We Asked Our Partners: **How Do You Differentiate in a Cluttered Marketspace?**

Here are their responses.

ForeScout

ForeScout is transforming security through visibility. Detailed visibility drives every aspect of enterprise security. The ForeScout platform provides comprehensive visibility into what's on the network—including traditional systems (infrastructure, PCs, laptops, tablets, smartphones, etc.), BYOD, IoT devices and operational technologies. It automatically categorizes these systems and assesses their security posture, then continuously monitors them to detect whether their security posture changes. We provide sophisticated access control to allow compliant devices onto the network while blocking non-compliant or compromised systems until they are made safe.

Today's enterprises typically have a dozen or more security products operating as independent security management silos. This disjointed approach prevents coordinated, enterprise-wide security response, allowing attackers more time to exploit system vulnerabilities. It also results in manual, inefficient processes that can't scale to address the growth of BYOD and the IoT.

ForeScout helps enterprises tear down operational silos that exist between multiple security and IT management tools. To achieve this, we partner with other security vendors to make their solutions and ours smarter by sharing information in real time and automating workflows and processes—making cybersecurity vastly more effective.

Our partner integrations, offered as ForeScout Extended Modules, use the power of ForeScout CounterACT®. These Modules bring the visibility, policy-based access controls and remediation functionality of CounterACT to many security tools that would otherwise lack enforcement capabilities. Enterprises can then share contextual device data and automate policy enforcement across disparate solutions, bridge previously siloed IT processes, accelerate system-wide response and more rapidly mitigate risks.

okta

Okta was founded in 2009 with a unique proposition: building identity management from the ground up as a cloud-based service. Our core differentiation lies in our ability to connect people and technology, and we've grown significantly in our ability to do so – today reaching nearly 4,000 customers around the world and surpassing a major corporate milestone with our IPO in April 2017.

What specifically sets us apart? We've continued to extend our ability to enable any organization to connect any combination of people and the technologies they need to be productive. With more than 5,000 cloud and on-premises integrations in our network, Okta today has by far the broadest and deepest technology catalog in the industry. We've also added capabilities to make those connections simpler and more secure not only within an organization, but with partners and customers – and today, Okta's identity-driven approach to security establishes us as a leader in helping organizations connect, protect and manage millions of identities. And don't just take our word for it: Okta has been named a category leader by both Gartner and Forrester.

Currently, there are **over 2,500 security technology organizations**, and **CISOs often struggle to differentiate and understand value** between them.

Read how these companies **stand out**.

Centrify®

Centrify provides Zero Trust Security through the power of Next-Gen Access.

As traditional network perimeters dissolve, security professionals must discard the old model of "trust but verify", which relied on well-defined boundaries. Instead, strengthen security levels by implementing an "always verify" approach for everything — including users, endpoints, networks, servers and applications.

The Centrify Zero Trust Security model assumes that untrusted actors already exist both inside and outside the network. Trust must therefore be entirely removed from the equation. Centrify's Zero Trust Security assumes users inside a network are no more trustworthy than those outside the network. It presumes that everything (users, endpoints, networks, resources) is untrusted and must be verified first so that security is not compromised.

Centrify's Next-Gen Access (NGA) offers an integrated set of mature and proven technologies and capabilities — including single sign-on, multifactor authentication, mobility management, privilege management and behavior analytics — that are aware of every device, know every user, limits access and privilege intelligently, and constantly learns and adapts without impacting user experiences.

Through a unified, integrated services offering, Centrify provides identity services across applications, endpoints and infrastructure for all users, without sacrificing best-of-breed features. Organizations may consider approaching Zero Trust by implementing IDaaS, MFA, EMM, PAM and User Behavior Analytics (UBA) technologies from separate vendors, but disparate solutions leave gaps and are expensive to separately license, implement, integrate and maintain your already cluttered set of security technologies.

For more information on how you can implement Zero Trust Security across your organization with Centrify, visit Centrify.com/ZeroTrust.

SentinelOne

Antivirus and other endpoint solutions have focused on binary and signature-based malware prevention since the 1980s—but today, attacks are sophisticated and executed in different ways. SentinelOne is shaping the future of endpoint security through its unified, converged platform that autonomously prevents, detects, and responds to threats in real-time for both on-premise and cloud environments. The SentinelOne platform tackles problems legacy antivirus and many other next-generation endpoint security solutions simply can't – and replaces legacy antivirus solutions in 80 percent of new deployments.

SentinelOne protects against all threat vectors pre-execution, on-execution and post-execution, and since it is powered by AI and machine learning, SentinelOne does not require any prior knowledge of an attack to detect and remediate. Its automated EDR capabilities can deploy rollback functionality post-execution to return a computer to a pre-infected state. The platform is equipped with a 360-degree view of endpoints and threats from inception to termination which powers forensics and policy enforcement.

The platform provides full threat hunting visibility without needing to decrypt and re-encrypt traffic as it travels across the network. This holistic approach allows for maximum prediction, detection, and response on file-based and fileless attacks online or offline, with a minimal system footprint.

SentinelOne is the only vendor in the space to offer a cyber threat protection guarantee program with financial assurance of $1,000 per endpoint, or up to $1 million per company, if it is unable to block or remediate the effects of a ransomware – taking endpoint security to the next level.