



TRAPX

## DECEPTIONGRID™

### Adaptive Defense for Advanced Threats

- ✓ Scale-out Virtual DeceptionGrid
- ✓ Automated Malware Traps & Sandboxing
- ✓ BotNet Detection
- ✓ Integrated Threat Intelligence
- ✓ Multi-Tenant Cloud Management

#### DeceptionGrid – Our Flagship Product

Deception-based cyber security defense enables customers to meet and defeat the threats of advanced persistent threats (APTs), zero day events and other sophisticated malware. DeceptionGrid automates the deployment of a network of camouflaged malware traps that are intermingled with your real information technology resources. These traps appear identical in every way to your real IT assets. Once attackers have slipped past your other cyber defense products, they move laterally to find high value targets. Just one touch of DeceptionGrid sets off a high confidence ALERT. Real-time automation isolates malware and delivers a comprehensive assessment directly to your security operations team (SOC). You are ready to defend your enterprise and defeat the malware. DeceptionGrid changes the rules of engagement and helps you take the initiative back from the attackers.

#### Uniquely – We Protect the Core of Your Enterprise

Real-time detection of malware movement anywhere within the vLan in your Deployment of DeceptionGrid sensors is comprehensive across the entire enterprise and provides virtually 100% coverage.

Reduction in the big data problems bringing hundreds to thousands of alerts that overwhelm the SOC Or missing key alerts due to the configuration of alert thresholds. A TrapX alert is over 99% accurate and immediately actionable.

Complete analysis of malware, even zero day events, is automated and your security operations center has everything they need to take action.

Automated deployment of your DeceptionGrid for your entire enterprise enables provision and management on a scale previously unattainable with legacy honeypot technology.

Protect all vLans for identified malware and malicious activity. When you find one instance of a threat within your network, our Threat Intelligence Center insures that this important information is rapidly communicated. DeceptionGrid moves rapidly to help you find other instances of the advanced malware anywhere within your networks and infrastructure.

Outbound Botnet detection rapidly detects hidden exfiltration activity. Working in conjunction with DeceptionGrid, we identify sources masking exfiltration through the use of encryption.