Contact:
Noelle LaPointe
(904) 928-8114
nlapointe@entint.com

FOR IMMEDIATE RELEASE:

Increase Operational Efficiencies with EI's Autonomous Security Visualization Tool

JACKSONVILLE, Fla. – Picture your employee receiving an email with an attachment that appears to be legitimate. However, your organizations' spam filter determined the attachment to be a phishing email and alerts your employee on the harmfulness of the file. Innocently, your employee bypasses the alert and opens the file. A data breach occurs and you need answers fast. In order to get to the root of this crisis, it will require your security analyst to quickly study the trend of malicious activity within the organization. While this task is imperative to contain the damage, the security analyst knows there's most likely malicious activities beyond this one alert and time is a huge factor. How can these malicious activities be found in a quick and efficient manner?

To better locate the root cause and communicate the attackers' findings on the network, the organization must be able to eliminate human intervention from intelligence sharing. Through security analytics and visualization, implementing an Indication of Compromise ("IOC") vision can help your organization quickly and effectively identify and eliminate compromising network behaviors. The IOC provides your organization with a greater understanding of the activity on your network, leading to faster remediation and a more resilient network security posture.

Through an extension of the IOC, Enterprise Integration's ("EI") SDI Endpoint Experience™ client provides your organization with rapid insight into all of your organizations network behaviors. The IOC uses data gathered by EI's SDI Endpoint Experience™ client and combines it with threat patterns to deliver a high-level threat assessment to each device. Furthermore, within the IOC, compromises on an endpoint can be narrowed down by a time of reference, application, processes, web requests and geography. By autonomously collecting all critical system information in less than 30 seconds, it points the Security Engineer to the root of the compromised application removing up to 5 hours of data research, per security incident.

After all, in a time of crisis, saving time is saving money. The longer it takes your organization to find the root of the compromised application, the higher probability of being faced with class-action lawsuits, fines, penalties and lost business opportunities. Protect your organization and your people by allowing EI Security Engineers to quickly and efficiently resolve the root of your problem with our autonomous security visualization tool.

EI's Director of Security Operations and leader behind the autonomous visualization tool, Mack Bhatia, said, "Given the proliferation of threat vectors to an organization's information technology infrastructure, the likelihood of impact, small or large, is very high. What matters is your incident response plan and specifically the tools you have within your incident response toolkit to limit the damage and reduce recovery time and cost. This is where EI's combination of automation tools and the IOC vision make a difference for our clients - providing us the ability to rapidly identify, contain, and eradicate the root cause and recover from the incident."

###

Enterprise Integration (EI) is a customer-service driven managed service provider headquartered in Jacksonville, FL, delivering the promise of IT worldwide. EI offers proactive IT monitoring and management, managed outsourcing, security solutions and ITIL consulting. By focusing on innovative technologies that prevent IT problems, EI allows companies to focus on their core business goals. EI employs the industry's most experienced people who are further empowered by best practice methodologies and best of breed tools. To learn more, visit www.entint.com.