



Securing a Global Infrastructure with Network Visibility and Access Control

CUSTOMER SEGMENT

Global Enterprise

INDUSTRY

Commercial

PROBLEM

Diminished visibility of network traffic due to continually expanding attack surface and digital transformation

SOLUTION

Reduce your risk and effectively mitigate attacks of your expanding attack surface with unified visibility, access control, and network segmentation across global sites leveraging Gigamon and Fortinet cybersecurity solutions

RESULT

Enhanced network traffic visibility with rapid vulnerability identification and incident management

and a bewildering array of applications and devices connect to the enterprise network. Enterprises are more interconnected than ever and there are no signs of a slowdown. Devices are connecting, creating, and sharing information at an unprecedented rate. Digital transformation and demand for data-driven decision-making will only accelerate these dynamics — creating greater volume, velocity, and variety of data than we've ever seen. This poses unique challenges for network operations and security teams as they grapple with business, operations and security requirements.

As workflows become more digitized and highly interconnected, the glue that binds it all together is the public, private, and software-defined networks supporting data transfer. The increased speed and growth of network traffic strains traditional point defense cybersecurity tools that can only address a limited set of threats but can't provide global insight or integrated response capabilities.

Adding more security devices isn't the solution because organizations already rely on as many as 75 different security products — many addressing only a single function.¹ This overreliance on point defense products creates gaps that leave vulnerabilities unpatched or open to attackers. In many cases, these gaps are all an attacker needs to gain entry and then move undetected across the enterprise network.

Indeed, research found that 67% of respondents to a study cited network blind spots as a major obstacle to effective security.² As many as three-quarters of organizations say their

Digital Transformation — a Distributed Enterprise and a Wider Attack Surface

Today's highly distributed enterprise network ecosystems must support agility, innovation, and better business outcomes, all the while maintaining security and privacy. The attack surface continues to expand as operations span IoT and OT industrial networks, across the traditional enterprise perimeter and multiple public and private cloud platforms. Hybrid and distributed is the new normal as new services are launched,

security architecture is disjointed due to nonintegrated security products,¹ and 50% of companies say they lack sufficient insight to identify the nature of network threats.² This results in reactive network security in which response occurs after a security incident has already occurred.

ePlus Eliminates Blind Spots Caused by Point Security Solutions

ePlus partners with Gigamon and Fortinet to effectively reduce the attack surface with a comprehensive approach to network cybersecurity protection that integrates visibility, access control, and network segmentation. It provides enterprises with complete visibility into network traffic — with traffic analysis to identify signs of breach or compromise. Endpoint protection strengthened by layered access control safeguards wired, wireless, and VPN networks with centralized policy enforcement that ensures only authorized devices and users are permitted to connect. Intent-based segmentation safeguards networks by allowing IT organizations to assign and manage fine-grained security policies in a broad, integrated, and automated fashion.

- **Global network visibility.** Reduce network blind spots with visibility into traffic and threats across physical nodes, virtual nodes, TAPs, and traffic aggregators with the ability to extract traffic intelligence and monitor all through a single pane of glass.
- **Access control.** Identify every device and user as they join the network with the ability to automate response time to breach.
- **Firewalls.** Protect distributed WAN edges and cloud connectivity with a next-generation firewall integrated with SD-WAN security.
- **Network segmentation.** Segment networks based on control risk with adaptive access control and automated threat protection.
- **Security fabric.** Unify and centralize cybersecurity management of networks, endpoints, applications, data centers, clouds, and access control in a single automated, orchestrated solution driven by artificial intelligence.

[Learn more at eplus.com/security](https://eplus.com/security)

Unified Cybersecurity Protection Reduces Risk and Cost

By deploying a network visibility platform, ePlus can help customers improve network visibility by as much as 75% with a cloud-based solution that reduces hardware and software costs by 50%.³ Global visibility into who and what is connected to networks helps enterprises identify suspicious network activity quickly so malicious attacks can be thwarted.

Fewer security incidents mean less business downtime and disruption. Companies that have deployed a network visibility platform have realized up to a 50% reduction in network downtime — and a 50% increase in security resource efficiency.³

Unified security protection also offers additional security benefits. Comprehensive access control makes it possible for global enterprises to manage network access across devices and users with insight and automation that can reduce reaction time to events from days to seconds.⁴ Safeguarding the WAN edge with SD-WAN firewall security ensures that enterprises can access cloud applications with security, ensuring the hybrid environments are protected from persistent threats.

ePlus empowers enterprises to embrace digital transformation securely, knowing they are protected and supported by a dedicated team of resources both regionally and nationally. ePlus has an unmatched breadth of engineering talent and expertise and deep industry relationships, resulting in countless satisfied customers.

About ePlus

ePlus is a leading security technology integrator with a broad solutions portfolio and strong industry relationships. Our security team designs and delivers effective, integrated cybersecurity programs centered on culture and technology, aimed at mitigating business risk, empowering digital transformation, and enabling innovation. We do this by understanding our customers' business challenges and tailoring comprehensive security programs that protect their entire IT infrastructure and help them achieve positive business outcomes.

¹Fortinet, "Fortinet Security Fabric Powers Digital Transformation," March 2019.

²Gigamon, "See What Matters" webpage, accessed Jan. 2020.

³Gigamon, "The Evidence Is Conclusive, Gigamon Visibility Fabric is the Choice for Managing and Securing Your Network Traffic" webpage, accessed Oct. 2019.

⁴Fortinet, "FortiNAC: Network Access Control" webpage, accessed Jan. 2020.

CONTACT US TODAY

eplus-security@eplus.com

eplus.com/security

t in f

CORPORATE HEADQUARTERS:

13595 Dulles Technology Drive
Herndon, VA 20171-3413
Nasdaq NGS: PLUS

© 2020 ePlus inc. - All Rights Reserved.

In Partnership with

Gigamon® FORTINET