Compromise Assessment

Identify ongoing or past attacker activity in your environment

- Comprehensive analysis of your specific environment focused on finding evidence of ongoing or past compromise
- Provides a view into systemic risks and exposures
- Identifies security hygiene issues
- Provides recommendations for furthering your organization's ability to effectively respond to future incidents
- Flexibility to deploy on-premises or cloud-hosted technology

The need for compromise assessments

High-profile data breaches in the news represent only a fraction of the intrusion activity carried out globally. Knowing whether your organization has been breached and identifying ways to reduce risk is crucial to preventing your organization from becoming the next major data breach headline.

Our approach

We combine our extensive experience responding to intrusions and industry-leading threat intelligence with technology that will deliver an assessment that meets your business objectives with speed, scale, and efficiency. In addition to identifying evidence of past or ongoing attack activity, the assessment offers:

- **Context derived from threat intelligence**

Provides insight into attacker attribution and motivation so organizations know if they are being targeted.

- **Identification of risks**

Identifies security architecture and configuration weaknesses, including missing patches or security software.

- **Facilitation of future investigations**

Recommends strategic options that can better prepare your organization's security team to respond to intrusions.

Double Technologies uses specific technology to search endpoints, monitor network traffic, inspect email and analyze logs from other security devices for evidence of attacker activity. Double Technologies also uses signatureless data analysis techniques to find previously unseen attacker activity. Customers choose the correct combination of technologies that makes the most sense for their environment.

- **Endpoint inspection.** Endpoint Security agents are used to provide real-time detection of attacker activity, including malware and other tactics, techniques and procedures, and investigate Windows, macOS and Linux endpoints. Double Technologies provides the flexibility of on-premises and cloud deployments.

- **Network inspection.** Security sensors are deployed in strategic monitoring locations in your enterprise to detect compromise activity such as malware command and control communication, unauthorized remote access, and data theft.

- **Email inspection.** Email Security monitoring is conducted on premises or from the cloud and can be configured to passively inspect inbound and outbound email. Dynamic inspection of attachments allows Double Technologies to identify intrusion campaigns before other signature-based products.

- **Log inspection.** Double Technologies leverages multiple technologies to review logs from applications and infrastructure to identify malicious activity.

ENDPOINT INSPECTION

- Real-time alerting of ongoing suspicious or malicious activity
- Commodity malware detection using specific agent's.
- Cross-platform operating system support
  - Windows
  - macOS
  - Linux
- Identification of anomalies that would indicate the presence of advanced malware

NETWORK INSPECTION

- Full packet capture combined with custom detection signatures
- Automated detection and decoding of attacker command and control traffic

- Detects targeted phishing attacks used by attackers to regain access to the environment after a remediation event

- Our technology utilizes an analysis engine to analyze email attachments and URLs against a comprehensive cross-matrix of operating systems, applications and web browsers
- Supports analysis against Microsoft Windows and macOS operating system images
- Analyzes threats hidden in files including password-protected and encrypted attachments