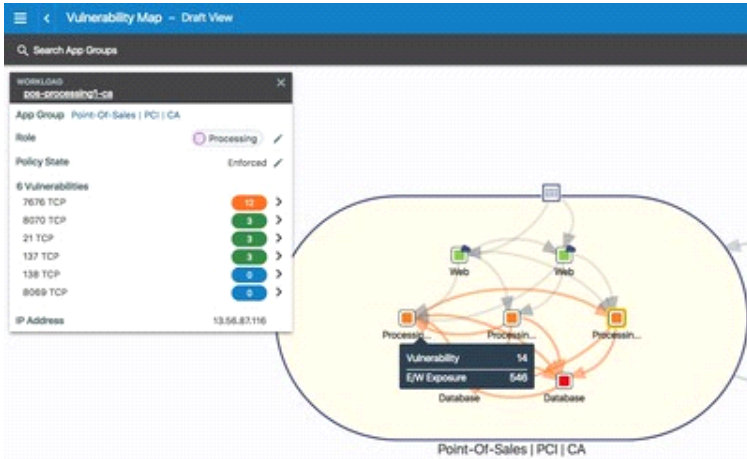
New capabilities of the Illumio Adaptive Security Platform:

- 1 **Vulnerability Maps:** Enable application security teams, vulnerability management teams, and segmentation teams to understand the paths that bad actors can leverage within data center and cloud environments. Vulnerability maps:
 - 1 Show in real time which applications are connecting into vulnerable ports.
 - 1 Show the risk inherited by destination applications when the initiating connections are unpatched.
 - 1 Eliminate unnecessary attack surface by showing vulnerabilities with no active or historic traffic.

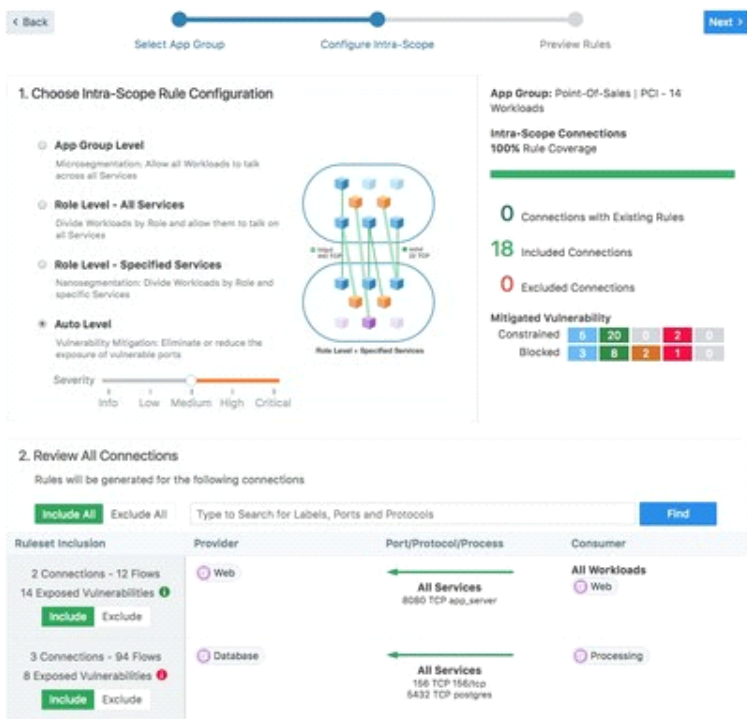


- 1 **East-West Exposure Score:** Using workload, application, and connectivity context, Illumio gives organizations an exposure score for their East-West traffic. The score is calculated based on how many workloads can potentially

exploit the vulnerabilities on any given workload. The lower the score, the smaller the chance that a bad actor can exploit it. If patching is not available, the optimal way to reduce exposure is to use micro-segmentation to reduce the number of workloads that can connect to it.



- Automated Policy Recommendations Based on Vulnerabilities:** Mitigates vulnerabilities through automatic policy recommendations. The Adaptive Security Platform now ties vulnerability data to application traffic in real time, providing organizations with the ability to use micro-segmentation to prevent the spread of breaches.



Illumio has maintained a track record of continuous innovation to meet the growing needs of the emerging micro-segmentation market. In 2017, Illumio achieved 300 percent year-over-year bookings growth. This rapid growth is being driven by organizations who are increasingly turning to Illumio to prevent the spread of breaches inside data center and cloud environments and to meet regulatory compliance standards such as SWIFT, PCI, GDPR, and HITRUST.

[Watch the demos](#) to learn more about vulnerability maps and the Illumio Adaptive Security Platform.

About Qualys Cloud Platform

As a revolutionary unified architecture powering more than 15 Qualys security and compliance Cloud Apps, the Qualys Cloud Platform offers customers a streamlined solution for avoiding the cost and complexities of managing multiple security vendors. By automatically gathering and analyzing security and compliance data from IT assets anywhere in one single-pane view, the Qualys Cloud Platform gives customers the scalability, visibility, accuracy and breadth of capabilities to fight cyber attacks and build security into their digital transformation initiatives.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 10,300 customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL Technologies, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance. For more information, please visit www.qualys.com.

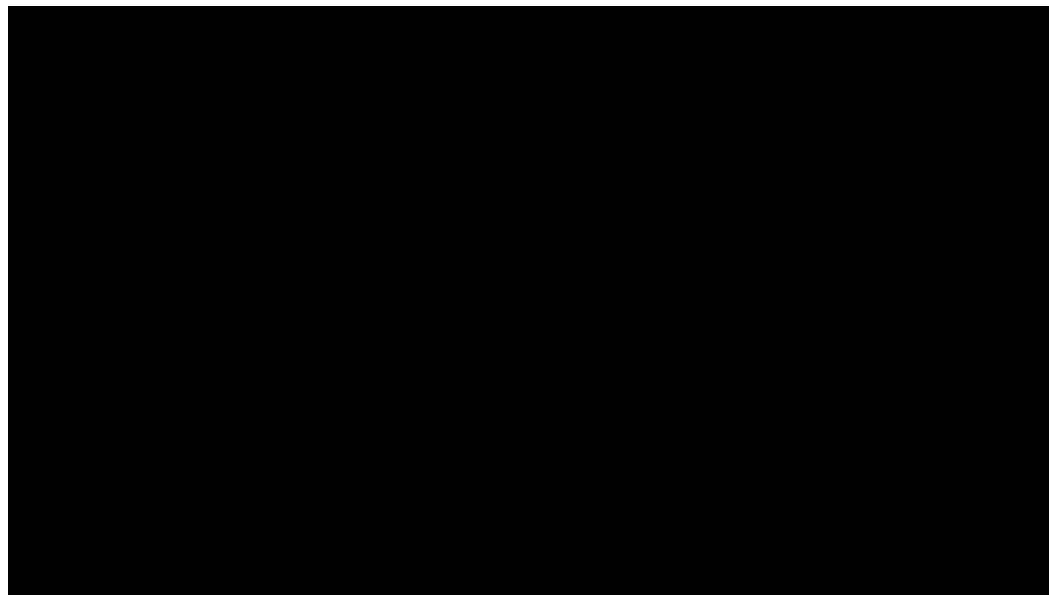
Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

About Illumio

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform[®] uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information, visit www.illumio.com/what-we-do or follow us @illumio.

- | [Engage with Illumio on Twitter](#)
- | [Follow Illumio on LinkedIn](#)
- | [Like Illumio on Facebook](#)
- | [Join Illumio on G+](#)
- | [Subscribe to the Illumio YouTube Channel](#)

Media and Analyst Contact
illumio@bateman-group.com



View original content with multimedia:<http://www.prnewswire.com/news-releases/illumio-and-qualys-integrate-their-solutions-to-deliver-the-industrys-first-vulnerability-based-micro-segmentation-300628657.html>

SOURCE Illumio

News Provided by Acquire Media