CASE STUDY

COMCAST BUSINESS | MASERGY

MASERGY SOLUTIONS

Managed Security

Intertrust tackles compliance with a security team that runs the extra mile

A provider of high-end legal and financial administrative services, Intertrust Group B.V. is recognized by the financial institutions and individuals it serves as a leader in the trust business.

Intertrust takes seriously its responsibility to ensure clients' valuable data is secure and that its systems don't become prey to cybercrime.

That job isn't getting any easier, though. Since conducting a successful IPO in 2015, the company has become more visible. Not surprisingly, a heightened public profile tends to increase security risks for companies.

Following the acquisition of Elian Group in 2016, Intertrust has 42 offices in 31 jurisdictions, each with their own regulatory security requirements.

"Intertrust needs to understand its threat profile at any moment in time and identify malicious threats on the network, said Intertrust Director of Strategy and Infrastructure."

It's not easy to effectively combat the dangers presented by the growing number of criminals who can simply buy exploit kits on the Dark Web to deploy against their targets. Intertrust was hardly able to keep up with these threats and protect themselves.

Security partner

Hiring a couple of dozen additional IT personnel to conduct 24x7 network monitoring could help Intertrust improve its security posture. Its IT department already provides firewalls, encryption, server software patching and business continuity operations. But taking on the responsibility for managing additional security solutions was not deemed an optimal approach for the organization.

Intertrust selected Masergy because it offers the flexibility and service focus that Intertrust required. Masergy's Unified Enterprise Security (UES) solution provides Intertrust with 24x7 continuous monitoring, integrated vulnerability

"Masergy staff is always willing to take on additional challenges and run the extra mile. That's very valuable."

Intertrust Group Director of Strategy and Infrastructure

management, and intrusion detection and prevention. The solution also includes network access policy monitoring, control and oversight.

The UES threat intelligence dashboard delivers a wealth of comprehensive reports about security status. "We get more insight of where the issues are in our network with Masergy," said Intertrust Director of Strategy and Infrastructure. "We get notified if there are serious issues that we need to do something about."

Masergy does the hard work behind the scenes in intelligently filtering the threat data results it provides to Intertrust. Its network behavioral analysis techniques means that it continuously adapts to Intertrust's unique network, applying multi-tiered correlation to provide better predictive and proactive threat data.

UES combines its machine learning and big data analytics with human security expertise in identifying, investigating and stopping threats. In sum, man and machine work together at Masergy to rapidly deliver highly detailed information to Intertrust about threats and help enact countermeasures to halt them before they cause material harm.

A team approach

The technology is a winner for Intertrust, and so too is the Masergy security support team to which the IT staff has ready access. "They've always had the right people onboard to make decisions, who can give you the right advice of what you should and should not do," said the Intertrust Director of Strategy and Infrastructure.

The technical specialists at Masergy's security operations center also provide training to Intertrust staff to help them interpret the detailed vulnerability reports they receive, which document things like risk indices and compliance classifications. That's been valuable in helping Intertrust IT personnel determine which vulnerabilities are most critical and of the highest priority to address.

Solution highlights

- Immediate, single-source access to threat data
- Intelligent filtering of threat data results
- Consolidated view of security posture
- Comprehensive, custom reports
- Detailed risk index documentation

Recognized results

- IT staff time is allocated more efficiently to support business needs
- Compliance with multi-country data protection laws is improved
- Proactive defense saves the business the potential costs of exploits in both dollars and time

Value achieved

Learning what security problems are out there so that Intertrust can proactively deal with them is an incredible benefit on a daily basis. One example: The company learned from Masergy of the registration of domain names contextually close to its own – intertrustgroup.com – whose existence raises a red flag about their possible use in phishing attacks. Before such attacks could occur, Intertrust was able to block email messages coming from those potentially fraudulent accounts.

Taking steps like these are the start of what Intertrust expects will be an ongoing, mission-critical process. "We have taken action in highly critical areas, but there are still lots of outstanding items that we need to solve," said Intertrust Director of Strategy and Infrastructure.

Intertrust now is taking its Masergy service deployment to the next level, moving its UES solution beyond its internal infrastructure to the cloud and expects to continue to use UES in the new environment.