ePlus Solution Brief

Reduce Your Attack Surface

Improve network visibility to better protect your organization.

A key challenge organizations are facing as they navigate their digital transformation is a lack of comprehensive network visibility, specifically as it pertains to internal security controls. Without proper access and policy controls and segmentation, your network is left open to threats, and in the event of compromise, lateral movement.

Who Can Access Your Network?

Companies must provide anytime, anywhere connectivity for employees without sacrificing security. Identifying and controlling who and what connects to the corporate network is the first step to securing your enterprise. Today, networks serve a vast array of traditional and non-traditional devices and other endpoints—everything from PCs, tablets and smartphones to industrial controls, virtualized servers, wireless access points and cloud-based applications.

How do the Bad Guys Get In?

Because attackers are often impersonating an authorized user, evidence of their existence can be hard to see. Once an attacker has an established connection to your internal network, they seek to compromise additional systems and user accounts—this is known as lateral movement. Recent well-published attacks were more devastating because lateral movement was unhindered—the bad guy was hiding in plain sight.

Assume that any bad actor with sufficient time and resources will eventually be successful. Therefore it is important to:

1. Rapidly detect breaches
2. Implement internal security controls to reduce post-breach damage

Why is Internal Security Critical?

Traditionally networks have strong boundary protection but no internal security. This gives attackers free reign to traverse the network once they have gained access. The chances of achieving their goals will increase the longer that they're able to maintain a foothold. Unmanaged laptops, tablets, smartphones as well as servers and IoT and industrial systems of all shapes and sizes significantly expand your attack surface, and are mostly invisible to many security tools. Enterprises need an efficient way to grant, limit or block network access depending on the identity and suitability of the user and device.

How ePlus Can Help

ePlus provides technology and services to help our clients mitigate the risks associated with lateral movement, compromised credentials and lack of network visibility. We help navigate the sea of solutions and software to provide you an efficient, integrated and affordable solution. We work with your organization and understand the skills, processes and technology you have made investments in and will tailor our approach to ensure your organization is best positioned to mitigate this critical risk.

Contact us today to learn more about how the ePlus approach to Reducing Your Attack Surface can be implemented for your environment.

Approximately **95% OF EMPLOYEES** say they use at least one personal device for work.

Worldwide internet users increased from 3.39 billion in 2016 to **3.58 BILLION** in 2017.

38% OF COMPANIES report 'detecting and reacting to security incidents' in the cloud as a top security challenge.

the number of 'internet-connected things' is expected to reach **50 BILLION** By 2020.

CONTACT US

eplus-security@eplus.com

1-888-482-1122

www.eplus.com/security

Where Technology Means More®

THE EPLUS APPROACH TO REDUCING YOUR ATTACK SURFACE

ePlus leverages partnerships with leading technology providers and couples that with deep technical knowledge and experience to provide a comprehensive approach to improving network visibility, tailoring access control methods and deploying organizationally appropriate network segmentation, with the ultimate goal of reducing your attack surface.

IMPROVE NETWORK VISIBILITY

Visibility and detection is a minimal starting point for securing your network. The distributed nature of today's infrastructure has made it more challenging to access data in motion in locations beyond the traditional data center. In order to receive telemetry from all network traffic on which to perform analysis, **blind spots need to be eliminated**. Architecting a security delivery platform, delivering network traffic visibility across the enterprise and enabling effective security for the enterprise, will maximize service assurance and quality of experience for subscribers. By leveraging technology that brokers network traffic, specific **policy enforcement points** can analyze traffic for any signs of nefarious activity, any unauthorized devices or users connecting or attempting to connect to valuable assets, then take appropriate action to isolate or contain the event.

IMPLEMENT ACCESS CONTROLS AND POLICY MANAGEMENT

A **layered access and policy control** solution must manage the corporate and employee-owned devices you know as well as the increasing numbers of unauthorized, 'under-the-radar', devices you don't. Being able to **centrally manage** and unify your network access polices across a highly distributed enterprise to provide consistent, highly secure access to end users, whether they connect to your network over a wired, wireless, or VPN connection, is paramount. Whether a contractor, student, corporate guest, staff or BYOD device connects to your network, **policy enforcement** should ensure the correct networks and applications from authorized devices. Additionally, the ability to perform **posture assessments** automatically can ensure compliance before a device is permitted to connect. Where possible, native access control features within the existing infrastructure should be leveraged to maximize security ROI. Where gaps in critical features or capability exist, overlay tools can be used to compliment those native to the infrastructure, or they can replace them completely.

SEGMENT YOUR NETWORK TO ISOLATE DEVICES AND FUNCTIONS

Network segmentation is a necessary step in an organization's network security strategy. Segmentation segregates and protects key company data and limits attackers' lateral movements across the corporate network. It is also effective in reducing the scope of audits. Micro-segmentation is the security technique that enables **fine-grained security policies** to be assigned to data center applications, down to the **workload level**. Having a strategy for segmentation and micro-segmentation in the enterprise is fundamental to ensuring the success of the implementation. Many infrastructure solutions today include fully featured and powerful capabilities natively. For those that do not, or where gaps in critical features or capability exist, overlay tools can be used. **Consolidating and centralizing** the network infrastructure is a key driver for segmentation. Previously isolated application infrastructures are now migrating to common shared physical and virtual networks that require separation to maintain some level of isolation. Similarly, networks have gone through a dramatic shift over the past few years with the introduction of virtualization, containers, smart phones, tablets, wireless connectivity, industrial control systems (ICS) and the Internet of Things (IoT). Network segmentation—which limits the scope of a breach—is arguably the best defense against the latest, sophisticated security threats.

Cyber Security Frameworks

ePlus provides advisory services to help companies pursue alignment to leading industry frameworks such as CIS and NIST.

Indicates control is either fully or partially addressed by this ePlus solution.

CIS CONTROLS ADDRESSED

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

NIST CYBERSECURITY FRAMEWORK ALIGNMENT

IDENTIFY

ID.AM	ID.BE	ID.GV	ID.RA	ID.RM	ID.SC

PROTECT

PR.AC	PR.AT	PR.DS	PR.IP	PR.MA	PR.PT

DETECT

DE.AE	DE.CM	DE.DP

RESPOND

RS.RP	RS.CO	RS.AN	RS.MI	RS.IM

RECOVER

RC.RP	RC.IM	RC.CO

Corporate Headquarters:
13595 Dulles Technology Drive
Herndon, VA 20171-3413

Nasdaq: PLUS